

11-UT-11



**The National Surface Transportation Safety
Center for Excellence**

**A Policy Review of the Impact
Existing Privacy Principles have on
Current and Emerging
Transportation Safety Technology**

Ray D. Pethel • James D. Phillips • Gene Hetherington

Submitted: May 12, 2011

Lighting	Technology
Fatigue	Aging

Housed at the Virginia Tech Transportation Institute
3500 Transportation Research Plaza • Blacksburg, Virginia 24061

ACKNOWLEDGMENTS

The authors of this report would like to acknowledge the support of the stakeholders of the National Surface Transportation Safety Center for Excellence (NSTSCE): Tom Dingus from the Virginia Tech Transportation Institute, John Capp from General Motors Corporation, Carl Andersen from the Federal Highway Administration, Chris Hayes from Travelers Insurance, Martin Walker from the Federal Motor Carrier Safety Administration, and Gary Allen from the Virginia Department of Transportation and the Virginia Center for Transportation Innovation and Research.

The NSTSCE stakeholders have jointly funded this research for the purpose of developing and disseminating advanced transportation safety techniques and innovations.

TABLE OF CONTENTS

LIST OF TABLES	ii
LIST OF ABBREVIATIONS AND SYMBOLS	iii
CHAPTER 1. INTRODUCTION	1
CHAPTER 2. PURPOSE AND SCOPE	3
WHAT IS PRIVACY?	3
CHAPTER 3. METHODS	5
LEGAL RESEARCH METHODOLOGY.....	5
ITSA MEMBER SURVEY METHODOLOGY	6
RESULTS	7
CHAPTER 4. DISCUSSION.....	9
HOW “PRIVACY” IS LEGALLY PROTECTED IN THE UNITED STATES.....	9
EVENT DATA RECORDER UPDATE	10
CHAPTER 5. EMERGING TECHNOLOGY AND SAFETY APPLICATIONS	13
BASIC CONCEPTS ABOUT EXISTING AND EMERGING TECHNOLOGY.....	13
EARLY VEHICLE TECHNOLOGY AND PRIVACY: AIRBAG MODULE DATA LOGGER	14
TRAFFIC ENFORCEMENT CAMERAS	15
AUTOMATIC NUMBER PLATE RECOGNITION	16
BIOMEDICAL IDENTIFICATION	16
GEO-POSITIONING AND ONBOARD TELEMETRIC COMMUNICATIONS SYSTEMS.....	18
CREATION OF FAIR INFORMATION AND PRIVACY PRINCIPLES	23
CHAPTER 6. THE ITSA PRIVACY PRINCIPLES	25
APPLICATION AND IMPLEMENTATION OF THE FAIR INFORMATION AND PRIVACY PRINCIPLES	26
CHAPTER 7. CONCLUSIONS.....	37
RECOMMENDATIONS.....	37
REFERENCES.....	41
APPENDIX A. The Legal Issues	43
APPENDIX B. ITSA Member Survey	44
APPENDIX C. Bibliographic Annotation of Selected Works Cited	45

LIST OF TABLES

Table 1. State ‘right to privacy’ laws and their sources..... 10

Table 2. Nature of common law torts regarding privacy..... 10

Table 3. Types of information collected..... 28

Table 4. Are ITS systems built in a manner "visible" to individuals?..... 29

Table 5. What types of disclosure do you make? 29

Table 6. Are data that the ITS collects secure? 30

Table 7. What technique or process do you use to ensure that data are secure?..... 31

Table 8. Can people choose to be anonymous to those other than law enforcement officials? 31

Table 9. What kind of information is collected? 32

Table 10. How is anonymity preserved? 33

Table 11. How do ITS businesses handle disclosure of ITS data collection processes? 34

Table 12. How does your business comply with the Fair Information and Privacy Principles and structure them to comply with the FOIA? 34

LIST OF ABBREVIATIONS AND SYMBOLS

AD	Archived Data
AmI	ambient intelligence
ANPR	Automatic Number Plate Recognition
APTS	Advanced Public Transportation Systems
ATIS	Advanced Traveler Information Systems
ATMS	Advanced Traffic Management Systems
AVSS	Advanced Vehicle Safety Systems
CVO	Commercial Vehicle Operations
DHS	U.S. Department of Homeland Security
EDR	event data recorder
EM	Emergency Management
FOIA	Freedom of Information Act
FTC	Federal Trade Commission
GM	General Motors Corporation
GPS	Global Positioning System
IBR	Iris Biometric Recognition
ITS	Intelligent Transportation Systems
ITSA	Intelligent Transportation Society of America
MCO	Maintenance and Construction Operation
NGO	Non-governmental organization
NHTSA	National Highway Traffic Safety Administration
OCR	Optical Character Recognition
RDS-TMC	Radio Data System-Traffic Message Channel
TEC	Traffic enforcement camera
USDOT	U.S. Department of Transportation
VDOT	Virginia Department of Transportation
VII	Vehicle Infrastructure Integration
VIN	Vehicle Identification Number
WBI	Whole Body Imaging

CHAPTER 1. INTRODUCTION

The safety and traffic management of the motoring public increasingly relies on transportation technologies and their applications. Many current and emerging technologies collect vehicular or personal data. Questions about the collected data include the extent to which the data contains, or can be used to derive, personal information, and how the data are managed to safeguard personal privacy. This project is designed to examine the issue of privacy in transportation from the perspective of state and federal laws, state and federal court decisions, and equipment manufacturers who are members of the Intelligent Transportation Society of America (ITSA).

In the United States there is a general perception that the protection of personal information is an absolute right of citizenship.⁽¹⁾ That is not the case. There is no explicit constitutional right to privacy, but there are hundreds of individual laws relating to privacy protection, many of which affect the technology and the applications that are intended to improve transportation safety and manage traffic flow. Three out of every four Americans feel the “right to privacy” should be constitutionally guaranteed in the same manner as the traditional rights to life, liberty, and the pursuit of happiness. However, a large segment of the U.S. population feels its privacy is now under assault.⁽¹⁾ The development of an array of new technologies is now allowing almost anybody with a computer and an Internet connection to collect information and track the movements of any individual without that person’s knowledge or permission. With emerging transportation technologies, the concept of personal privacy is a continuing concern, both in terms of understanding the way these technologies affect personal privacy and how personal privacy can be safeguarded.

While privacy protection is not the only rationale that state and local governments have used for banning technology applications, some state and local jurisdictions have responded to citizens’ objections regarding the invasion of their privacy and lack of due process. For example, in 2009, a Montana state legislator introduced a bill to ban the use of red light cameras. He argued:

We've got a real problem with these red light cameras and how they infringe upon our constitutional rights. Rights to privacy, rights to equal protection under the law, rights to due process and the right to confront our accuser.⁽²⁾

Transportation is fundamental to the working of the country and society and reflects the benefits and detriments that can be realized by the latest technological developments. For example, vehicles equipped with communication devices are in constant contact with a customer service center that will provide help in an emergency or remotely check a vehicle’s system for problems. The same technology allows trucking companies to constantly monitor the movements of their trucks, ensuring that they are avoiding traffic congestion and following the most efficient route. In the not-too-distant future it is envisioned in automated systems that every vehicle may be part of an *ad hoc* network communicating with other vehicles, informing drivers of road and traffic conditions they will encounter.⁽³⁾ While this type of technology presents the promise of improving transportation safety and managing traffic flow, there are questions regarding the collection of personal data and how data are used and protected.

In response to these concerns, in 1998, ITSA assumed a leadership role in developing a set of guidelines (i.e., privacy principles) that spoke to the concerns of the public about how this type of technology should be limited and controlled to protect the privacy of the general public. ITSA's role in creating a set of industry guidelines could be described as a positive example of industry and government collaborating to create a voluntary set of regulations that would protect the interests of the public. The extent to which those voluntary standards are in place and followed is one of the central questions of this study.

CHAPTER 2. PURPOSE AND SCOPE

WHAT IS PRIVACY?

The term “privacy” does not have a common or legally accepted definition in the United States.⁽¹⁾ Understanding privacy concerns is further exacerbated by the apparent lack of consensus across society regarding what privacy means and if and how it should be protected. Wikipedia, the collaboratively written free online encyclopedia, describes privacy as “the ability of an individual or group to seclude themselves or information about themselves and thereby reveal themselves selectively. Privacy is sometimes related to anonymity, the wish to remain unnoticed or unidentified in the public realm.”⁽⁴⁾ When something is private to a person, it usually means it is something that is considered inherently special or personally sensitive.

The U.S. culture places a premium on stressing the privacy rights of the individual and usually associates privacy with personal information and the unwanted prying into our personal lives. This has led the United States to approach the protection of individual privacy differently than the approaches taken in other countries.⁽¹⁾ For the purposes of this study, “privacy” is defined as the traveling public’s expectation that its personal information, communicated to transportation providers, will be protected from uses for which they have not consented (in this case, certain transportation safety and traffic applications).

Accordingly, the fundamental purpose of this policy study then is to gain an appreciation of the broad public viewpoint (public officials and citizens alike) about collection, use, and safeguards of the privacy of personal information collected by others while “on the road” and to examine the legal standards that are applied to determine if these “privacy” expectations have been violated. Nearly all “on the road” technology applies to every vehicle passing through such devices as electronic tolls, vehicle tracking, traffic monitoring, red-light running, several forms of telematics, and the emerging Vehicle Infrastructure Integration (VII), or Connected Vehicle Systems.

While much of that technology is safety-related, many of the concerns that were found relate to technology applications that also serve traffic management such as speed monitoring, red-light running, and vehicle tracking. Much of the public’s understanding of this technology is based on the perception of the invasion of personal privacy. Much of that perception is derived directly from media reports.

The study content and conclusions contained herein relate directly to the collection, management, and use and/or abuse of personal information, not to the safety attributes of transportation technology or the technology itself.

The scope of this study includes two extensive data-gathering techniques: a state-by-state compilation of privacy laws that relate to transportation applications, and a web-based survey of all 360 members of ITSA.

The organization of this report is intended to discuss each aspect of the privacy issue in sequential flow from the laws that govern privacy to the extent to which the industries involved in development, implementation, operation, and enforcement are sensitive to and comply with

the existing privacy principles adopted by ITSA. Moreover, this research will discuss, where appropriate, the relationships between the state and federal legal standards and the underlying constructs of the privacy principles.

This study was felt to be important because of a growing interest in questions of privacy while traveling highways and with regard to other transportation modes in the United States. For example, as stated later in the report, 13 states to date have banned the use of certain safety applications, in part because of privacy concerns; and, where permitting those same technology applications have been put to citizens on the ballot, none have passed.⁽⁵⁾ The scope of this research examined the legal position of privacy protection on state-by-state, federal, and federal district court levels, as well as the extent to which the Intelligent Transportation Systems (ITS) industry complies with the privacy principles adopted by ITSA.

CHAPTER 3. METHODS

In order to present a clear picture of the privacy issues, the following methods were used: (1) a survey was conducted of existing state laws relating to the privacy of personal information (Appendix A, which contains a detailed listing of federal laws and a state-by-state inventory); (2) a list of significant documents that relate to privacy in transportation applications was created; and (3) a survey was administered to the 360 members of ITSA, to which 91 members responded (Appendix B).

LEGAL RESEARCH METHODOLOGY

The first research activity was to inventory current privacy laws within the United States. The point of departure for this research was the work entitled *Privacy and Intelligent Transportation Systems: Legal Research Reports* (1995), edited by Dorothy J. Glancy (“Glancy Report”).⁽⁶⁾ The Glancy Report compiled statutes and case law related to privacy from the 50 states and the District of Columbia. For the current project, the initial task was to update the Glancy Report to account for statutory and case law changes that occurred between 1995, when the Glancy Report was published, and May 2009. As the project progressed, the authors opted to expand the legal research to include a survey of federal privacy laws and additional privacy law topics that were not originally presented in the 1995 Glancy Report. At its completion, the inventory includes federal privacy laws, laws for all 50 states, the District of Columbia, and the 13 Federal Circuit Courts.

The privacy law update used two main tools—LexisNexis and Westlaw. Both search engines provide databases of the state codes and the U.S. Code, which is the source of federal statutory law. These databases are searchable using keywords, natural word queries, and terms and connectors. Accordingly, after formulating a list of pertinent privacy law topics (e.g., public records, motor vehicle identification numbers, and electronic surveillance), string searches were conducted within the individual state code databases and the U.S. Code to find relevant laws.

In addition to the topical searches within the statutory codes, the study accessed 50 state survey databases that address subject matters of interest. The LexisNexis database is called “50 State Comparative Legislation/Regulations” and includes 50 state surveys of laws applicable to topics such as “Commercial Use of Public Records,” “Third Party Disclosure of Personal Data,” and “Non-governmental Surveillance.” Westlaw’s database is called “50 State Statutory Surveys” and includes state surveys of laws applicable to “State Freedom of Information Acts,” “Electronic Surveillance,” and “Constitutional Privacy Protections.” Although these 50 state surveys were not exhaustive and did not include all privacy law topics actually examined or contained in the Glancy Report, they did provide a solid starting point for locating statutory privacy laws.

Once the statutory survey was compiled, the next iteration was a search of case laws within each state and federal district to determine if the court system had weighed in with statutory interpretation. Similar to the statutory searches, a Boolean string search was conducted of the case law databases on LexisNexis and Westlaw. Like the statutory databases, the case law databases are searchable by keyword, natural word, and terms and connectors.

Finally, after completing the statutory and case law surveys, the findings were summarized and condensed into a table format focusing on an aggregation of the most pertinent findings such as privacy tort law and constitutional protections for privacy.

ITSA MEMBER SURVEY METHODOLOGY

This study assessed the currently available and emerging technologies related to “on the road” applications. This was accomplished by utilizing a three-track methodology.

The first method used to develop the report involved identifying and selecting those technologies that most directly involve the collection and use of personal information, or vehicular information from which personal data can be derived. Since the focus was on technology that is used “on the road,” the in-vehicle technologies (about which owners are required to be advised) were not included except in general references.

The second method used was to perform a comprehensive survey of the available body of literature pertaining to transportation privacy. Sources included web-based general and specialized engineering and transportation sources, along with those dealing with the social sciences that presented literature specific to the concept of privacy. The literature search was supplemented with daily monitoring and a collection of general and technical news items from publicly available sources. Finally, the direct professional experience of the authors was drawn upon where applicable.

The third approach was to develop and administer a survey to ITSA members. The ITSA membership was considered a quality sample group because it includes developers, manufacturers, marketers, researchers, and those organizations that deploy the various types of technology relevant to this study. Additionally, ITSA members are expected to be aware of currently published privacy guidelines. It was felt that their responses would provide a valid metric for assessing the level of sensitivity and compliance with these guidelines. The 10 privacy principles require that ITS:

- must recognize and respect the individual's interests in privacy and information use.
- will be built in a manner visible to individuals.
- will comply with applicable state and federal laws governing privacy and information.
- will be secure.
- have an appropriate role in enhancing travelers’ safety and security interests; but absent consent, statutory authority, appropriate legal process, or emergency circumstances as defined by law, information identifying individuals will not be disclosed to law enforcement.
- will only collect personal information that is relevant for ITS purposes.
- should provide individuals the ability to utilize ITS on an anonymous basis where practicable.
- information, stripped of personal identifiers, may be used for non-ITS applications.
- should balance in database arrangements the individual's interest in privacy and the public's right to know.
- should have an oversight mechanism to ensure that such deployment and operation complies with the Fair Information and Privacy Principles.

The survey was written in two main sections. The first separated the respondents by the eight architectural classifications: Advanced Traffic Management Systems (ATMS), Maintenance and Construction Operation (MCO), Advanced Public Transportation Systems (APTS), Advanced Traveler Information Systems (ATIS), Commercial Vehicle Operations (CVO), Emergency Management (EM), Archived Data (AD), and Advanced Vehicle Safety Systems (AVSS). Each organization was queried regarding the types and usages of its technologies and its primary market within the transportation industry. The second section inquired how the organizations collected and handled data in their possession. All respondents were asked the same set of questions, covering how they collected data, data security procedures, and if they shared data with other organizations. This section was designed to provide at least a nominal picture of how data and information are being utilized within the ITS industry. The survey was administered via the Internet tool SurveyMonkey; a link to the survey was then emailed to each ITSA member with an introductory letter.

During the construction of the survey, advice was requested from the Virginia Tech Center for Survey Research about structure and content. In total, 360 surveys were sent by email and 91 responses were received.

The survey data were manipulated with raw counts, percentages of respondents to each question, and cross tabulations. In some cases, the responses to questions were combined to permit a better understanding of the extent of sensitivity and compliance with each principle.

RESULTS

In this section of the report, the discussion follows the same sequence of information used in the methodology. First discussed are the legal research findings used to establish an understanding of the statutory and court-ordered basis for the protection of privacy in transportation applications. Next discussed is the technology on which the project team chose to focus; the selected technology is briefly described in order to place the privacy issue into a contextual relationship with the technology and its applications. Finally, there is a discussion of the way in which the ITS industry complies with specific privacy principles using information derived from the survey.

CHAPTER 4. DISCUSSION

HOW “PRIVACY” IS LEGALLY PROTECTED IN THE UNITED STATES

The U.S. Constitution and the Bill of Rights contain no provision for the protection of privacy. Despite the Fourth Amendment’s protection from unreasonable government search and seizure, and the Fifth Amendment’s protection from self-incrimination being interpreted as implying privacy protection, there is disagreement between legal and constitutional scholars as to whether privacy is a valid legal concept.⁽⁷⁾ The controversy has been made even more complex with the development of new and emerging technologies and applications (e.g., camera-based transportation applications, satellite communications and tracking, electronic databases, and the Internet) that have made it easier to collect and store personal information.

The U.S. Supreme Court has been inconsistent in its rulings concerning privacy issues. While the Court has made several precedent-setting decisions regarding privacy, few deal directly with the issue. In the decision announced in *Katz v. United States*,⁽⁸⁾ the U.S. Supreme Court ruled that the use of electronic surveillance in a public telephone booth without the issuance of a search warrant by a magistrate violated the Fourth Amendment's protection against unreasonable search and seizure, affirming that the Fourth Amendment's protection extends to public places.

The Court further noted in *United States v. Miller* that individuals had no expectation of privacy for information supplied voluntarily for commercial uses.⁽⁹⁾ Finally, the court attempted to define a balance between the interests of privacy and government in *Whalen v. Roe*.⁽¹⁰⁾ There, the court ruled that New York State had the right to collect data about individuals and create a database if it was for the public good and if there were adequate security measures taken to protect the privacy and identification of individuals. As part of this ruling, the court recognized and defined what it called a “zone of privacy,” in which an individual may have the expectation of the nondisclosure of personal matters and independence in making certain types of important decisions. These three decisions, along with a host of others, have created a privacy environment that can be described as muddled at best.

This approach to privacy has had the unintended consequences of spreading the promulgation of regulation across a number of varied government entities. The Federal Trade Commission (FTC) Act of 1914 granted the agency the power to prevent unfair business practices, which now includes the *Principles of Fair Information Practices* which governs information over the Internet.⁽¹¹⁾ In 1998 Congress recognized that the privacy protections provided by the FTC were inadequate, describing the situation as “sectoral,” consisting of a handful of disparate statutes directed at specific industries that collect personal data, none of which specifically cover the general collection of personal information. This resulted in the FTC creating the *Principles of Fair Information Practices* and attempting to encourage the private sector to adopt a system of self-regulation.

The ambiguities of both the social and legal situations have conspired to create an environment where any regulation of privacy is not only open to an endless number of interpretations but also creates a liability minefield for companies that develop, manufacture, and deploy technology that involves the collection of private information. Additionally, the existing government control or guidance has left the door open for the private sector and non-governmental organizations

(NGOs) to fill the void by creating regulatory systems designed to fit and protect their institutional interests. (An extensive compilation of state statutory protections is included in Appendix A.) Shown below in Table 1 is a summary of the statutory and common law protections found in the inventory.

Table 1. State ‘right to privacy’ laws and their sources.

	Express Privacy Guarantee in Constitution	Implied Privacy Right from Constitution	Constitutional Restriction on Search and Seizure	Electronic Surveillance Statute	Electronic Surveillance Does Not Include Tracking Devices
Number of States	11	14	51	44	23

There are also a number of federal and state court decisions that grant protection against the invasion of privacy. The detailed information on a state-by-state basis is included in Appendix A. The summary of each category of common law tort is shown in Table 2.

Table 2. Nature of common law torts regarding privacy.

	Appropriation	False Light	Intrusion	Public Disclosure
	Using one’s likeness for commercial purposes without permission	Disseminating material falsehoods about a person	Invasion of one’s seclusion or privacy	Disseminating true but sensitive and private information about a person
Number of states	48	43	46	45

EVENT DATA RECORDER UPDATE

The Glancy Report concluded with a discussion of a California statute that mandates automobile manufacturers to disclose the presence of event data recorder (EDR) mechanisms in the owner’s manuals of new automobiles manufactured after July 1, 2004, and sold or leased in the state of California. These EDR “black boxes” have the capacity to collect and record information from the vehicle such as speed, direction, travel history, seatbelt use by the driver, and accident-related data.⁽⁶⁾ The statute further requires that releasing data from the device can occur only with the consent of the owner for certain types of research about safety issues or in response to a lawful court order. Glancy hypothesizes that, given the California statute’s level of privacy protection for EDR data, “other types of information derived from the activities of people on the open road, protection for driver’s information privacy and autonomy privacy interests will be substantially enhanced.”⁽⁵⁾

Eleven other states have enacted a statute similar to California's "black box" legislation since 2004, which indicates that Glancy's hypothesis was, at least in part, accurate (see Appendix A). As with the California statute, most, if not all, of these 11 state statutes require the owner's consent prior to data being released. Exceptions include: pursuant to a valid court order or search warrant, for safety research purposes, or for diagnostic purposes for servicing or repairing the motor vehicle. An additional bolstering of the owner's consent requirement is available in Oregon and North Dakota where state statutes prohibit insurers from requiring the insured to provide automatic consent for the insurer to retrieve EDR data as a condition of obtaining an insurance policy. One other exception worthy of mention is that the data can be released without the owner's consent if "a law enforcement officer, firefighter or emergency medical services provider seeks to obtain data . . . in responding to . . . an emergency involving the physical injury or the risk of physical injury."⁽¹²⁾ Maine and Washington have exceptions similar to those of Oregon for releasing vehicle data in the event of medical emergencies in order to treat injured individuals.

At the federal level, the *Code of Federal Regulations, Title 49, Sections 563.1–563.12* establish "national requirements for vehicles equipped with event data recorders (EDRs) concerning the collection, storage, and irretrievability of onboard motor vehicle crash event data" for vehicles manufactured after September 1, 2012. The primary purpose of these regulations, however, is directed at safety concerns, advancing the understanding of accident causation, and developing safer vehicle designs, rather than protecting driver privacy. *Section 563.11* does mandate disclosure of the EDR device in the owner's manual, but none of the regulatory sections specifically require the owner's consent prior to releasing data after an accident. Although no personal data, name, gender, age or accident location is either recorded or released by the EDR, federal regulations explicitly acknowledge that law enforcement officials have access to personal identifying information in accident investigations, which could be combined with EDR data without an owner's consent.

Based on this discussion, the conclusion can be drawn that the courts, state legislatures, and federal agencies have generally allowed the release of personal information, otherwise thought to be private, to achieve a public purpose; e.g., protecting the health and safety of the individuals associated with travel in public areas.

CHAPTER 5. EMERGING TECHNOLOGY AND SAFETY APPLICATIONS

This section examines emerging “on the road” technology from the perspective of its privacy implications, placing privacy protection into the context of the technology application. Five overarching examples are included and described with a brief summary of the technology, its safety application, and issues related to the collection, maintenance, and control of personal information. Each technology is capable of recording and storing personal information or vehicle information that can be tracked directly to the owner of the vehicle. How this type of personal information is protected is the subject of our industry survey. Although this study is not concerned with the specific application of the technology, it is concerned with the personal information that each technology collects and uses.

As commonly understood, the development of now commonplace technologies such as sophisticated electronics, computers, and the Internet have provided society the capabilities that previous generations could only conjure in the writings of science fiction. Currently, even the average individual has an almost unimaginable level of technology, connectivity, and information available by simply accessing the Internet. The development of new technologies and capabilities was perceived in the popular media as a positive phenomenon for society. Extensively advertised, each wondrous new technological development could be used for quality purposes and would result in creating a better world and life for society.

BASIC CONCEPTS ABOUT EXISTING AND EMERGING TECHNOLOGY

Two critical concepts associated with technology play a fundamental role in the understanding of privacy issues and need to be introduced: “ambient intelligence (AmI)” and “symbiotic technologies.”

AmI describes the rapidly growing number of “intelligent” items that function in the background of the environment, usually outside of the general public’s consciousness.⁽¹³⁾ This includes items such as the computers that run a city’s traffic light system in an attempt to minimize congestion. All of these “smart” systems function without any notice and keep working in the background. This concept applies to privacy in much the same manner. In places such as London, England, video surveillance cameras are now so numerous and have been in place for so long that people under their watchful eye no longer take notice of them. The cameras have now become “ambient,” blending into the background of the city environment. Londoners on the streets now go about their business as if they were not being observed, with little or no concern that they are constantly under surveillance.⁽¹⁴⁾ The reaction of Londoners to being under constant surveillance presents a possible future reaction to new methods and technologies that further encroach upon personal privacy. As each new method and technology is implemented, an incremental portion of personal privacy is lost, and with each additional technology, a little more is lost again. Since this is all happening slowly in small increments, the public simply accepts it as a new part of life, and the new intrusion becomes just another part of the environment.

Understanding symbiotic technologies is especially important when considering emerging technologies. Symbiotic technologies describe the phenomenon when two or more unrelated technologies are combined to create a totally different capability, as is frequently happening in transportation applications. For example, video cameras, street lights, and the Internet are all

unrelated technologies.⁽¹²⁾ Obviously, street lights are not only numerous in both urban and rural settings but the electrical connection that powers the light can also be utilized to power many other devices. It is a simple task to mount a video camera on a street light and connect it wirelessly to the Internet. What was originally a simple device designed to provide lighting for a dark roadway has been transformed into a surveillance device that provides images of the surrounding area. Multiply the number of cameras mounted on lights throughout a locality, connect them to a central location running currently available tracking software, and all three technologies in combination now form a sophisticated surveillance system that has the ability to watch and track the movements of people and vehicles. Additionally, since this type of system would be out of the common view of the general public, it is likely that this system will become just another piece of AmI.

To place these current technological intersections with personal privacy issues into perspective, a discussion of the historical development of transportation technological applications is in order.

EARLY VEHICLE TECHNOLOGY AND PRIVACY: AIRBAG MODULE DATA LOGGER

In the early 1980s, the National Highway Traffic Safety Administration (NHTSA) mandated that all passenger vehicles sold in the United States must include some form of passive passenger-restraint system.⁽¹⁵⁾ The first response from the automobile manufacturers was the inclusion of a passive seatbelt system that belted in the driver and passenger as they closed the vehicle door. This system proved to be universally disliked by the driving public, which resulted in a large number of owners finding a means for disabling the system. This placed the manufacturers in a no-win situation, where NHTSA required them to include a system that the car-buying public not only disliked but was rendering useless after purchasing the vehicles. In response, the manufacturers moved to another passive restraint technology—airbags.

Starting in the mid-1980s, all new vehicles sold in the United States included a driver-side airbag. This was quickly followed by the addition of a passenger-side airbag. At the heart of the system is the airbag module that monitors the vehicle's movements to determine when a crash is occurring and if the airbags should be deployed. Included in the module is a very small data logger that records the last milliseconds of a crash. The original purpose of the logger was to provide real crash data that could be utilized by the airbag supplier and the vehicle's manufacturer to improve the airbag system. At the time, every manufacturer staffed several employees whose job was to go to the location of a crashed airbag-equipped vehicle, download the logger, and send the data back to the engineers responsible for the system. While the existence of the logger was general knowledge throughout the vehicle safety units, it was considered closely guarded proprietary information and kept from the general public.

The reasons for keeping the logger's existence from the driving public were to protect the vehicle and airbag manufacturers from becoming involved in litigation that resulted from an accident. It was believed that if parties to legal actions knew of the existence of data regarding the crash, they would subpoena the data. This had the potential for placing the vehicle manufacturers in the middle of every major crash, even minor "fender benders." While the inclusion of the data logger in the airbag module was part of the development to improve vehicle

passenger safety, it was also perceived as an early intrusion into the personal privacy of the vehicle driver. While vehicle operators might be under the impression that their driving and minor accidents that occur are private events, the reality is that the airbag module logger is monitoring vehicle speed and accelerations. The privacy concerns associated with this technology are further enhanced by drivers that have no knowledge that their driving is being monitored, and they are not being given the opportunity to consent to being monitored. When the existence of the loggers became general public knowledge, it was described as “having your vehicle testify against you.”⁽¹⁶⁾

TRAFFIC ENFORCEMENT CAMERAS

Traffic enforcement camera (TEC) technology is now commonly used throughout the developed world. In its most fundamental form, video cameras are placed on traffic signal masts with sensors that identify when a vehicle runs an intersection after the light has turned red. The system records an image of the vehicle—and, in some variants, the face of the driver—with a second camera recording an image of the vehicle’s license plate. The same technology is also applied to speed enforcement by utilizing speed sensors and recording the same images of any vehicle that exceeds the speed pre-programmed into the system.

In its earliest form, the TECs utilized the standard film technology, and law enforcement officials had to travel to each camera location to retrieve the photographs. This type of system proved to be cumbersome and unworkable since the number of violator recordings overwhelmed the capacity of the camera system and the ability of law enforcement officials to process the offenses. This led to the creation of what could be labeled as a “traffic enforcement lottery” where all of the camera systems were functioning, but only a maximum of 10 percent were actually loaded with film.⁽³⁾ The advent of digital technology revolutionized the TEC, transforming it into a practical method of vehicle law enforcement. Digital technology allowed an almost unlimited number of images to be recorded and, when combined with networking technology, eliminated the need to retrieve any data from the camera site.

The digitizing of TEC technology has allowed it to be utilized wherever law enforcement officers deem it useful. With the implementation of new software, cameras that currently record only speeding offenses can be configured to record driver cell phone usage and/or failure to wear seat belts. While this is largely an “emerging” technology, it is an extension of the facial recognition function already in use in some TEC systems. Additionally, recording digital images provides the data in a format that is easily processed by standard computer technology and entered into digital databases.⁽¹⁷⁾

Today, images and data are directly transmitted over a network to a central processing center. The TEC systems send images of the vehicle, its license plate, and—in speed enforcement applications—the vehicle’s speed at the time of the offense. At the processing center, the image of the license plate is converted from a digital image to a character string that can be utilized in any text-based software. The offense is entered into a central computer database and processed to match it to the vehicle owner’s identity, address, and driving record. Hard copies are created to be sent to the vehicle owner’s recorded address, informing him or her of the offense along with instructions regarding a court date and the amount of the fine.

AUTOMATIC NUMBER PLATE RECOGNITION

Derived from Optical Character Recognition (OCR) technology that scans physical documents to move them into digital format, Automatic Number Plate Recognition (ANPR) utilizes the same technology to scan vehicle license plate characters into an image which is then converted to a digital text format that is usable within the digital domain.⁽¹⁸⁾ This allows the license plate character string to be easily queried in any database (such as stolen vehicle, insurance verification, and confirmation of owner data). If the vehicle license is known, it is relatively easy to obtain personal information about the vehicle owner.

This technology is utilized by law enforcement in speed and traffic monitoring as a proactive method of catching offenders. In traffic enforcement applications, the video camera is directly connected to a central server where the data pertaining to each offense are stored and the video image of the vehicle's license plate is converted to digital text characters. This allows law enforcement to query the vehicle databases for the owner's data so a hard copy of the offense paperwork can be sent to the vehicle owner. Additionally, by possessing a combination of vehicle and owner data, law enforcement agencies can delve deeper into any available databases regarding any outstanding warrants on the vehicle owner, his/her driving history, and other times and any other locations where the vehicle owner had been caught on a traffic enforcement camera.

The proactive law enforcement function is the current practice of videotaping the license plates of vehicles parked in publicly viewable locations.⁽¹⁸⁾ Currently, law enforcement officials may drive vehicles through parking structures equipped with video cameras positioned to record the plate numbers of the parked vehicles. The recording system is directly connected to the enforcement vehicle's onboard network connection where each number is recorded along with the associated data for the vehicle, its current location, and time. Once the data have been moved into the digital domain, they are is utilized in the same manner as data collected from traffic enforcement cameras. All available databases are queried for any outstanding traffic offenses or warrants, along with any criminal history.

If the databases show the owner of the vehicle to be a fugitive for any reason, law enforcement officials now have knowledge of the general location of the offender and an increased possibility of where he/she will be returning.

BIOMEDICAL IDENTIFICATION

Biomedical identification takes advantage of the inherent differences that make every human being unique.⁽¹⁹⁾ This not only includes basic physical characteristics such as body type and facial characteristics, but also items such as the pattern of an individual's iris, fingerprints, DNA, and chemical composition. Each of these characteristics, individually or in combination, can be used to identify and isolate an individual. While biomedical technology has not been used in many transportation safety applications, it is used more and more in security programs such as "Real ID" (used to deter illegal drivers' licensing) and in airport screening programs (as part of the U.S. Department of Homeland Security [DHS]). Information about this emerging technology has been included because of types of transportation applications that occur when traveling or applying for transportation licenses.

The oldest and most common form of bio-identification is fingerprinting. Fingerprints have the advantage of being a unique characteristic that changes very little throughout a person's life and can be collected in a non-invasive method. It is estimated that there is more than a billion-to-one chance of any two individuals sharing the same fingerprint pattern. Generally, fingerprint data are no longer collected utilizing ink and paper. Standard technology scans fingers and/or the whole hand and stores the data as an image file that can be digitally analyzed and compared to other images for a match. An advantage of this method is that personal data are collected and stored within the digital domain. As a digital file, it can be easily analyzed by software and is highly portable, so it can be transferred via the Internet to any location or storage facility anywhere in the world. For example, web-based fingerprint databases are used to identify every individual who transports hazardous materials. Similar identification processes are available for airport screening purposes.

A second method that is currently less common is Iris Biometric Recognition (IBR). This technology is similar to the current scanning technology used in fingerprint identification, the difference being that the iris of the individual's eye is scanned. Advocates of this technology claim that every individual's iris pattern is just as unique as fingerprints. This point has proven not to be entirely accurate over time. IBR technology is used infrequently in mobile personal identification, but the technology is constantly being refined and, like fingerprinting, is becoming part of the ambient technology in society.

The third type of biomedical technology is Facial Recognition. Like fingerprinting and IBR, Facial Recognition relies on the uniqueness of every human's facial characteristics. A video camera is employed to scan the individual's face, which is then analyzed by software for factors such as the spacing between the eyes, the overall shape, and the spacing between the prominent features of the human face. Each of the measurements is compared to an existing database of facial measurements, looking for an identification that matches. If none are found, the data are then stored and become part of the searchable data resource. Facial recognition has been suggested as a way to identify violations of High Occupancy Vehicle lanes and has become highly controversial in a number of court cases.⁽¹⁸⁾

An emerging biomedical technology is Whole Body Imaging (WBI), a technology that visually screens travelers to detect weapons, explosives, and other threat items. WBI is currently being used as a secondary screening procedure for airplane security. The technology is based on low intensity x-rays. Although recently introduced as a transportation technology, it is one of the more intense topics of privacy issues in the area of transportation security. Rep. Jason Chaffetz (R, Utah's third Congressional District), who sponsored a measure that would prohibit the use of WBI for primary screening, argued:

“...as a society, we're going to have to figure out the balance between personal privacy and the need to secure an aircraft. And there is no easy answer.”⁽²⁰⁾

If utilized separately, each of these technologies presents problems in finding an individual; but, when these technologies are used in combination, the accuracy increases to what is now considered acceptable levels. It is now current practice in airport pre-screening programs to combine facial recognition with fingerprinting to provide a definitive identification of a traveler.

GEO-POSITIONING AND ONBOARD TELEMETRIC COMMUNICATIONS SYSTEMS

Onboard telemetric and satellite communications systems are now almost considered a standard feature on many vehicles sold in the United States. The General Motors (GM) OnStar system is probably the best known.⁽²¹⁾ OnStar is a vehicle monitoring and communication system intended to be a driver safety and convenience feature. While the system is subscription-based (i.e., vehicle owners pay an annual fee for the service), owners are increasingly introduced to it in the sale of a vehicle equipped with the technology. Telemetric information is transmitted wirelessly to a satellite (in most cases), and then to a central control installation.

While these examples of technological applications in various transportation modes are impressive and have resulted in increased efficiencies in safety and security, the potential for abuse is ever present and continuing, as described later in this report.

CELL PHONE TRACKING

In an article written by Declan McCullagh, a contributor to CNET News and a correspondent for CBS News.com, McCullagh recounts how FBI agents used cell phone tracking to identify and eventually convict two men involved in multiple bank robberies.

“The way tracking works is simple: mobile phones are miniature radio transmitters and receivers. A cellular tower knows the general direction of a mobile phone (many cell sites have three antennas pointing in different directions), and if the phone is talking to multiple towers, triangulation yields a rough location fix. With this method, accuracy depends in part on the density of cell sites.”⁽²²⁾

Although not originally intended to be used as a tracking device, cell phone use can identify an individual’s location when cell phone calls were originated and received. Transportation agencies and consultants can, among other applications, use cell phone tracking to help manage traffic flow, predict travel times between two points, and do research on origins and destinations. According to Kevin Bankston, an attorney at the Electronic Frontier Foundation, who represents groups that have opposed a Justice Department position that Americans have no reasonable expectation of the privacy of cell phone locations:

“This is a critical question for privacy in the 21st century. If the courts do side with the government, that means that everywhere we go, in the real world and online, will be an open book to the government unprotected by the Fourth Amendment.”⁽²³⁾

POTENTIAL FOR ABUSE OF PERSONAL DATA ASSOCIATED WITH TRANSPORTATION SAFETY APPLICATIONS

We live in what has been described as the “Information Age.” Information is considered an invaluable commodity that is traded and sold by those who have the ability to collect it and those who want to use it to further their interests. Whether to enhance business opportunities, monitor the habits of employees, or identify potential terrorists, information is the lifeblood that makes

these endeavors function. The application of transportation technologies can provide a particularly rich source of useful information. Observing the transportation routine of an individual or a group provides information beyond simply where they are going and how they get there.

There are significant ways that transportation-related personal data can be abused. One way that is most likely to occur is gaining unauthorized access to data. The potential for this kind of abuse is especially high where wireless data collection methods are used. For example, according to Nate Lawson of Root Labs, several electronic toll systems were found to be “rife with privacy risks” in that strangers with the right transponder reader could steal the ID number off of toll transponders visible through the windshield of a parked car, put the data on their devices, and pass through tolls for free, with the victim paying the bill.⁽²⁴⁾

Italian researchers have discovered a way to hack into some wireless systems and potentially “own” the messages your car provides you. At risk are satellite-based navigation systems that use a Radio Data System-Traffic Message Channel (RDS-TMC) to receive traffic broadcasts and emergency messages in an insecure database; these can also be “hacked” and personal data stolen.⁽²⁵⁾

Another potential for abuse lies beyond the simple collection of information. Each type of abuse can be further interpreted in terms of analyzing and assessing risk. At the foundation of any discussion of personal privacy is our society’s recent desire to manage security risk. Both government and commercial interests oversee decisions and policy initiatives based on the amount of risk posed to the organization and/or the public at large. The DHS attempts to manage the risks associated with any individual or organization that might present a potential threat to the security of the United States. In the same manner, a health insurance company needs to manage the risks of insuring individuals who might result in a large payout for the company. The accuracy of either organization’s risk analysis is fundamentally dependent on the amount and the accuracy of the information it can obtain. The greater the amount and the better the quality of the information an organization has at its disposal, the better its chances are of arriving at the best decisions that minimize risks. This creates a potential situation where organizations seeking to minimize their risks might be willing to violate personal privacy in order to gain as much information as they can about the operating environment. This includes finding methods and sources of information that allow them to avoid any data and privacy-protection regulations. Many organizations are now employing a pre-emptive rather than a preventive approach to risk management.⁽²⁶⁾ A pre-emptive approach places emphasis on the screening and filtering of individuals, along with continuous surveillance of those who present the highest risk factors, as is becoming common for airline passenger screening. Managing this type of risk requires a continuing and complete knowledge that identifies individuals and situations that present the highest risk potential.

Additionally, information gathering is further enhanced by networking with other information-gathering entities such as the police, Internet providers, and even supermarkets to gain as much information as is available. This has resulted in the employment of a host of technologies and techniques (i.e., data mining, Internet searches, and networking with other organizations) designed to find available data.

Current levels of technology have provided anyone or any organization an almost unlimited ability to monitor an individual without that person having any idea of the surveillance. Software is now easily obtainable that will allow access to the federally mandated tracking feature incorporated in every cell phone to track the movements of the phone and the person who is carrying it.

A major factor contributing to the abuse of individual privacy is that the majority of individuals are not aware of the capabilities of current technology. Very few members of the general public are fully aware of the extent of the capabilities of technologies that are now being incorporated into new vehicles.⁽²⁵⁾ The technology is sold to the public, stressing its positive aspects, with little disclosure of other capabilities that might make it undesirable. An example of this type of marketing relates to emerging internal information systems. These systems are advertised throughout the media as a vital safety system that will monitor vehicle systems and, in the event of an accident, send help if the occupants are unable to do so themselves. What is omitted from the ads is that the same system is also monitoring information such as seatbelt usage, vehicle speed, and location. All of these data are being sent back to the information center for uses over which the vehicle owner has no control.⁽¹²⁾

Another emerging technology that presents opportunities for the abuse of privacy is the development of inter-vehicle *ad hoc* networking and smart roadway systems. *Ad hoc* networking is when computers communicate directly with each other without the use of any type of server. Applied to vehicle and transportation systems, it means that all vehicles traveling within a specific range could be in constant communication with each other's broadcasting information; e.g., traffic conditions, accident locations, and weather. Additionally, if the highway is a "smart road" and equipped with technology such as Connected Vehicle Systems, the same vehicles could be in constant communication with the highway's traffic management system, informing it of the vehicles' location, speed, and destination. These data would be analyzed by the highway's computer system, broadcast back to the vehicles, and made accessible via the Internet to aid travelers in planning their trip. While this type of system does present travelers with a number of improvements that would help streamline their travels and enhance safety, it also presents an almost unending potential for privacy abuses.

A significant potential security problem is presented by the *ad hoc* network itself. This type of network possesses much of the same security problems as does the Internet. Not only is the data stream subject to being received by unauthorized parties, but it can also allow those unauthorized parties to communicate back to the vehicles. This would present a hacker with almost unlimited possibilities to create havoc in the transportation system. Since the majority of vehicle systems (such as the radio, engine, and body management computers) are connected to the same system as the networking system (this is also true for the OnStar system), any hacker that could break into the system would have access to all of these vehicles' control systems. It is difficult to comprehend the disorder that would ensue if a hacker broke into a vehicle network and instructed the engine management systems to stop their motors, or simply started broadcasting erroneous information.

There have already been a number of recorded cases of smart sign systems being broken into and the verbiage changed.⁽²⁷⁾ While these cases have been nothing more than "college student" pranks, it does illustrate the vulnerabilities of these systems. In today's world, the Internet has

become an integral part of society. Not only do we depend on it for general day-to-day personal communications and information but many infrastructure systems rely on it to function and/or deliver services. However, with the new services comes a greater vulnerability to personal privacy.

Today it is accepted that computer anti-virus and/or anti-spyware protection is essential. The types of vehicles and roadway networks previously discussed face a similar situation. The development of those types of transportation networking systems could result in requiring all vehicles to have a form of network protection software onboard. This creates another type of problem common to web-browsing security: the constant battle between the hackers and the developers of security software. As the hackers develop new and more complicated methods of breaking into a network, the developers of security software are forced to develop more advanced systems to meet the new challenges. As a result, computer owners are forced to constantly update their network security software to ensure that their privacy is protected. The same would be true for vehicles that are members of any type of networking system. Not only would they need some form of security protection software, but it would have to be constantly kept up-to-date to ensure that the vehicle and highway systems are protected from any malicious accesses.

ABUSE THROUGH VEHICLE CLONING

One of the fastest growing vehicle crimes is “vehicle cloning”.⁽²⁸⁾ This occurs when a stolen vehicle’s Vehicle Identification Number (VIN) is changed by accessing its onboard vehicle control computer system. Since a VIN is the universally accepted identification, the vehicle’s original identity disappears and it acquires the identity and history of the vehicle with which it now shares the new VIN. This type of crime poses two possible problems for personal and vehicle information privacy. Since all VINs are associated with an owner, the VIN provides a direct path to the owner’s personal information such as address, insurance data, and driving record. A cloned vehicle will now provide a path to the owner of the vehicle with which it now shares its VIN. Combine this with any type of vehicle tracking system and the vehicle will now be identified as belonging to the owner of the other vehicle. This opens a variety of doors for criminal activities, from reselling the vehicle as a different vehicle to leading law enforcement to a different owner (if the vehicle is being tracked due to use in the commission of a crime).

Another concern relates to driver aids such as vehicle communications, infotainment, and vehicle systems-monitoring capabilities, considered essential by some drivers to the functionality of an automobile. These systems will not only provide a vehicle’s location through Global Positioning System (GPS) technology, they will also communicate with the vehicle’s manufacturer, informing it of mileage, engine condition, and any need for maintenance. Unknown to most drivers, however, is the fact that the same system also monitors seatbelt usage, vehicle speed and acceleration, tire pressure, and—in the event of an accident—vehicle deceleration and airbag deployment data. All of these data are available not only to the vehicle’s manufacturer but also to anybody who possesses the technology to receive and interpret the data stream being transmitted from the vehicle.⁽¹⁵⁾

Another wireless service is GM’s OnStar system. OnStar is a vehicle monitoring and communication system intended to be a driver safety and convenience feature. The system

allows drivers to communicate with a GM representative who can inform them of the health of their vehicle's various systems and, in the event of an accident, will alert OnStar of the vehicle's location so that rescue services can be sent.

OnStar monitors a wide variety of additional functions as well. These include:

- name, address, telephone number, email address, credit card number;
- VIN, make, model, year, date of purchase or lease, and selling/preferred dealer;
- license plate and the name and contact information of other drivers of the car and emergency contact information;
- diagnostic trouble codes; oil life; tire pressure; fuel economy; odometer readings; and, in specific circumstances, approximate speed data as calculated from GPS data; and
- collisions involving the car, safety belt usage, the direction from which the car was hit, and air bag deployment.⁽²⁹⁾

GM has a very detailed privacy information explanation on its website that describes the nature of the data, provides personal access to it, permits certain "opt-outs," and discusses the type of access it provides to others. However, the website also cautions OnStar users that wireless communications can be intercepted, placing personal information at risk.

The implications for transportation systems of this type are similar to those associated with security and privacy protection of personal data in general. Both commercial and government interests will have the opportunity to store personal data (such as vehicle tracking information, driver and owner data, and driving habits) in a location beyond the jurisdiction of any authority or personal protection regulations. In addition, the data will be out of the reach and control of the individuals on whom the data have been collected. This essentially allows both government and commercial interests to use the personal data collected without having checks on their usage or the outcomes.

The insurance industry is now employing the onboard vehicle tracking system on a large number of vehicles as a method of monitoring insured drivers' driving safety and habits. In return for lower premiums, drivers agree to have their driving monitored, and any actions that are interpreted by the insurance company as being unsafe or potentially dangerous will result in an increase in insurance premiums. While anything that results in improving driver safety is positive for the transportation system in general, this situation also presents an almost endless potential for abuse and misuse of driver data.⁽³⁰⁾

In our highly competitive economic environment, any information or data describing the market or customer base is highly valuable. The data regarding individuals' travel habits and the stores they frequent are valuable to everyone from the general business community to the drivers' Internet providers, as well as to their employers and a host of government agencies. For example, if the insurance company sells driver data to an Internet provider, the provider can now pass it along to advertisers who can use it to present the driver with "pop-up ads," targeting interests that are specific to the driver. Often cited in a humorous way, employers might be interested in driving data as a method of protecting themselves from an employee who frequents bars or liquor stores, which might indicate a substance abuse problem. Drivers are not given any option

to disable the monitoring functions of their vehicle. "For example, data collected in the airbag control module is entirely beyond the control of the driver and can be downloaded from the vehicle in the event the communications system malfunctions or is tampered with (i.e., in order to disable it)."⁽¹⁵⁾

In order to minimize the invasion and piracy of personal data, various efforts have been made during the years to standardize the collection and dissemination of information that could be argued to be "private." One organization participating in this effort is ITSA.

CREATION OF FAIR INFORMATION AND PRIVACY PRINCIPLES

ITSA was created in 1991 as a public/private partnership to advocate and act as a clearinghouse for the development and deployment of a wide range of intelligent transportation technologies. ITS applications may include any technology or device that has a transportation application and may be in the vehicle or infrastructure. Examples include wireless communications between vehicles and/or traffic control systems, collision avoidance systems, crash notification systems, red-light-running cameras, satellite tracking, electronic toll collections, and several emerging bio-information applications (including fingerprints, iris prints, facial recognition, and full body scanning). Along with its advocacy role, ITSA acted as a technical advisor to the U.S. Department of Transportation (USDOT) in the creation of regulations regarding the deployment and usage of intelligent transportation technology.

A critical component of ITSA's mission is to inform and advocate for the benefits that can be achieved by the adoption of intelligent transportation technology to interest groups, stakeholders, and government agencies. In 1997, this informational function was tasked to the ITSA general counsel.⁽³¹⁾ During the course of each presentation by the general counsel—and among the usual questions regarding costs, funding, and government involvement—was a question for which there appeared to be no acceptable answer; that is, What about privacy? Privacy questions usually took the form of: *Isn't this just big brother again?* or *What's to stop somebody using the information against me?* The common thread in all of these concerns was: Is this technology going to violate my privacy, and, if it is used, how can I protect myself?⁽³¹⁾

Moreover, concerns about privacy issues were being expressed by many other groups that had an interest in intelligent transportation technology. Private individuals and privacy advocacy groups expressed concerns that the technology had the obvious potential for misuse by private and government entities. "*What is the potential for the system tracking my vehicle and reporting any traffic violations to law enforcement agencies? If my vehicle is in constant communication with a network, what kind of data would be collected and who would have access?*"⁽³¹⁾ These were just a few of the concerns expressed by these groups. Commercial interests such as manufacturers and companies that would deploy the technologies were equally concerned. The primary concern was the potential for liability exposure, for instance, *Could they be legally held responsible for any violation of privacy?* The same was true for governmental agencies that saw not only the potential for privacy litigation but also interagency conflicts about the entity that would eventually be responsible for regulating the systems. All groups came to the conclusion that, while the technology had the potential to improve transportation safety, it was far outweighed by its potential for misuse and the invasion of privacy.⁽³¹⁾

All of these concerns and conclusions presented ITSA with a major problem. How could it advocate for technologies that were perceived by the public, commercial interests, and a host of government agencies as having the potential for doing more harm than good? As an organization charged with promoting new technology, how could it achieve its goals and yet answer the issues of the interest groups? As a consequence, ITSA formed a task force charged with investigating the issues and making recommendations about actions that would mitigate these privacy concerns.

CHAPTER 6. THE ITSA PRIVACY PRINCIPLES

In 1997, a privacy study task group was formed comprised of members representing ITSA, the relevant government agencies, and the various commercial entities involved with intelligent transportation technologies. Specialized expertise was provided by TRW (one of the world's largest automotive safety suppliers) that assigned a security and privacy expert from its data systems and credit reporting unit to the team. Additionally, TRW submitted to the group its internal corporate and public information privacy guidelines, "TRW Privacy Values," as a guide and starting point for what issues the task force needed to research.⁽³¹⁾

The increasing use of camera and video technology as a means of traffic enforcement was a major subject of discussion during the course of the task force operations, with questions posed such as: "*Should these types of technologies and traffic enforcement in general be included as a potential privacy issue?*" This issue had been a point of contention when ITSA was originally formed in 1991. At that time it was decided that ITSA was primarily concerned with traffic and congestion issues and that traffic engineers should not be dealing with law enforcement. On revisiting the issue, the task force came to a different conclusion. Since 1991 the usage of video cameras as a method of traffic law enforcement had become much more prominent, and presented jurisdictions using the technology with a very lucrative revenue source. However, the use of video cameras has proven not to be particularly popular. An article in the Missouri digital news pointed out: "photo enforcement has never survived a public vote."⁽²⁾

As part of dealing with traffic congestion issues, ITSA also promotes traffic safety. This provided the justification for including law enforcement technologies under the ITSA function of promoting traffic safety. An unexpected consequence of that decision was that ITSA was placed squarely in the middle of simultaneously promoting and attempting to manage the use of the technology by law enforcement. While the organization possessed an advanced degree of knowledge regarding the video and surveillance technologies, it knew little about the legal issues of police and enforcement work.

In 1998, the ITSA privacy task force submitted "*Fair Information and Privacy Principles*" for the approval of its board of directors. The principles were created as "non-binding" guidelines. Members were not forced to follow the principles but only to agree to take them into account in the development process of any new technology. By relegating the principles to only guideline status, ITSA created a situation where the interests of all the stakeholders were satisfied. While ITSA now had an answer when privacy concerns were voiced, it was also relieved from any responsibility of acting as an enforcement agency for its members. The same was true for its members. When any privacy issues were raised, they referred to the ITSA privacy guidelines as an acceptable method for answering questions about privacy issues. After completing its task, the ITSA privacy task force was dissolved, leaving the guidelines essentially dormant for the next nine years. No follow-up or revisiting actions were contemplated or scheduled during this time period.⁽³¹⁾

These fair information and privacy principles were prepared in recognition of the importance of upholding individual privacy while implementing the ITS. The principles are designed to be flexible and durable to accommodate a broad scope of technological, social, and cultural changes. These principles are advisory, intending to educate and guide transportation

professionals, policy makers, companies, organizations, and the public as they develop fair information and privacy guidelines for specific intelligent transportation projects. Initiators of ITS projects are urged to publish the fair information and privacy principles that they intend to follow. Parties to its systems are urged to include enforceable provisions for safeguarding privacy in their contracts and agreements.

APPLICATION AND IMPLEMENTATION OF THE FAIR INFORMATION AND PRIVACY PRINCIPLES

The ITSA survey of members was conducted to inform this research about each of the eight ITS categories within each of the 10 principles. The tables in the following pages are intended to measure in a qualitative sense the extent to which the ITSA members are “sensitive to and comply with” the principles.

The first part of this section examines the nature of the ITSA members’ involvement with the technology cited by respondents to the survey. The possible responses could be activities that manufacture, operate, research, deploy, or build technology, and whether the technology was for use in a vehicle, in the infrastructure, or in both. In each response, the project team focused on the total number of respondents to each question and, in some cases, the percentage of the respondents to a particular question is reported. The team is not suggesting that the responses are representative of all ITSA members; they represent the respondents’ answers to questions.

This section of the report also examines the way in which the responding ITSA members said that they apply the fair information and privacy principles. The data are from the membership survey and the technologies follow the ITS architecture categories of:

- ATMS
- MCO
- APTS
- ATIS
- CVO
- EM
- AD
- AVSS

Principle 1: Intelligent Transportation Systems Must Recognize and Respect the Individual's Interests in Privacy and Information Use

ITS technologies create value for both individuals and society as a whole. The primary focus of information is to improve travelers' safety and security, reduce travel times, enhance individuals' ability to deal with highway disruptions, and improve air quality. Traveler information is collected from many sources, some from the infrastructure and some from vehicles, while other information may come from transactions (such as electronic toll collections) that involve interaction between the infrastructure and vehicles, as shown in Table 3. Personal information may have value in both ITS and non-ITS applications. For an individual's interest in privacy to be respected, there must be disclosure with respect to the information collected, and the

individual must have the opportunity to express a preference as to whether or not personal identification is collected.⁽³²⁾

The type of information collected as a result of that principle was of interest in the survey for this project. Based on the information that was obtained, two-thirds of the survey respondents reported that they collect personal information of some type. Industries involved in ATMS are most likely, by far, to collect personal information. Moreover, of the types of personal information collected, a greater number were related to the make, model, year, and license plate number of the vehicle. Few asked for financial information or the debit or credit card number of the user.

Table 3. Types of information collected.

Personal Information				Vehicle Information				Financial Information			
Type of Personal Information	# Yes	# No	# of Respondents	Type of Vehicle Information	# Yes	# No	# of Respondents	Type of Financial Information	# Yes	# No	# of Respondents
Address	5	42		License Plate/State	14	32	46	Credit Card #	5	42	47
Driver's License #/State	1	45	46	Make	11	36	47	Debit Card	3	43	46
Email	9	40	49	Model	11	36	47	Bank Account	2	45	47
Fax	3	46	49	Color	11	35	46				
Medical Information	2	46	48	Year	8	38	46				
Name	9	40	49	# Axles	15	31	46				
Phone	10	39	49	# Tires	9	36	45				
Shipping Address	2	45	47	Vehicle Class	19	27	46				
Signature	2	45	47	Complete VIN	5	41	46				
				Partial VIN	3	42	45				
				Registration Name	1	43	44				
				HAZMAT Code	7	38	45				

Principle 2: Intelligent Transportation Systems will be Built in a Manner Visible to Individuals

Individuals should have a means of discovering what information is collected and how the data flows operate.⁽³⁴⁾ "Visible" means to disclose to the public the type of data collected, how it is collected, what its uses are, and how it will be distributed. The concept of visibility is one believed to be of central concern to the public; consequently, this principle requires assigning responsibility for disclosure.

According to the survey, most respondents who collect personal data report that it is collected in a manner that is visible to the individual. One-half of the 24 respondents report that they allow persons to opt in or opt out of the database. In addition, 19 of 20 respondents will remove personal information from their database on request. Left unaddressed is the fact that many of these systems collect vehicle data or financial data which does not permit an opt-out provision. Table 4 shows whether personal data are collected in a manner that is visible to individuals and Table 5 provides a summary of responses as to the nature of disclosure provided.

Table 4. Are ITS systems built in a manner "visible" to individuals?

ITS Function	# Responding	Yes Visible To Individuals	No Visible To Individuals
ATMS	26	21	5
MCO	26	12	14
APTS	26	10	16
ATIS	26	21	5
CVO	26	6	20
EM	26	17	9
AD	26	14	12
AVSS	26	4	22

Table 5. What types of disclosure do you make?

ITS Function	The type of data collected?	How data are collected?	The purpose for collecting the data?	How data are used?	How data are processed?	Who has access?	How data are stored?	How data are distributed?	How long the data are retained?
ATMS	18	18	18	16	13	13	14	15	14
MCO	10	10	10	8	8	7	8	8	8
APTS	8	9	9	9	7	6	6	6	6
ATIS	18	19	19	17	14	14	15	15	15
CVO	4	4	4	3	3	3	3	3	2
EM	14	15	15	13	10	10	11	11	12
AD	12	13	13	11	10	10	11	10	10
AVSS	4	4	4	4	4	2	2	2	2

Principle 3: Intelligent Transportation Systems Will Comply With Applicable State and Federal Laws Governing Privacy and Information.

Privacy law is a patchwork of federal and state statutes, as well as federal and state judicial opinions.⁽³⁴⁾ The “right” to privacy as a matter of law in the context of transportation on public roads and other facilities is limited. ITS applications should provide, at a minimum, privacy protections in conformity with the law of the respective jurisdictions. An extensive appendix reviewing each state’s privacy laws relevant to transportation concerns and applications is contained in Appendix A. Summary tables, shown earlier in Table 1 and Table 2, show that all states and the District of Columbia have constitutional restrictions on search and seizure, and 25 states have either an expressed provision in the state’s constitution or have an implied constitutional right that has been determined by the state’s highest court. Table 2 shows the number of states that also have common law torts regarding the invasion of privacy. The data displayed in Table 2 show that 40 or more states recognize the common law tort of the invasion of privacy, or one of its constituent components, which provides for a civil remedy in the courts for individuals who believe that their personal privacy has been violated. This is a significant number of states and it adds another legal argument for the protection of an individual’s right to privacy in addition to the statutory and court decision authority discussed herein.

Principle 4: Intelligent Transportation Systems will be secure.

ITS databases may contain information that is sensitive and personal. Information system providers should make use of data security technology and audit procedures appropriate to the sensitivity of the information. ITS applications should use technological and administrative safeguards to ensure that access to personally identifiable information is restricted to duly authorized individuals because the data have the potential to make it possible to know where individuals travel, what routes they take, and the duration of their travel.³⁴

The data collected and displayed in Table 6 and Table 7 below show that the number of respondents who secure data are determined by the ITS function. In two functions, MCO and AD, the numbers that do and do not secure the data are almost evenly split.

Table 6. Are data that the ITS collects secure?

ITS Function	# Responding	#Yes	#No
ATMS	40	34	6
MCO	40	18	22
APTS	40	14	26
ATIS	40	31	9
CVO	40	10	30
EM	40	26	14
AD	40	22	18
AVSS	40	8	32

Table 7. What technique or process do you use to ensure that data are secure?

Encryption	Passwords	Activity Logs	Check Sums for Alteration	Written Policies	Training Programs	Have Chief Privacy Officer
19	26	18	10	21	18	14

Principle 5: Intelligent Transportation Systems Have an Appropriate Role in Enhancing Travelers’ Safety and Security Interests, but Absent Consent, Statutory Authority, Appropriate Legal Process, or Emergency Circumstances as Defined by Law, Information Identifying Individuals Will not be Disclosed to Law Enforcement.

The ITS can increase the efficiency of traffic law enforcement by providing aggregate information necessary to target resources. States may legislate conditions under which ITS information will be made available to law enforcement agencies. Absent government authority, however, ITS applications should not be used as surveillance means for enforcing traffic laws, nor should the system be used as a tool for criminal investigation. Although individuals are concerned about public safety, persons who voluntarily participate in ITS programs or purchase ITS products should be informed regarding how they are used.⁽³⁴⁾

Table 8 shows the number of respondents who provide an opportunity to remove or correct personal information. States may legislate conditions under which information will be made available to law enforcement agencies. Absent government authority, however, ITS applications should not be used as surveillance means for enforcing traffic laws, nor should the system be used as a tool of criminal investigation. Although individuals are concerned about public safety, persons who voluntarily participate in ITS programs or purchase ITS products should be informed regarding how the information they are providing is used.

Table 8. Can people choose to be anonymous to those other than law enforcement officials?

ITS Function	Organization will Remove Personal Information		Allows Correction of Personal Information		Provides an Opportunity for Individuals to Opt Out		Develops Protocol, Internal Policies, or Procedures for Treatment of Personally Identifiable Information	
	Removes Personal Information	Gives Individuals a Choice	Yes	No	Yes	No	Yes	No
ATMS	13	7	7	14	9	10	7	12
MCO	8	3	5	8	6	5	6	5
APTS	10	5	4	6	7	2	3	6
ATIS	15	8	9	11	12	7	9	9
CVO	6	2	3	5	3	3	2	4
EM	14	7	8	8	9	5	8	7
AD	9	4	6	7	7	5	5	7
AVSS	5	3	1	4	3	0	0	3

Principle 6: Intelligent Transportation Systems will only Collect Personal Information that is Relevant for ITS Purposes.

Participating ITS organizations should collect personal information that contains individual identifiers that are needed for the ITS service function. Furthermore, information systems should include protocols that call for the purging of personal information that is no longer needed to meet ITS needs.⁽³⁴⁾ Respondents reported collecting more data related to the vehicle as compared to personal or financial data, as shown in Table 9.

Table 9. What kind of information is collected?

ITS Function	# Collecting Personal Information	# Collecting Vehicle Information	# Collecting Financial Data
ATMS	9	21	8
MCO	6	13	5
APTS	6	6	5
ATIS	13	19	8
CVO	4	9	4
EM	10	17	6
AD	8	11	4
AVSS	3	6	1

Principle 7: Where Practicable, Individuals Should Have the Ability to Utilize Intelligent Transportation Systems on an Anonymous Basis.

Certain ITS applications (for example, those used for CVO or "mayday") require personally identifiable information to function. Others (such as automated fee payments) may be designed to enable use by individuals without identifying themselves (through anonymous debit accounts) or with identifiers for convenience (e.g., credit cards). Unless a provision of identifiers is required by the ITS application, users should be provided with the opportunity to choose anonymity.⁽³⁴⁾

Table 10 demonstrates how an individual’s anonymity is thwarted; 14 out of 22 respondents (63.6 percent) indicated that they disclose changes in privacy policies. With one exception (EM), more respondents in each ITS function reported not giving individuals access to correct their personal data. Moreover, more respondents in each ITS function reported that they remove personal information rather than giving the individual the choice to do so. Interestingly, 47 out of 69 respondents (68 percent) skipped this question.

Table 10. How is anonymity preserved?

Security Mechanisms in Place to Prevent Tampering with Data and Preserving Anonymity			
Data encryption	Access control through passwords	Activity logs	Checks to detect alteration of data
16	20	13	7
9	14	9	5
7	11	7	3
14	21	15	9
7	8	5	3
13	18	12	7
7	17	10	5
4	5	2	3

Principle 8: Intelligent Transportation Systems Information, Stripped of Personal Identifiers, may be used for Non-ITS Applications.

American consumers want information to be useful for economic choice and value, but they also want their interest in privacy preserved. ITS information is often predictive of goods and services that interest consumers.⁽³⁴⁾ However, personally identifiable information collected by ITS surveillance technologies is extremely sensitive. Therefore, the following practices are encouraged by this principle:

- ITS information, absent personal identifiers, may be used for ITS and other purposes (see Table 11).
- Data collectors should ensure that ITS information provided to private organizations for secondary uses is stripped of personal identifiers.
- Individuals, however, may contract to allow use of personal identifiers for secondary use if full disclosure of the intended use is made and informed consent is obtained.

In determining whether to disclose ITS information, governments should, where possible, balance the individual's right to privacy against the preservation of the basic purpose of the Freedom of Information laws to open agency action to public scrutiny.

Table 11. How do ITS businesses handle disclosure of ITS data collection processes?

The Nature of the Non-ITS Purposes Included:	# of Respondents	Reason Request was Granted	Other Information on Requests Granted
Law Enforcement	25	Evidence	Of 41 Respondents, 17 had received requests and 9 had granted them. Six of the 9 were private entities.
Insurance Company	17		
Mobile Phone Company	7		
Government Planning Agencies	31	Planning	
Developers	16	Location of Facilities	
Research Units	24	University Research	
Market Research	19		
Fleet Operator	15	Use on Traffic Websites	
Private Investigators	13		
Others	9	Non-specified Use	

Principle 9: Federal and State Freedom of Information Act (FOIA) Obligations Require Disclosure of Information from Government Maintained Databases. Database Arrangements Should Balance the Individual's Interest in Privacy and the Public's Right to Know.

Travelers should not presume to have an expectation of privacy of personal information while traveling. Pursuant to the individual's interest in privacy, the principles of the Freedom of Information Act (FOIA) suggest that the database system should be structured to anticipate and resolve problems of access created by the FOIA.⁽³⁴⁾

As shown in Table 12, survey responses indicate that FOIA requests for data collected by ITS applications are not uncommon. Seven survey respondents reacted to a request for data from a public entity by court order or other form of request, and six respondents honored requests from private entities.

Table 12. How does your business comply with the Fair Information and Privacy Principles and structure them to comply with the FOIA?

ITS Function	Protocols For Collection, Use, Distribution, Retention, Disposal Of Personal Information		Have A Chief Privacy Officer		Has A Policy On Giving Or Selling Data	
	#Yes	#No	#Yes	#No	#Yes	#No
ATMS	7	12	12	21	20	13
MCO	6	5	7	12	13	4
APTS	3	6	2	11	7	6
ATIS	9	9	12	19	20	11
CVO	2	4	1	13	6	2
EM	8	7	8	6	16	8
AD	5	7	6	17	15	6
AVSS	0	3	1	5	5	2

Principle 10: Jurisdictions and Companies Deploying and Operating Intelligent Transportation Systems should have an Oversight Mechanism to Ensure that such Deployment and Operation Complies with their Fair Information and Privacy Principles.

Governments and companies should implement proper procedures to ensure that they protect the individual user's right to privacy and, at a minimum, to the extent outlined in these principles. This mechanism may include internal directives, the appointment of a privacy officer, and/or penalties for violations. Governments and companies should ensure that their ITS applications, while operating within their respective needs, also comply with the Fair Information and Privacy Principles.⁽³⁴⁾

As shown in Table 12 above, ITSA members have frequently developed policies or hired chief privacy officers to maintain regular oversight.

CHAPTER 7. CONCLUSIONS

Since the original adoption of the ITSA privacy guidelines in 1992, the privacy environment has changed dramatically. The attacks of 9/11 coupled with the development of new technologies have fundamentally changed the federal government's viewpoint on what is considered private. The new privacy environment now includes national and personal security interests and a reassessment of what information is considered necessary for the well-being of the nation as a whole.

Both the ITSA and its private sector members have used the guidelines as a method of bolstering their response to privacy concerns. As guidelines, however, they are self-regulatory and have no effective provision for enforcement. In reality, their principal effect is to create voluntary compliance to show that all parties are concerned with protecting privacy.

There is little doubt that protection of the privacy of personal information collected as part of transportation safety technology is gaining political attention. The fact that 13 states have banned the use of speed monitoring and red-light-running cameras does not bode well for much of the existing or emerging technology that collects personal information or for other technology from which private information can be derived. On the other hand, the technology industry appears to be generally sensitive to the concerns, although some practices do not comply with the ITSA privacy principles.

The survey of ITSA members did inform the study about the extent of compliance. Although a more specific follow-up survey is called for, there may be value in additional analysis of the survey responses. The collection of privacy laws on a state-by-state basis may offer access to questions regarding how states legislate privacy issues and how federal courts have interpreted the laws.

RECOMMENDATIONS

1. A number of recommendations are offered as a result of this work. Many of these recommendations must be undertaken by entities other than the Virginia Department of Transportation (VDOT), as noted below. As transportation safety technology has become more sophisticated, the protection of personal information continues to be a key factor in the development, installation, and operation of safety applications. Clearly, after more than a decade of change in technology and national security, the privacy principles should be revisited. **Although voluntary regulations are highly desirable from a business perspective, and most ITSA respondents appear to be aware of the privacy principles, some increased effort needs to be made by all concerned to encourage greater compliance.**

2. Concerns about the right to privacy regarding specific safety applications (e.g., cameras used for speed monitoring and red-light running) are growing to the point that many states are prohibiting their use. With the changing environment regarding homeland security, privacy issues and concerns have become a much larger part of the national discussion. **It is recommended that ITSA consider a program of public education about privacy protection if the safety applications they advocate, but citizens object to, are to be used for their intended purpose.**

3. The ITSA addressed privacy concerns with the adoption of the 10 privacy principles 18 years ago. The survey of ITSA members clearly indicates a “mixed bag” of privacy protection methods and attitudes. For the most part, the ITSA members who responded to the survey appeared sensitive to the need to protect personal information, but it should be noted that some did not fully comply with them. Whether the principles are extensive enough to ensure that personal information cannot be obtained or derived from emerging safety applications—especially in light of the ubiquities of newer, more intrusive technology—should be considered in the review process. This survey looked at member responses in an aggregate form. **ITSA should consider a follow-up survey to determine the extent to which member organizations are sensitive to the privacy principles and the extent to which each individual organization complies with them.**

4. Unquestionably, in the deployment of transportation technology to achieve transportation safety, privacy is increasingly subjected to outside forces; including those related to homeland security, political philosophy, and both domestic and international events. Consider, for example, the highly controversial impact of full body scanning on airplane passenger clearance, which was an immediate result of a terrorist’s unsuccessful attempt to bring down a major airline by hiding explosives in his underclothing. **In order to achieve safety, security, and mobility, ITSA needs to revisit the privacy principles as new and emerging technologies become more intrusive on personal privacy.**

5. The protection of one’s personal information is as much a responsibility of each individual as it is the responsibility of the transportation industry. In order to protect against potential abuses, several options can be suggested. **For example, it is advisable and recommended that individuals consider using separate bank accounts or credit cards for toll transactions, thereby limiting abuse of personal information to gain illegal access to financial data and to resist identity theft. Furthermore, in the event that individuals have concerns about the data collected from them, they need to take personal responsibility to understand the privacy safeguards that are available.**

6. Developments such as the EDR statutes that place greater legal restrictions on open road surveillance technology can be viewed as further indicators of the sensitivity surrounding the collection of personal information as the result of an individual’s decision to travel. Whether these statutes and regulations are extensive enough to protect personal privacy remains an open question, one that will be debated in the face of improving technological advances. The growing numbers of states that have adopted “black box” legislation and the emergence of federal regulations similar to the states’ protections reflect an increasing level of importance and awareness that the public is attaching to the protection of their privacy interests. **If EDR data continue to be available to insurance companies and civil litigants, state legislatures may wish to consider legislation to further define the legitimate reasons for access to data recorded in motor vehicles.**

7. There are a variety of ways to invade the personal privacy of a traveler on the open road, through the use of devices other than existing transportation safety applications. For example, existing privacy protections through the use of the ITSA principles do not apply to cell phone tracking. **It is recommended that consideration of such symbiotic relationships of**

external technology applications and transportation safety applications needs to be taken into account in the future by ITS manufacturers and transportation decision-makers.

8. The objective of providing a safe and efficient transportation system inherent to transportation agency purposes may not be the same as the objectives of others who wish to use transportation facilities and transportation applications for their diverse purposes. **It is recommended that each state transportation agency should take issues of personal privacy protection into account when considering use of highway rights-of-way for traffic safety, security, or traffic management purposes as well as other public or private purposes.**

REFERENCES

- (1) Sadofsky, D. *The Question of Privacy in Public Policy: An Analysis of the Reagan-Bush Era*. Praeger, New York, 1993.
- (2) Missouri Digital News, February 18, 2009, <http://www.mdn.org/2009/stories/redlight.htm>. (Accessed 01/30/2010)
- (3) Dotzer, F, Privacy Issues in Vehicular Ad Hoc Networks. Rep. Munich Germany, BMW Group Research and Technology, 2006, Print.
- (4) Privacy, Wikipedia, the Free Encyclopedia, The Wikimedia Foundation, Inc., <http://en.wikipedia.org/wiki/Privacy>, (Accessed 02/23/2010)
- (5) TheNewspaper.com, A journal of the politics of driving, <http://www.safespeedlafayette.com>. (Accessed 01/30/2010)
- (6) Glancy, Dorothy J. "Privacy on the Open Road", 30 *Ohio Northern University Law Review* 295, (2004). http://law.scu.edu/site/dorothy-glancy/File/open_road.pdf. (Accessed, 06/15/2009)
- (7) 199-206, 210-13 (1990) with Laurence H. Tribe, Constitutional Choices 12-13 (1985).
- (8) Katz v. United States, 389 U.S. 347 (1967)
- (9) United States v. Miller 425 U.S. 435 (1976).
- (10) Whalen vs. Roe, 429 U.S. at 605-06.
- (11) Federal Trade Commission, <http://www.ftc.gov/reports/privacy3/fairinfo.shtm>. (02/14/2010)
- (12) Oregon. Rev. Stat Ann. §105.935 (2009)
- (13) Wright, David. "The Dark Side of Ambient Intelligence." *The Journal of Policy, Regulation and Strategy for Telecommunications* 7.6 (2005): 33-51. Print.
- (14) CCTV Boom Has Failed to Slash Crime, Say Police, *The Guardian*, June 26, 2008, <http://www.guardian.co.uk/uk/2008/May/06/ukcrime1>.
- (15) Interview, Gene Hetherington, This discussion is based on the co-author's 6 years of experience working in the Ford Safety section. His experience dealt extensively with this technology. (12/08/2008)
- (16) Is Your Vehicle Spying On You, *Communication*, November 2005, <http://www.globalsecurity.org/security/library/news/2005/08/sec-050805-rferl03.htm>.

- (17) National Traffic Safety Administration. (2005). "Red Light Camera Operational Guidelines", Publication No. FHWA-SA-05-002. Washington, DC: U.S. Government Printing Office.
- (18) APR, Kiralyhago ter 8-9., 1126 Budapest, Hungary, <http://www.anpr.net>. (Accessed 02/15/2010)
- (19) Bio-Identification-New Biometric Technologies Enhance Security and Add Convenience to Daily Life, Dr. Baldev Krishan, President of Shimon Systems Inc. http://englishnovmexico.com/biometric_article.pdf.
- (20) Rep. Jason Chaffetz, Utah, <http://www.anpr.net/Newsweek, January 11, 2010, p.35>. (Accessed 02/20/2010)
- (21) Adapted from OnStar web site: <http://www.onstar.com>. (Accessed 02/10/2010)
- (22) Declan McCullagh, Feds Push for Tracking Cell Phones, CNET News, http://news.cnet.com/8301-13578_3-10451518-38.html (Assessed 02/10/2010)
- (23) (Kevin Bankston, as cited in McCullagh), Feds Push for Tracking Cell Phones, CNET News, http://news.cnet.com/8301-13578_3-10451518-38.html (Accessed 02/10/2010)
- (24) Nate Lawson, Hacking Electronic Toll Systems, CNET News, <http://news.cnet.com/8301-10093-10009-83.html>. (Accessed 02/10/2010)
- (25) Goodin, Dan. "Satnav hacking made simple." *The Register*. 27 Apr. 2007. Web. 12 Jan. 2010. http://www.theregister.co.uk/2007/04/20/satnav_hack/. (Accessed 02/10/2010)
- (26) Wood, David M., and Kirstie Ball, Eds. *A Report on the Surveillance Society*. Rep. Surveillance Studies Network. Print.
- (27) Daniel Terdiman, Hacking programmable road signs, cnet news, http://news.cnet.com/830113772_3-10149229-52.html. (Accessed 02/10/2010)
- (28) Attack of the Clones: Identity Theft Hits the Road, USA Today, http://www.usatoday.com/news/nation/2005-05-19-clone-inside_x.htm. (Accessed 10/20/2009)
- (29) Adapted from OnStar web site: <http://www.onstar.com>. (Accessed 02/10/2010)
- (30) Big Brother Can Save You Money, CNN on Line, 7/13/2008, http://money.cnn.com/autos/gmac_onstar_insurance. (Accessed 10/09/2009)
- (31) Interview, Craig Roberts, Former General Council ITSA, November 9, 2008.
- (32) ITS America's Fair Information and Privacy Principles, www.itsa.org/itsa/files/ITSAFairinformation Privacy.doc. (Accessed 12-2008)

APPENDIX A. THE LEGAL ISSUES

This appendix contains the relevant statutory law references for each of the 50 states and the District of Columbia and Federal Circuit Court decisions for each of the 11 Federal Circuits and the District of Columbia.

The following subject areas were reviewed:

- Computer Crimes
- Credit Reporting
- Electronic Transactions
- Mandatory Government Redaction of Personal Information
- Third Party Disclosure of Personal Data
- Commercial Use of Public Records
- Consumer Finance
- Drug & Alcohol Testing (Employee Privacy)
- Freedom of Information
- Non-governmental Surveillance
- Employee Privacy
- Electronic Surveillance
- Motor Vehicle Registration
- Constitutional Provisions on Privacy and Electronic Surveillance
- Holder in Due Course State Statutes
- State Equal Credit Opportunity Statutes

State Privacy Laws

[Alabama](#) [Alaska](#) [Arizona](#) [Arkansas](#) [California](#) [Colorado](#) [Connecticut](#) [Delaware](#)
[District of Columbia](#) [Florida](#) [Georgia](#) [Hawaii](#) [Idaho](#) [Illinois](#) [Indiana](#) [Iowa](#) [Kansas](#)
[Kentucky](#) [Louisiana](#) [Maine](#) [Maryland](#) [Massachusetts](#) [Michigan](#) [Minnesota](#) [Mississippi](#)
[Missouri](#) [Montana](#) [Nebraska](#) [Nevada](#) [New Hampshire](#) [New Jersey](#) [New Mexico](#)
[New York](#) [North Carolina](#) [North Dakota](#) [Ohio](#) [Oklahoma](#) [Oregon](#) [Pennsylvania](#)
[Rhode Island](#) [South Carolina](#) [South Dakota](#) [Tennessee](#) [Texas](#) [Utah](#) [Vermont](#) [Virginia](#)
[Washington](#) [West Virginia](#) [Wisconsin](#) [Wyoming](#)

[State Laws Summary Matrix](#)

[Event Data Recorder Update](#)

(Contains an update on 13 state EDR statutes as of December 2009.)

Federal Circuit Court Decisions

[1st Circuit Court](#) [2nd Circuit Court](#) [3rd Circuit Court](#) [4th Circuit Court](#) [5th Circuit Court](#)
[6th Circuit Court](#) [7th Circuit Court](#) [8th Circuit Court](#) [9th Circuit Court](#) [10th Circuit Court](#)
[11th Circuit Court](#) [District of Columbia Circuit Court](#)

Federal Privacy Laws

[Federal Circuit Court](#) [Federal Privacy Law](#)

APPENDIX B. ITSA MEMBER SURVEY

This appendix contains the data from the ITSA survey used in the tables throughout the report. Part 1 shows that, in developing informative tables, the responses to several questions were combined to create a more complete response. Part 2 contains the raw survey sent to the ITSA members. Part 3 contains a summary of the raw survey responses. Part 4 contains open-ended responses to the related questions.

[Part 1 – Sources of Information for Tables](#)

[Part 2 – ITSA Survey](#)

[Part 3 – ITSA Survey Response Summary](#)

[Part 4 – Survey Comments](#)

APPENDIX C. BIBLIOGRAPHIC ANNOTATION OF SELECTED WORKS CITED

Bohn, Jurgen, Coroama, Vlad, Langheinrich, Marc and Friedemann Mattern. "Living In A World of Smart Everyday Objects-Social, Economic, and Ethical Implications." *Human and Ecological Risk Assessment* 10 (2004): 763-85. Print.

The authors of this article present a discussion of current and future computer technologies that are incorporated into general objects, turning them into what is now labeled smart objects. One of the major contributors to this is that hardware is continually getting smaller with each new generation. This allows it to be incorporated in an increasing number of objects and services. But as everyday objects get smarter, the amount of data they collect also increases. The authors use this as a framework to analyze the privacy implications for society. Concepts such as "Privacy as Empowerment" and "Privacy as a Regulating Agent" are cited as areas where surveillance from smart objects could intersect with personal privacy issues. While this article doesn't directly address transportation issues, the general adoption of intelligent transportation technology would allow it to be categorized as a smart everyday object. This brings the discussions within this article within the scope of this study.

Casal, Carlos R. "Privacy Within In-Car Systems." *The Journal of Policy, Regulation and Strategy for Communication* 7.1 (2005): 66-75. Print.

Intelligent in-car systems such as GM's OnStar, are now commonly included in vehicles sold in the U.S. The author discusses the capabilities of these systems and the hidden threats to personal privacy that they present to drivers. Integral to his discussion is how, currently, there is no universally accepted definition of privacy and the popular concept has changed with the development of new technology and society. This article contributes another general source describing current vehicle technology and how it intersects with personal privacy.

Dotzer, Florian. *Privacy Issues in Vehicular Ad Hoc Networks*. Rep. Munich Germany: BMW Group Research and Technology, 2006. Print.

This article specifically addresses the privacy issues related to ad hoc vehicle networking. This type of technology is being proposed as a method of relaying information about traffic congestion, weather and road conditions, and any accidents to all vehicles on and entering a highway. The author cites that before any moves to generally adopt this technology, any privacy issues must first be dealt with. To address these issues, Florian describes several proposed technologies that will protect the vehicle and its passengers from being identified as it travels and any data collected from having any value beyond the road system. Since the author is working for one of the automobile manufacturers it does illustrate that the industry realizes the privacy implications of intelligent transportation technology. It also provides a collection of proposed solutions that might allow its adoption but still protect privacy.

Hewitt, Daniel J. "Don't Accept Rides from Strangers: The Supreme Court Hastens The Demise of Passenger Privacy In American Automobiles." *The Journal of Criminal Law & Criminology* 90.3 (2000): 875-915. Print.

This article is a comprehensive analysis of the U.S. Supreme Court's ruling in *Wyoming v. Houghton*, 119 S. Ct. 1297 (1999). While the ruling specifically dealt with search and seizure of

a private vehicle, it also created a precedent on what is considered private in a vehicle being operated on a public highway. The legal concepts discussed are fundamental to what type of access intelligent transportation technology and those who employ it can have to a vehicle, its operator, and its passengers. Any limitations the court implements will also dictate what types of technology can be deployed on a public highway.

Laberge, Gaetan. *Radiofrequency Identification Technology (RFID): Is There Reason To Mistrust It?* Rep. Direction de l'analyse et de l'évaluation, 2006. Print.

This article presents a technical, social and legal discussion of Radiofrequency Identification Technology (RFID). The author opens the article by defining RFID technology and describing a number of typical ways it is currently utilized. Within the transportation sector, Laberge cites the proposals to incorporate RFID technology as an identification method into driver's licenses and vehicles. But along with potential benefits, the article describes a number of current objections that consumer and privacy groups have expressed about RFID technology. The relevance of this article is that it presents another discussion and analysis of a technology that is integral to intelligent transportation systems.

Wood, David M., and Kirstie Ball, eds. *A Report on the Surveillance Society*. Rep. Surveillance Studies Network. Print.

This report presents an in-depth analysis of how new and emerging technologies might affect the current and future privacy environment. It takes a two-track approach by combining a discussion and analysis of each technology with a continuous narrative of a story that illustrates the potential effects it could have on the lives of a typical English family. While this report goes far beyond transportation issues, it does address them along with presenting concepts relevant to any discussion of privacy.

Wright, David. "The Dark Side of Ambient Intelligence." *The Journal of Policy, Regulation and Strategy for Telecommunications* 7.6 (2005): 33-51. Print.

The concept of ambient intelligence is one of the newest terms used to describe intelligent objects throughout society. It describes the new collection of intelligent objects that keep it working, but function totally in the background out of the mainstream consciousness. While many perceive this new class of objects as enhancing society, Wright takes the view that, along with the benefits, these objects present a collection of undesirable attributes that must be taken into account. The relevance to this study is his discussion of how many of these objects include surveillance and tracking capability that would fit into any implementation of any intelligent transportation technology.

LEGAL FILES

ALABAMA PRIVACY LAW

- **State Constitutional Privacy Rights**
 - none
- **Search and Seizure**
 - ALA. CONST. art. I, § 5 (2009) Unreasonable search and seizure; search warrants. That the people shall be secure in their persons, houses, papers, and possessions from unreasonable seizure or searches, and that no warrants shall issue to search any place or to seize any person or thing without probable cause, supported by oath or affirmation.
 - **Auto Exception**
 - Reid v. State, 388 So. 2d 208 (Ala. 1980) - recognized the automobile exception in accordance to Supreme Court precedent. There was little difference between an immediate search without a warrant and the vehicle's immobilization until a warrant was obtained. Because the toolbox was affixed to the body of the vehicle, the court applied the automobile exception in determining the reasonableness of the search. Given probable cause to search, either seizing or holding a vehicle before presenting the probable cause to a magistrate, or carrying out an immediate search without a warrant, was reasonable under the Fourth Amendment.
 - **Open Fields**
 - Doggett v. State, 791 So. 2d 1043 (Ala. Crim. App. 2000) the 'search' for and discovery of the contraband occurred from the airplane and before any law enforcement officer set foot on Tidwell's property. The officers could legitimately 'search' the open fields without violating any Fourth Amendment rights.
 - **Plain View**
 - Seeley v. State, 669 So. 2d 214 (Ala. 1995) - Under the "plain view" doctrine, if the police are lawfully in a position from which they can view an object, if the incriminating character of the object is immediately apparent, and if the officers have a lawful right to access to the object, then they may seize it without a warrant.
- **Statutory Privacy Rights**
 - ALA. CODE § 13A-6-90 (2009) - A person who intentionally and repeatedly follows or harasses another person and who makes a credible threat, either expressed or implied, with the intent to place that person in reasonable fear of death or serious bodily harm is guilty of the crime of stalking.
- **Individually Identifiable Government Records**
 - ALA. CODE § 41-13-6 (2009) Government must take steps to redact social security numbers from all public records, but the provisions of this section shall not be applicable to a document originating with any court or taxing authority, any document that when filed by law constitutes a consensual or nonconsensual lien or security lien or security interest, or any record of judgment, conviction, eviction, or bankruptcy.

- **Public Records**
- ALA. CODE § 36-12-40 (2009) - Rights of citizens to inspect and copy public writings, except as otherwise provided.
 - ALA. CODE § 41-13-23 (2009) - Preservation of government records, commission has the responsibility of determine which records will be permanently preserved.
 - ALA. CODE §§ 22-9A-21 through 22-9A-28 (2009) - Inspection of Records. Prohibits vital statistics records from being viewed by anyone except for registrant, a member of his or her immediate family, his or her guardian, and their respective legal representatives. A vital record is defined as data derived from certificates and reports of birth, death, fetal death, induced terminations of pregnancy, marriage, divorce, and related reports. However, the State Registrar may permit the use of data from vital records for statistical or legitimate research purposes, subject to conditions he or she may impose. No data shall be furnished from records for legitimate research purposes until the State Registrar has received in writing an agreement signed by a responsible agent of the research organization agreeing to conform to the conditions.
 - ALA. CODE § 38-1-4 (2009) - Reports of Recipients of Public Welfare. Reports filed with a probate judge are open for public inspection, but there is no disclosure of any records of the county department of human resources pertaining to adoptions or the placement of foster children. In addition, the records cannot not be disclosed for any other reason than public assistance.
 - ALA. CODE § 8-1A-1 through -20 (2009) - Uniform Electronic Transactions Act. Allows electronic transactions and signatures but requires control processes and procedures as appropriate to ensure adequate preservation, disposition, integrity, security, confidentiality, and auditability of electronic records
- **Motor Vehicle Records**
 - ALA. CODE § 32-7A-9 and -11 (2009) - The department will suspend registration for any person not carrying insurance or using falsified insurance. Upon a violation, the owner's name and identifying information shall be provided to the director by the department, for the purpose of requiring the owner to purchase and maintain insurance.
 - ALA. CODE § 32-8-45 (2009) - Every dealer shall maintain for five years a record in the form the department prescribes of every vehicle bought, sold or exchanged by him or received by him for sale or exchange, which shall be open to inspection by representatives of the department and law-enforcement officers during reasonable business hours.
 - ALA. CODE § 32-8-65. Freedom of information. A lienholder named in a certificate of title shall, upon written request of the owner or of another lienholder named on the certificate, disclose any pertinent information as to his security agreement and the indebtedness secured by it.
- **Vehicle Identification Numbers**
 - ALA. CODE § 32-8-8 (2009). Investigations by law enforcement officials. Any sheriff, deputy sheriff, policeman of an incorporated municipality or duly authorized representative of the Department of Public Safety or Department of Revenue of this state may enter into the premises of any automobile salvage dealer, junkyard, automobile or other motor vehicle dealer licensed therefore by

the State of Alabama or any political subdivision thereof and inspect the identification numbers of all motor vehicles or parts thereof contained on said premises

- ALA. CODE § 32-8-37 (2009) - Uniform Certificate of Title and Anti-theft Act. The dept must check the VIN shown on an application for certificate of title against a list of stolen or converted vehicles.
- ALA. CODE § 32-8-37 (2009) - Each certificate of title shall contain a description of the vehicle including the VIN.
- ALA. CODE § 32-8-86 (2009). Identification numbers. A person who willfully removes or falsifies an identification number of a vehicle, engine, transmission or other identifiable component part of a vehicle is guilty of a Class A misdemeanor and shall be punished as required by law.
- **Consumer Credit**
 - ALA. CODE §§ 13A-8-190 through -201 (2009) The Consumer Identity Protection Act. Deals with ramifications of identity theft.
 - If a consumer submits to a consumer reporting agency a court order as described in Section 13A-8-198, the consumer reporting agency shall, within 30 days of receipt, employ reasonable procedures to block reporting any information in the consumer's credit report identified in the court order that is the result of a criminal violation of the Consumer Identity Protection Act so that the information cannot be reported and, at the consumer's request, include the fact of the order in the consumer's credit report.
 - In any case in which a person obtains identification documents or identifying information of another person in violation of this article and uses the documents or information to commit a crime in the name of another person, the court records for the crime shall reflect that the victim of this act did not commit the crime.
- **Financial Records**
 - ALA. CODE § 5-5A-43 (2009). Disclosure of customer records. A bank shall disclose financial records of its customers pursuant to a lawful subpoena, summons, warrant or court order issued by or at the request of any state agency, political subdivision, instrumentality, or officer or employee thereof and served upon the bank. No bank, director, officer, employee or agent thereof shall be held civilly or criminally responsible for disclosure of financial records pursuant to a subpoena, summons, warrant or court order which on its face appears to have been issued upon lawful authority.
 - ALA. CODE § 30-3-192 (2009) - Alabama Child Support Act of 1997. The state Title IV-D agency may disclose financial records only for the purpose of and to the extent necessary in establishing, modifying, or enforcing a child or spousal support obligation of an individual. No liability shall arise to the state Title IV-D agency or any of its employees from any disclosure which results from a good faith but erroneous attempt to comply with this section.
 - Note: State Title IV-D agency. The state agency designated to administer the statewide child support program authorized under Title IV-D of the Social Security Act.

- ALA. CODE § 36-25-1 (2009) - must disclose financial records for candidacy.
- **Employee Privacy**
 - Martin v. State, 2003 WL 21246587 (Ala. Crim. App. 2003), *aff'd in part, rev'd in part on other grounds*, 2004 WL 2829051 (Ala. 2004), *cert. denied*, 2006 WL 690675 (U.S. 2006) (unpublished opinion; applying the Fourth Amendment) - employees must establish both that he or she had an actual subjective expectation of privacy in the place searched and that this subjective expectation of privacy is one that society is prepared to recognize as reasonable.
 - In this case, Martin had no expectation of privacy in a footlocker he kept in the patrol car issued to him during his employment as a state trooper, and thus no standing to challenge a search of the footlocker under the Fourth Amendment, where, when the officer resigned his commission as a state trooper, he left the footlocker and its contents in the vehicle, which he returned to his state trooper post. Court would not suppress the evidence found in the footlocker.
 - ALA. CODE § 25-5-330 through -340 (2009) Drug-Free Workplace. Employers are permitted to test employees as long as some notice is given the first time the procedures are instituted or if notified as a condition of employment.
 - All information, interviews, reports, statements, memoranda, and test results, written or otherwise, received by the employer through a substance abuse testing program are confidential communications, but may be used or received in evidence, obtained in discovery, or disclosed in any civil or administrative proceeding, except in criminal proceedings.
 - ALA. CODE § 16-22A-10 (2009) Criminal Background checks of Education Applicants. Any criminal history background information reports received by the State Department of Education from the Department of Public Safety shall be confidential, conspicuously marked as confidential, and not further disclosed or made available for public inspection. Criminal history background information reports are specifically excluded from any requirement of public disclosure as a public record as the Legislature finds these documents to be sensitive personnel records.
- **Electronic Surveillance**
 - ALA. CODE § 13A-11-31 (2009) - Criminal eavesdropping. A person commits the crime of criminal eavesdropping if he intentionally uses any device to eavesdrop, whether or not he is present at the time.
 - ALA. CODE § 13A-11-32 (2009) - Criminal surveillance. A person commits the crime of criminal surveillance if he intentionally engages in surveillance while trespassing in a private place.
 - ALA. CODE § 13A-11-33 (2009) - Installing eavesdropping device
 - ALA. CODE § 13A-11-34 (2009) - Criminal possession of eavesdropping device
 - ALA. CODE § 13A-11-35 (2009) - Divulging illegally obtained information
 - ALA. CODE § 13A-11-36 (2009) - Exceptions. Law enforcement, employment as a communication carrier, believed to be following the law.
 - ALA. CODE § 13A-11-37 (2009) Forfeiture of eavesdropping device to law enforcement or other appropriate department if illegally held.

- **Computer Statutes**

- ALA. CODE § 13A-8-100 through -103 (2009) Alabama Computer Crime Act. A person who willfully, knowingly and without authorization attempts to access or accesses a computer or computer device commits an offense against intellectual property.
- ALA. CODE § 41-10-390 (2009). Alabama Supercomputer Authority Act. The privacy, security and confidentiality of data collected, stored, processed or disseminated by the supercomputer system under the provisions of this article are the responsibility of the person, organization or entity collecting, storing, processing or disseminating such data. Data collected, stored, processed or disseminated through utilization of the supercomputer system under the provisions of this article are not subject to the requirements of the public record laws of the State of Alabama, and are therefore not subject to public disclosure by the authority. Requires the owner's permission to disclose any info.
 - The supercomputer system has the primary purpose of providing state-of-the-art technology in supercomputer processing for scientific research and development to governmental agencies, educational institutions, private-sector businesses and industries.

- **Common Law**

- Butler v. Town of Argo, 871 So. 2d 1 (Ala. 2003) - It is generally accepted that invasion of privacy consists of four limited and distinct wrongs: (1) intruding into the plaintiff's physical solitude or seclusion; (2) giving publicity to private information about the plaintiff that violates ordinary decency; (3) putting the plaintiff in a false, but not necessarily defamatory, position in the public eye; or (4) appropriating some element of the plaintiff's personality for a commercial use.

ALASKA PRIVACY LAW

- **State Constitutional Privacy Rights**
 - **Express**
 - ALASKA CONST. art. I, § 22 (2009) - The right of the people to privacy is recognized and shall not be infringed. The legislature shall implement this section.
 - **Implied**
 - ALASKA CONST. art. I, § 1 (2009) - This constitution is dedicated to the principles that all persons have a natural right to life, liberty, the pursuit of happiness, and the enjoyment of the rewards of their own industry
 - ALASKA CONST. art. I, § 14 (2009) - The right of the people to be secure in their persons, houses and other property, papers, and effects, against unreasonable searches and seizures, shall not be violated.
- **Search and Seizure**
 - Cowles v. State, 23 P.3d 1168 (Alaska 2001) - Federal and State Constitutions prohibit not only unreasonable physical searches, but also unreasonable technological searches, and thus, placing a hidden video camera in a house in order to record activities there without a warrant is prohibited just as is a warrantless entry to search for evidence; however, not all technological monitoring of places or individuals is regarded as a search for constitutional purposes.
 - General test used to determine whether particular technological monitoring is a search is the expectation of privacy test, and under this test, courts ask whether person harbored an actual subjective expectation of privacy, and, if so, whether that expectation is one that society is prepared to recognize as reasonable.
 - ALASKA STAT. § 16.05.180 (2009) - Power to search without a warrant. Authorizes peace officers and other authorized employees of the Department of Fish and Game to conduct searches without a warrant when investigating potential fish and game violations. However, the statute requires the officers conducting the warrantless searches to first provide written notice to the person in control of the property.
 - The notice requirement of ALASKA STAT. § 16.05.180 does not apply if a defendant has no constitutionally protected expectation of privacy in the area searched, or if the warrantless search is justified under another exception to the warrant requirement.
 - **Auto Exception**
 - State v. Daniel, 589 P.2d 408 (Alaska 1979) - recognized the automobile exception, but made sure to limit it in accordance with the constitutional provisions. In short, we embrace the observation that "the word "automobile" is not a talisman in whose presence the Fourth Amendment fades away and disappears." We think that protection of the interiors of closed luggage, briefcases, containers and packages transported in a vehicle reflects fundamental expectations of privacy which Alaska society would recognize as reasonable. Alaska seems to rely on the plain view doctrine for these cases.

- Daygee v. State, 514 P.2d 1159 (Alaska 1973) - recognized the automobile exception where a plastic bag of marijuana was observed by officers in an automobile, but noted that the latitude given to automobile searches had been reined in by the Court in recent years.
- **Open Fields**
 - Ingram v. State, 703 P.2d 415 (Alaska 1985) - a tool shed that housed refuse and other discarded items is not public, open area that may be searched without a warrant.
 - Woods & Rohde, Inc. v. State, 565 P.2d 138 (Alaska 1977) - referencing the open fields exception but not explicitly deciding the case on its merits.
- **Plain View**
 - State v. Beltz, 160 P.3d 154 (Alaska Ct. App. 2007) - There are four factors relevant to the question of whether society is prepared to recognize a reasonable expectation of privacy in trash: (1) where the trash was located; (2) whether the dwelling consisted of multiple units or a single unit; (3) who removed the trash; and (4) where the search of the trash took place.
 - At one end of the continuum is trash located close to a single-family dwelling, on the same property as the dwelling, and searched by police officers at that location. This would be a strong case for holding the expectation of privacy to be reasonable.
 - At the other end of the continuum is trash located off the premises of a multiple-unit dwelling, and searched by a person authorized to remove it. In such a case a court would be unable to hold that the expectation of privacy was reasonable.
 - Pearce v. State, 45 P.3d 679 (Alaska Ct. App. 2002) - recognizing the plain view doctrine, but declining to reach the issue because Pearce did not even have a subjective expectation of privacy in the seized item.
 - Guidry v. State, 671 P.2d 277 (Alaska 1983) - In order for there to be a reasonable seizure under the plain view doctrine, the initial presence must be lawful.
 - Anderson v. State, 555 P.2d 251 (Alaska 1976) - recognizing the plain view doctrine, but noting that in all of the precedent cases, the incriminating quality of the item subsequently seized was readily apparent and required no movement of either the observer or the observed object to detect.
 - State v. Spietz, 531 P.2d 521 (Alaska 1975) - Police officers were not authorized to enter the house and remove the marijuana plants they observed through an open doorway. Plainview just gives them probable cause to obtain a warrant to search the house, but does not give them the right to enter and seize evidence. Considers the home a more sacred location.
 - Daygee v. State, 514 P.2d 1159 (Alaska 1973) - recognized the plain view doctrine where a plastic bag of marijuana was observed by officers in an automobile.

- Erickson v. State 507 P.2d 508 (Alaska 1973) - held that marijuana which had been removed by officers from a suitcase could not be held to have been in plain view, hence, a violative search occurred.
 - Pope v. State, 478 P.2d 801 (Alaska 1970) - recognized the plain view doctrine where a gun was observed by officers on the seat of an automobile.
 - **Statutory Privacy Rights**
 - Personal Information Protection Act, ALASKA STAT. §§ 45.48.010 through 45.48.995 (2009) - All of the Act goes into effect July 1, 2009. It has seven parts in total, four of which specifically deal with personal privacy issues that pertain to ITS:
 - Breach of Security Involving Personal Information - ALASKA STAT. §§ 45.48.010 through 45.48.095. If a covered entity has a breach of security that discloses personal information about a state resident, that entity must inform the individual without delay.
 - Protection of Social Security Number - ALASKA STAT. §§ 45.48.400 through 45.48.480. Not allowed to disclose to third parties, some exception for transfer of the number interagency
 - Disposal of Records - ALASKA STAT. §§ 45.48.500 through 45.48.590. Speaks to the due diligence of limited access during and after the disposal of records containing personal information.
 - Truncation of Credit Card Information - ALASKA STAT. § 45.48.750. A person who accepts credit cards or debit cards for the transaction of business may not print more than the last four digits of the card number or the expiration date on any receipt or other physical record of the sale.
 - ALASKA STAT. §§ 11.41.260 & 11.41.270 (2009) - Stalking in the first and second degree. A person commits the crime of stalking if the person knowingly engages in a course of conduct that recklessly places another person in fear of death or physical injury, or in fear of the death or physical injury of a family member. Includes contacting the victim by telephone or electronic mediums. The difference between first and second degree includes using a deadly weapon and/or contacting a person under the age of 16.
 - **Individually Identifiable Government Records**
 - ALASKA STAT. § 40.25.300 (2009) - Personal information in state public records. Requiring written notices when a state agency requests or changes personal information in a public record.
 - ALASKA STAT. § 40.25.310 (2009) - allows a person to challenge the accuracy and completeness of their personal information in a state public record. This section does not apply to criminal intelligence or criminal investigative records, criminal justice information under § 12.62, state agency personnel or retirement system records, records of applicants for employment with the state agency.
 - ALASKA STAT. § 09.80.150 (2009) - Uniform Electronic Transactions Act - Acceptance and distribution of electronic records by governmental agencies.
 - To the extent that a governmental agency uses electronic records and electronic signatures under (a) of this section, the governmental agency, giving due consideration to security, may specify control processes and

procedures as appropriate to ensure adequate preservation, disposition, integrity, security, confidentiality, and auditability of electronic records.

- **Public Records**
 - ALASKA STAT. § 40.25.110 (2009) - Unless specifically provided otherwise, the public records of all public agencies are open to inspection by the public under reasonable rules during regular office hours.
 - ALASKA STAT. § 40.25.120 (2009) - exceptions to inspections for public records including: vital statistics, medical records, compiled for law enforcement purposes, names and addresses of certain persons, state safety or security information, trade secrets.
 - ALASKA STAT. § 40.25.140 (2009) - library records are confidential
 - ALASKA STAT. § 40.25.151 (2009) - certain records of the state retirement system are confidential.
- **Motor Vehicle Records**
 - ALASKA STAT. § 28.10.505 (2009) - Disclosure of personal information contained in motor vehicle records. General prohibition for disclosing personal information contained in motor vehicle records. Some exceptions for vehicle theft or driver safety and for use in research activities, or in producing statistical reports, if the personal information is not published, redisclosed, or used to contact an individual.
 - ALASKA STAT. § 28.05.061 (2009) - The Department of Administration shall file, maintain, and appropriately index motor vehicle records, stolen vehicles, driver's licenses. Motor vehicle records must be furnished to child services if requested.
 - ALASKA STAT. § 28.35.031 (2009) - anyone who is operating a motor vehicle in the state is said to have consented to drug and alcohol testing
- **Vehicle Identification Numbers**
 - ALASKA STAT. § 28.10.071 (2009) - Records shall be maintained by a distinctive registration number assigned to the vehicle, by the vehicle identification number, including but not limited to a record of identification numbers replaced or assigned under AS 28.10.061, by the name and residence and mailing address of the owner. The department may compile a record of the number and types of vehicles registered in this state and may make statistical data available to the public for a fee as prescribed in regulations adopted by the commissioner. The department may also provide vehicle registration lists to the public for a fee as an electronic service or product
- **Consumer Credit**
 - ALASKA STAT. § 21.36.165 (2009) - Anticoercion and antitying [for Insurance Trade Practices and Frauds] - a person must use separate documents for an insurance transaction, other than credit insurance or flood insurance, and for a credit transaction; and maintain separate and distinct records relating to insurance transactions, including consumer complaint information, and make the records available to the director for inspection upon notice.
 - ALASKA STAT. § 21.36.460 (2009) - Uses of and restrictions on credit history or insurance scoring applicable to personal insurance.
 - An insurer must: inform the consumer that the consumer has the right to correct errors in the credit report;

- An insurer must not cancel or deny insurance coverage if the absence of credit history or the inability to determine the consumer's credit history if the insurer has received accurate and complete information from the consumer; OR using credit inquiries not initiated by the consumer.
 - ALASKA STAT. § 06.60.330 (2009) - Compliance with federal requirements for mortgage loan activities includes complying with Consumer Credit Protection Act, 15 U.S.C. 1601.
 - ALASKA ADMIN. CODE tit. 18, § 78.529 (2009) - Confidentiality of loan information. The following information is considered confidential and is not subject to public disclosure unless ordered by a court: financial information, including income tax returns, financial statements, business income statements, pro forma profit and loss statements, credit information obtained directly from banks and other creditors, and reports from consumer credit reporting agencies.
- **Financial Records**
 - ALASKA STAT. § 06.01.025 (2009) - Information in the records of the department obtained through the administration of this title [Banks and Financial Institutions] is confidential, is not subject to subpoena, and may be revealed only with the consent of the department.
 - ALASKA STAT. § 06.01.028 (2009) - The records of financial institutions relating to their depositors and customers and the information in the records are confidential. A financial institution may not disclose the records and information to another person except for limited exceptions.
 - ALASKA STAT. § 06.26.610 (2009) - The trust company records relating to customers are confidential and may not be made public but for some limited exceptions.
 - ALASKA ADMIN. CODE tit. 18, § 78.529 (2009) - Confidentiality of loan information. The following information is considered confidential and is not subject to public disclosure unless ordered by a court: financial information, including income tax returns, financial statements, business income statements, pro forma profit and loss statements, credit information obtained directly from banks and other creditors, and reports from consumer credit reporting agencies
 - ALASKA ADMIN.CODE tit. 3, §§ 26.605 through 26.749 (2009) - Privacy of Consumer Financial and Health Information. Provides regulations for opt out, notice requirements and third party disclosure of private information.
- **Employee Privacy**
 - ALASKA STAT. § 23.10.037 (2009) - employers may not require employees to take polygraph tests as a condition of employment.
 - ALASKA STAT. § 18.80.220 - makes it unlawful for employers to inquire into such topics (like , religion, color, national origin, age, sex, marital status, changes in marital status, pregnancy, or parenthood) in connection with prospective employment. This statute demonstrates that in Alaska certain subjects are placed outside the consideration of employers in their relations with employees.
 - ALASKA STAT. § 23.10.600 through 699(2009) - employee drug testing rules and requirements. Results are to be kept confidential and may only be disclosed to the tested employee, anyone the employer designated to interpret the results and discuss with the employee, or by court order.

- ALASKA STAT. § 23.10.430 (2009) - Access to personnel files. An employer shall permit an employee or former employee to inspect and make copies of the employee's personnel file and other personnel information.
- ALASKA ADMIN. CODE tit. 2, § 37.177 (2009) - The administrator will release information regarding personal or financial data on employees or former employees [of the Judicial, Elected Public Officers, And National Guard/Naval Militia Retirement Systems] in accordance with policies promulgated by the administrator. The administrator will release information on an employee or former employee to that individual, to the individual's employer or former employer, and to state agencies authorized to secure that information, or by court order.
- Cowles v. State, 23 P.3d 1168 (Alaska 2001) - employees must establish an actual subjective expectation of privacy in the place searched and that this subjective expectation of privacy is one that society is prepared to recognize as reasonable. Defendant, who was manager of box office for university, did not have reasonable expectation of privacy with respect to hidden video surveillance which recorded her in the act of theft.
 - When an individual enters into an employment situation with high security requirements, it becomes less reasonable for her to assume that her conduct on the job will be treated as private for Fourth Amendment purposes.
 - What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.
- Luedtke v. Nabors Alaska Drilling, 768 P.2d 1123 (Alaska 1989)
 - Alaska law clearly evidences strong support for the public interest in employee privacy. First, state statutes support the policy that there are private sectors of employees' lives not subject to direct scrutiny by their employers.
 - There is a sphere of activity in every person's life that is closed to scrutiny by others. The boundaries of that sphere are determined by balancing a person's right to privacy against other public policies, such as the health, safety, rights, and privileges of others. The court permitted an employer to test an employee for drug and alcohol use if the testing was done in accordance with good faith and fair dealing.
- Woods & Rohde, Inc. v. State, 565 P.2d 138 (Alaska 1977)
 - Interpreting ALASKA STAT. § 18.60.083(a) (Alaska's Occupational Safety and Health Act provides, as to the right of entry and inspection) and concluding that the Alaska Constitution prohibits warrantless administrative inspections of the business premises of respondents.
- **Electronic Surveillance**
 - ALASKA STAT. § 09.65.215 (2009) Immunity of peace officer for use of body wire eavesdropping device. Not liable for damages if the peace officer took appropriate steps to use the device (was part of the communication or did not record it) and did so for the right reasons (investigating crime)
 - ALASKA STAT. § 12.37.010 Authorization to intercept communications. Attorney General or his designee may apply to a court to intercept communications if there

- is evidence the person they wish to intercept plans to or has committed murder, kidnapping or a class A felony.
- ALASKA STAT. § 12.37.020 Application for order authorizing a communication interception.
 - ALASKA STAT. § 12.37.030 Requirements for an order authorizing a communications interception.
 - ALASKA STAT. § 12.37.040 Contents of order authorizing a communications interception; limitations on disclosure.
 - ALASKA STAT. § 12.37.050 Privileged communications. An otherwise privileged communication intercepted in accordance with, or in violation of, the provisions of AS 12.37.010 -- 12.37.130 does not lose its privileged character by reason of the interception.
 - ALASKA STAT. § 12.37.060 Collateral authority of court; interpretation of 12.37.010--12.37.130
 - ALASKA STAT. § 12.37.070 Records and recordings and custody of them. Will be sealed by the court who ordered the interception.
 - ALASKA STAT. § 12.37.080 Custody of applications and orders; penalty for disclosure.
 - ALASKA STAT. § 12.37.090 Notice of interception and disclosure. Within 90 days (there can be extensions however) the person who was intercepted needs to be informed of this fact.
 - ALASKA STAT. § 12.37.100 Approval for unanticipated interception. If a peace officer intercepts a communication that relates to a felony offense other than one specified in the order of authorization, the attorney general, or a person designated in writing or by law to act for the attorney general, may file a motion for an order approving that interception so that the communication, or evidence derived from it, may be used during testimony in an official proceeding.
 - A court may enter an order approving the interception if it finds that the person who intercepted the communication was otherwise acting appropriately under the original order.
 - ALASKA STAT. § 12.37.110 (2009) - to use the intercepted material all parties need to be informed within 10 days of the use.
 - ALASKA STAT. § 42.20.300 Unauthorized publication or use of communications
 - Except for a party to a private conversation, a person who receives or assists in receiving, or who transmits or assists in transmitting, a private communication may not divulge or publish the existence, contents, substance, purport, effect, or meaning of the communication, except through authorized channels of transmission or reception (lawful purposes).
 - ALASKA STAT. § 42.20.310 Eavesdropping - an eavesdropping device may not be used to hear or record an oral conversation unless at least one party to the communication consents.
 - ALASKA STAT. § 42.20.320 Exemptions. Public conversations that are overheard advertently are an exemption from this section.

- ALASKA STAT. § 42.20.325 Duty to report anyone who knows of someone who is violating the unauthorized publication or eavesdropping provisions must report this to the proper authorities.
- ALASKA STAT. § 42.20.330 Penalty for disclosure
- ALASKA STAT. § 42.20.390 Definitions.
 - (3) "eavesdropping device" means a device or apparatus, including an induction coil, that can be used to intercept an oral, wire, or electronic communication
 - (4) "electronic communication" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photo-optical system, including a cellular or cordless telephone communication, but does not include:
 - (A) wire or oral communications; (B) communications made through a tone-only paging device; (C) communications made through a tracking device consisting of an electronic or mechanical device that permits the tracking of the movement of a person or object; or (D) communications that are disseminated by the sender with the intent or expectation, or through a method of transmission that is so configured, that the communication is readily accessible to the general public;
- **Computer Statutes**
 - ALASKA STAT. § 11.46.740 (2009) - Criminal use of computer. Carries a penalty of a Class C felony if an individual accesses a computer, computer system, computer program, or computer network, to obtain information about a person or introduce false information or encrypt or decrypt information about a person.
 - ALASKA STAT. § 11.46.200 (2009) - Theft of Services. Commits theft if a person obtains the use of computer time, a computer system, a computer program, a computer network, or any part of a computer system or network, with reckless disregard that the use by that person is unauthorized.
- **Common Law**
 - **Appropriation**
 - Luedtke v. Nabors Alaska Drilling, 768 P.2d 1123 (Alaska 1989) - recognizing appropriation branch of the invasion of privacy.
 - **Disclosure**
 - Falcon v. Alaska Pub. Offices Comm'n, 570 P.2d 469 (Alaska 1977) - recognizing the tort of public disclosure of sensitive information as an invasion of privacy, but not finding evidence of the tort in this particular case where general information that certain persons visited a doctor was disclosed.
 - **False Light**
 - State v. Carpenter, 171 P.3d 41 (Alaska 2007) - An action for false light invasion of privacy differs from an action for defamation because a defamation claim redresses damage to reputation while a false light privacy claim redresses mental distress from exposure to public view. Like defamation liability, however, false light liability requires at least knowing

or reckless disregard of the falsity of the assertion of fact. Because opinions cannot be proved false, they cannot give rise to false light liability.

○ **Intrusion**

- Greywolf v. Carroll, 151 P.3d 1234 (Alaska 2007) - Alaska law recognizes the claim for invasion of privacy based on the Restatement (Second) of Torts § 652B, which reads: “One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.”

ARIZONA PRIVACY LAW

- **State Constitutional Privacy Rights**
 - **Express**
 - ARIZ. CONST. art. II, § 8 (2008) - No person shall be disturbed in his private affairs, or his home invaded, without authority of law.
 - **Implied**
 - Malmin v. State, 246 P. 248 (Ariz. 1926) - The right to privacy under the Arizona Constitution has the same effect and purpose as the Fourth Amendment to the United States Constitution.
- **Search and Seizure**
 - State v. Superior Court, 691 P.2d 1073 (Ariz. 1984) - Roadblocks to check for DWI are constitutional because of the gravity of public concern, compelling state interest in deterring drunk drivers, and the minimal intrusion to drivers imposed by the stops.
 - State ex rel. Ekstrom v. Justice Court, 663 P.2d 992 (Ariz. 1983) - The court determined that the intrusions generated by the state's intrusion were not minimal because of the lack of inspection guidelines provided, and the stops were unreasonable because the state's stipulation indicated an adequate alternative method of enforcing the drunk driving statute and no pressing need for using an intrusive roadblock.
 - State v. White, 574 P.2d 840 (Ariz. Ct. App. 1977) - Illegally seized evidence is admissible when seized by a non-government agent who is not acting in concert with police.
 - **Auto Exception**
 - State v. Dean, 76 P.3d 429 (Ariz. 2003) - Recognizing the "automobile" exception to the warrant requirement of the Fourth Amendment. Under that exception, searches of vehicles may be allowed absent a warrant if the police have "probable cause" to do so, but finding that the officer did not have probable cause in this particular case.
 - When a policeman has made a lawful custodial arrest of the occupant of an automobile, he may, as a contemporaneous incident of that arrest, search the passenger compartment of that automobile and any containers found within the passenger compartment.
 - **Open Fields**
 - State v. Caldwell, 512 P.2d 863 (Ariz. Ct. App. 1973). The court held that the boxes of marijuana were not protected by the Fourth Amendment because they were found in an open field, where there was no expectation of privacy.
 - **Plain View**
 - Mazen v. Seidel, 940 P.2d 923 (Ariz. 1997) Once the privacy of the residence has been lawfully invaded, it is senseless to require a warrant for others to enter and complete what those already on the scene would be justified in doing. We hold that where firefighters have lawfully discovered evidence of criminal activity under the plain view doctrine, it is not necessary for sheriff's officers to obtain a warrant before entering a residence to seize the evidence.

- **Statutory Privacy Rights**

- ARIZ. REV. STAT. ANN. § 13-2923 (2008) - person commits stalking if the person intentionally or knowingly engages in a course of conduct that is directed toward another person and if that conduct either: 1. Would cause a reasonable person to fear for the person's safety or the safety of that person's immediate family member and that person in fact fears for their safety or the safety of that person's immediate family member. 2. Would cause a reasonable person to fear death of that person or that person's immediate family member and that person in fact fears death of that person or that person's immediate family member.
- ARIZ. REV. STAT. ANN. § 13-3002 (2008) - False or forged messages; classification. Knowingly to send to any person by telegraph or telephone a false or forged message, purporting to be from a telegraph or telephone office, or from any other person. With intent to deceive, defraud or injure.
- ARIZ. REV. STAT. ANN. § 13-3003 (2008) - Opening, reading or publishing sealed letter of another without authority; classification
- ARIZ. REV. STAT. ANN. § 13-3004 (2008) Sending threatening or anonymous letter; classification is prohibited.
- ARIZ. REV. STAT. ANN. § 13-3019 (2008) - Surreptitious photographing, videotaping, filming or digitally recording or viewing; exemptions; classification; definitions. It is unlawful for any person to knowingly photograph, videotape, film, digitally record or by any other means secretly view, with or without a device, another person without that person's consent if the content includes nudity or other very personal images. Security purposes is acceptable use of recording devices, as long as there is notice if the recording is in a place where the person has a reasonable expectation of privacy.

- **Individually Identifiable Records**

- ARIZ. REV. STAT. ANN. § 41-1750 (2008) - criminal history information collected by the Central State Repository is confidential.
- ARIZ. REV. STAT. ANN. § 36-665 (2008) - health information regarding communicable diseases is confidential and may not be released, but for some exceptions including a compelling need for disclosure of the information for the adjudication of a criminal, civil or administrative proceeding.
- ARIZ. REV. STAT. ANN. § 8-121 (2008). Confidentiality of information between adoptive and birth parents shall remain confidential except upon agreement between the two or if the person requesting the information provides a compelling reason for the disclosure.
- ARIZ. REV. STAT. ANN. § 44-1373 (2008). Confidentiality Of Personal Identifying Information. Restricted use of personal identifying information. No person or entity may intentionally communicate or otherwise make an individual's social security number available to the general public or require the transmission of the number without taking proper encryption precautions.
- ARIZ. REV. STAT. ANN. § 11-484 (2008). Records maintained by county assessor and county treasurer; redaction; Notwithstanding any other provision of this article, in any county an eligible person may request that the general public be prohibited from accessing that person's residential address and telephone number

that are contained in instruments, writings and information maintained by the county assessor and the county treasurer.

- ARIZ. REV. STAT. ANN. § 11-461 (2008) Social Security Numbers - on or before January 1, 2009, the recorder in a county with a population of more than eight hundred thousand persons, shall redact references to complete nine digit social security numbers that are available on the recorder's website. Social security numbers may be retained on instruments that are not available on a website.

- **Public Records**

- ARIZ. REV. STAT. ANN. § 39-121 (2008). Inspection of public records. Public records and other matters in the custody of any officer shall be open to inspection by any person at all times during office hours.
- ARIZ. REV. STAT. ANN. § 39-121.03 (2008) - Exceptions. Public records can be used for commercial purposes as long as the individual wanting the records fully explains the purpose and this is deemed acceptable by the record custodian.
- ARIZ. REV. STAT. ANN. § 39-123 (2008). Information identifying eligible persons; confidentiality. Nothing in this chapter requires disclosure from a personnel file by a law enforcement agency or employing state or local governmental entity of the home address or home telephone number of eligible persons. But this information can be released with the permission of the person named in the record.
- ARIZ. REV. STAT. ANN. § 39-128 (2008). Disciplinary records of public officers and employees. A public body shall maintain all records that are reasonably necessary or appropriate to maintain an accurate knowledge of disciplinary actions, including the employee responses to all disciplinary actions, involving public officers or employees of the public body. The records shall be open to inspection and copying pursuant to this article, unless inspection or disclosure of the records or information in the records is contrary to law.
- ARIZ. REV. STAT. ANN. § 22-9A-21 (2008) Vital Statistics. To protect the integrity of vital records, to insure their proper use, and to insure the efficient and proper administration of the system of vital statistics, it shall be unlawful for any person to permit inspection of, or to disclose information contained in vital records, or to copy or issue a copy of all or part of any record, except as authorized by this chapter and by rules of the board or by order of a court of competent jurisdiction. The person who is named in the record or his guardian or representative may review these records.
- ARIZ. REV. STAT. ANN. § 22-9A-26 (2008) unlawful to request these vital statistics records if unauthorized.
- Carlson v. Pima County, 687 P.2d 1242 (1984) Despite the unlimited disclosure expressed by the wording of Ariz. Rev. Stat. § 39-121, the availability of records for public inspection is not without qualification. There are numerous statutory exemptions to the general "open access" policy toward public records.

- **Motor Vehicle Records**

- ARIZ. REV. STAT. ANN. § 28-447. Public records. An application for a license, permit, title or registration made to the department and a document required by law or by the department to accompany the application is a public record, except a medical report and a report voluntarily submitted by a physician or a registered

nurse practitioner as defined in section 28-3005, except as provided by section 28-455 and except as otherwise provided by law.

- ARIZ. REV. STAT. ANN. § 28-454 (2008). Records maintained by department of transportation. Notwithstanding sections 28-447 and 28-455, an eligible person may request that persons be prohibited from accessing the person's residential address and telephone number contained in any record maintained by the department.
 - “Eligible person” means a peace officer, justice, judge, commissioner, public defender, prosecutor, code enforcement officer, adult or juvenile corrections officer, corrections support staff member, probation officer, member of the board of executive clemency, law enforcement support staff member, national guard member who is acting in support of a law enforcement agency, person who is protected under an order of protection or injunction against harassment or firefighter who is assigned to the Arizona counterterrorism center in the department of public safety.
- ARIZ. REV. STAT. ANN. § 28-455 (2008). The department shall disclose personal information for use in connection with the following matters: 1. Motor vehicle or driver safety and theft; 2. Motor vehicle emissions; 3. Motor vehicle product alterations, recalls or advisories; 4. Performance monitoring of motor vehicles and dealers by motor vehicle manufacturers; 5. Removal of nonowner records from the original owner records of motor vehicle manufacturers. Otherwise this information may not be disclosed.
- ARIZ. REV. STAT. ANN. § 28-456 (2008). Subsequent sale or disclosure of record information by authorized recipient. An authorized recipient of personal information may resell or redisclose the information only for a use permitted under section 28-455, subsection B or C.
- ARIZ. REV. STAT. ANN. § 28-667 (2008) - Written Accident reports are public records, except, shall not allow a person to examine the accident report or any related investigation report or a reproduction of the accident report or a related investigation report if the request is for a commercial solicitation purpose.
- **Vehicle Identification Numbers**
 - ARIZ. REV. STAT. ANN. § 28-4846 (2008). Stolen vehicles; inspection; violation; classification A. For the purposes of enforcing this title or locating stolen vehicles or parts of those vehicles, peace officers may: 1. Inspect a vehicle to examine any vehicle identification number, serial number or other unique distinguishing number, sign or symbol in any public garage, vehicle storage, repair, leasing or rental lot or facility, vehicle equipment rental yard, vehicle salvage pool or other similar establishment. 2. Inspect the title or registration of those vehicles in order to establish their rightful ownership or possession. B. Peace officers may also inspect a bicycle, an implement of husbandry, special construction equipment and a motor vehicle designed for off-highway use that is on the premises described in Subsection A or if such a vehicle is incidentally operated or transported on a highway.
 - State v. Renfrow, 597 P.2d 546 (Ariz Ct. App. 1979) Car door can be opened to inspect VIN by police if there is reasonable suspicion.
- **Consumer Credit**

- ARIZ. REV. STAT. ANN. § 44-7501 (2008) - Notification for Compromised Personal Information. When a person that conducts business in this state and that owns or licenses unencrypted computerized data that includes personal information becomes aware of an incident of unauthorized acquisition and access to unencrypted or unredacted computerized data that includes an individual's personal information, the person shall conduct a reasonable investigation to promptly determine if there has been a breach of the security system BUT A person is not required to disclose a breach of the security of the system if the person or a law enforcement agency, after a reasonable investigation, determines that a breach of the security of the system has not occurred or is not reasonably likely to occur.
- ARIZ. REV. STAT. ANN. § 44-1692 (2008) Permissible use of consumer reports.
 - A. Except as provided in section 44-1693, a consumer reporting agency may furnish a consumer report only under the following circumstances and no other:
 1. In response to the order of a court having jurisdiction to issue such an order.
 2. In accordance with the written instructions of the consumer to whom it relates.
 3. To a person that it has reason to believe: (a) Intends to use the information in connection with a credit transaction involving the consumer on whom the information is to be furnished and involving the extension of credit to, or review or collection of an account of, the consumer. (b) Intends to use the information for employment purposes. (c) Intends to use the information in connection with the underwriting of insurance involving the consumer. (d) Intends to use the information in connection with a determination of the consumer's eligibility for any license or other benefit granted by a governmental instrumentality required by law to consider an applicant's financial responsibility or status. (e) Otherwise has a legitimate business need for the information in connection with a business transaction involving the consumer.
- ARIZ. REV. STAT. ANN. § 44-1696 (2008) Unlawful acts. Anyone who falsely requests a credit report commits a misdemeanor.
- ARIZ. REV. STAT. ANN. § 44-1698.01 (2008). Consumer credit reports; extension of credit. An entity extending credit must take reasonable steps to verify the identity of requesting the individual.
- **Financial Records**
 - ARIZ. REV. STAT. ANN. § 25-523 (2008) - Family Support Duties. The department shall enter into agreements with financial institutions that conduct business in this state to develop and operate a data match system to assist the department in the establishment, modification and enforcement of child support orders. The data match system shall use automated data exchange procedures to the maximum extent possible. Data exchanges between financial institutions and the department shall occur quarterly and shall include the name, record address, social security number or other taxpayer identification number and any other identifying information for each obligor who maintains an account at the institution and who owes past due support as identified by the department by name and social security number or other taxpayer identification number.
 - ARIZ. REV. STAT. ANN. § 6-129 (2008) - Records; disclosure and limitations on disclosure; evidentiary effect. Except as otherwise provided by this title, the

records of the department relating to financial institutions shall not be public documents nor shall they be open for inspection by the public and neither the superintendent nor any member of the superintendent's staff shall disclose any information obtained in the discharge of official duties to any person not connected with the department. Exceptions include: federal insurers of accounts, attorney general, etc.

- **Employee Privacy**

- ARIZ. REV. STAT. ANN. § 23-493 through 493.11 (2008) - All communications received by an employer relevant to drug test or alcohol impairment test results and received through the employer's testing program are confidential communications and may not be used or received in evidence, obtained in discovery or disclosed in any public or private proceeding, except in a proceeding related to an action taken by an employer or employee under this article.

- **Electronic Surveillance**

- ARIZ. REV. STAT. ANN. § 13-3001 (2008) "Electronic communication" means any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature that is transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system but that does not include any of the following: (a) Any wire or oral communication. (b) Any communication made through a tone-only paging device. (c) Any communication from a tracking device.
- ARIZ. REV. STAT. ANN. § 13-3005 (2008) - Interception of wire, electronic and oral communications; installation of pen register or trap and trace device; classification; exceptions
- ARIZ. REV. STAT. ANN. § 13-3006 (2008) - Divulging communication service information; classification; exception
- ARIZ. REV. STAT. ANN. § 13-3008 (2008) - Possession of interception devices; classification
- ARIZ. REV. STAT. ANN. § 13-3009 (2008) - Duty to report to law enforcement officers; classification. If any person is using surveillance and is unauthorized, anyone having knowledge of this must report to law enforcement.
- ARIZ. REV. STAT. ANN. § 13-3010 (2008) - Ex parte order for interception; definition. Application for from a court with jurisdiction.
- ARIZ. REV. STAT. ANN. § 13-3011 (2008) - Disclosing confidential information relating to ex parte order; exceptions; classification. Except in a trial can't disclose the application for a pen register, identity of a person who was investigated. However, peace officers and prosecuting attorneys can disclose the information in accordance with their duties.
- ARIZ. REV. STAT. ANN. § 13-3016 (2008) - Stored oral, wire and electronic communications; agency access; backup preservation; delayed notice; records preservation request; violation; classification. Stored recordings can be obtained by law enforcement with or without a subpoena, warrant or court order depending on the length of time the communication was stored (less or more than 180 days) and whether the request was made to the subscriber or party.
- ARIZ. REV. STAT. ANN. § 13-3019 (2008) - Surreptitious photographing, videotaping, filming or digitally recording or viewing; exemptions; classification;

definitions. It is unlawful for any person to knowingly photograph, videotape, film, digitally record or by any other means secretly view, with or without a device, another person without that person's consent if the content includes nudity or other very personal images. Security purposes is acceptable use of recording devices, as long as there is notice if the recording is in a place where the person has a reasonable expectation of privacy.

- State v. Cramer, 851 P.2d 147 (Ariz. Ct. App. 1984) - Use of extra-sensory, non-intrusive equipment, infrared meter, is not a search.
- **Computer Statutes**
 - ARIZ. REV. STAT. ANN. § 13-2316 (2008). Computer tampering; venue; forfeiture; classification. Accessing, altering, damaging or destroying any computer, computer system or network, or any part of a computer, computer system or network, with the intent to devise or execute any scheme or artifice to defraud or deceive, or to control property or services by means of false or fraudulent pretenses, representations or promises. Knowingly altering, damaging, deleting or destroying computer programs or data. Knowingly introducing a computer contaminant into any computer, computer system or network.
 - ARIZ. REV. STAT. ANN. § 13-2316.02 (2008). Unauthorized release of proprietary or confidential computer security information; exceptions; classification. A person commits unauthorized release of proprietary or confidential computer security information by communicating, releasing or publishing proprietary or confidential computer security information, security-related measures, algorithms or encryption devices relating to a particular computer, computer system or network without the authorization of its owner or operator. Some exceptions apply.
- **Common Law**
 - **Appropriation**
 - Martinez v. Green, 131 P.3d 492 (Ariz. 2006) - seems to accept the tort of appropriation of one's likeness, even if the individual is deceased.
 - **Disclosure**
 - A.H. Belo Corp. v. Mesa Police Dep't, 42 P.3d 615 (Ariz. 2002) - Arizona imposes a presumption in favor of disclosure under the Public Records Act, Ariz. Rev. Stat. § 39-121 (2001), to defend a refusal to release a public record, the government must demonstrate that the policy in favor of public disclosure and access is outweighed by considerations of "confidentiality, privacy, or the best interests of the state."
 - **False Light**
 - Godbehere v. Phoenix Newspapers, 783 P.3d 781 (Ariz. 1989) - The distinct tort of false light invasion of privacy is recognized in Arizona. Only have to find that the conduct was highly offensive to the reasonable person, not extreme and outrageous.
 - **Intrusion**
 - Hart v. Seven Resorts, 947 P.2d 846 (Ariz. Ct. App. 1997) The tort of intrusion upon seclusion provides that one who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion

of his privacy, if the intrusion would be highly offensive to a reasonable person.

ARKANSAS PRIVACY LAW

- **State Constitutional Privacy Rights**
 - **Express**
 - none
 - **Implied**
 - State v. Harris, 372 Ark. 492 (Ark. 2008) Our Constitution provides greater rights of privacy and greater protection than that afforded under the Federal Constitution. We have made it abundantly clear that though the search-and-seizure language of Article 2, § 15, of the Arkansas Constitution is very similar to the words of the Fourth Amendment, we are not bound by the federal interpretation of the Fourth Amendment when interpreting our own law. We have deviated from federal precedent by embracing a heightened privacy protection for citizens in their homes against unreasonable searches and seizures. *See State v. Brown*, 56 S.W.3d 722 (2004)
 - *See also Jegley v. Picado*, 80 S.W.3d 332 (2002); State v. Sullivan, 74 S.W.3d 215 (2002); Griffin v. State, 67 S.W.3d 582 (2002). Providing more privacy stringent interpretation of § 15 search and seizure.
 - ARK. CONST. art. 2, § 8 (2009). Rights of due process and against self-incrimination.
- **Search and Seizure**
 - ARK. CONST. art. 2, § 15 (2009). Unreasonable searches and seizures. The right of the people of this State to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated; and no warrant shall issue, except upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the person or thing to be seized.
 - **Auto Exception**
 - McDaniel v. State, 990 S.W.2d 515 (Ark. 1999) - recognized the automobile exception to the warrant requirement in accordance with Supreme Court precedent.
 - **Open Fields**
 - Izzard v. State, 663 S.W.2d 192 (Ark. Ct. App. 1984) - Open fields are not areas where one can have a reasonable expectation of privacy. Warrantless aerial observation of marijuana plants was valid because the field was clearly exposed.
 - **Plain View**
 - Durjam v. State, 471 S.W.2d 527 (Ark. 1971) Seizure of objects in "plain view" cannot be justified if the seizing officers had to physically invade a constitutionally protected area in order to secure the view. Officers must be in a place they have a right to be before viewing anything in plain view.
- **Statutory Privacy Rights**
 - ARK. CODE. ANN. § 5-71-229 (2008) - A person commits stalking in the first degree if he or she purposely engages in a course of conduct that harasses another person and makes a terroristic threat with the intent of placing that person in imminent fear of death or serious bodily injury or placing that person in imminent

fear of the death or serious bodily injury of his or her immediate family and the person. Becomes aggravated if done with a deadly weapon or does so repeatedly.

- **Individually Identifiable Government Records**

- ARK. CODE. ANN. 12-12-213 (2008). Invasion of privacy prohibited. Nothing in this subchapter [on crime information center] shall be construed to give authority to any person, agency, corporation, or other legal entity to invade the privacy of any citizen as defined by the General Assembly or the courts other than to the extent provided in this subchapter. Crime Information Center shall make criminal history records on persons available in accordance with a court order or for use by this information center.
- ARK. CODE. ANN. § 9-9-504 (2008) - Adoption birth parent identities may be placed on a registry voluntarily, but if not the adoptee will have to obtain a court order to determine this information
- ARK. CODE. ANN. 27-23-206 (2008) Commercial Driver Alcohol and Drug Testing Act. Notwithstanding any other provision of law to the contrary, personally identifying information of employees in the Commercial Driver Alcohol and Drug Testing Database is confidential and shall be released by the office only as provided under § 27-23-207.
- ARK. CODE. ANN. § 4-110-101 through -108 (2008) Personal Information Protection Act. It is the intent of the General Assembly to ensure that sensitive personal information about Arkansas residents is protected. To that end, the purpose of this chapter is to encourage individuals, businesses, and state agencies that acquire, own, or license personal information about the citizens of the State of Arkansas to provide reasonable security for the information. Protect personal information and disclose breaches
 - "Personal information" means an individual's first name or first initial and his or her last name in combination with any one (1) or more of the following data elements when either the name or the data element is not encrypted or redacted: (A) Social security number; (B) Driver's license number or Arkansas identification card number; (C) Account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account; and (D) Medical information.

- **Public Records**

- ARK. CODE ANN. § 25-19-101 through -109 (2008) Freedom of Information Act. Promotes the idea that public business is performed in an open and public manner.
 - All records maintained within the scope of public employment are presumed to be public records
 - except as otherwise provided records are available for inspection
 - for electronic data, the record custodian may in his discretion choose to summarize the data for the requester.
- ARK. CODE ANN. § 12-12-1003 (2008) - Criminal history information is not a public record under the Freedom of Information Act.
- ARK. CODE ANN. § 12-12-1014 (2008) - Authorizes development of procedures ensuring the security and confidentiality of criminal history records.

- ARK. CODE ANN. § 4-35-107 (2008) All meetings and records of a water authority shall be subject to the Freedom of Information Act of 1967
- ARK. CODE ANN. § 7-4-113 (2008) County board; financial records - The county board of election commissioners of each county shall maintain a record of all funds the county board receives and all expenditures of the county board. These records shall be open to the public under the provisions of the Freedom of Information Act of 1967
- ARK. CODE ANN. § 2-7-202 (2008) All materials, data, and information received by the Arkansas Farm Mediation Office are confidential and are not subject to examination or disclosure as public information under the Freedom of Information Act
- ARK. CODE ANN. § 9-27-352 (2008) Records of the arrest of a juvenile, the detention of a juvenile, and the proceedings under this subchapter shall be confidential and shall not be subject to disclosure under the Freedom of Information Act of 1967
- ARK. CODE ANN. § 10-4-422 (2008) Records--Public inspection - The Legislative Auditor shall keep, or cause to be kept, a complete, accurate, and adequate set of fiscal transactions of the Division of Legislative Audit. Any working papers are not open to public inspection, but the final audit is.
- ARK. CODE ANN. § 19-11-711 (2008) Procurement information shall be public record to the extent provided in the Freedom of Information Act of 1967
- ARK. CODE ANN. § 25-18-501 (2008) any state contract is a public record under the state Freedom of Information Act.
- ARK. CODE ANN. § 17-1-104 (2008) Collection of personal information for the purpose of child support enforcement. Licensing agencies are required to provide information to the Office of Child Support Enforcement, but must not make this information available publically.
- **Motor Vehicle Records**
 - ARK. CODE. ANN. § 27-53-209 (2008). Reports open to public inspection. All motor vehicle accident reports made by the Department of Arkansas State Police, and its records of traffic violations, shall be open to public inspection at all reasonable times.
 - ARK. CODE. ANN. 27-50-906 (2008) Authorizes an abstract of any driver's record furnished to certain persons named in the code besides the driver himself.
 - ARK. CODE. ANN. 27-23-117 (2008). Driving record information to be furnished. Notwithstanding any other provision of law to the contrary, the Office of Driver Services must furnish full information regarding the driving record of any person: (a) To the driver license administrator of any other state, or province or territory of Canada, requesting that information. (b) To any employer or prospective employer upon request and payment of a fee of ten dollars (\$10.00). (c) To others, authorized to receive such information pursuant to § 27-50-906, upon request and payment of a fee of seven dollars (\$7.00).
- **Vehicle Identification Numbers**
 - ARK. CODE. ANN. 27-14-2206 (2008). Report of vehicle left in storage or parked over thirty days. Whenever any vehicle of a type subject to registration in this state has been stored, parked, or left in a garage, trailer park, or any type of

storage or parking lot for a period of over thirty (30) days, the owner of the garage, trailer park, or lot shall, within five (5) days after the expiration of that period, report the make, model, serial or vehicle identification number of the vehicle as unclaimed to the Automobile Theft Section of the Department of Arkansas State Police.

- **Consumer Credit**

- ARK. CODE. ANN. § 4-110-101 through -108 (2008) Personal Information Protection Act. Disclose security breaches.
- ARK. CODE. ANN. 4-86-107 (2008) Consumer Protection. Prohibiting the misappropriation of social security numbers. Except as provided by court rules or federal law, a person or entity may not do any of the following: request a social security number online without having a secure connection, print a social security number on a public document, print the number on any card the consumer may need to access products.
- ARK. CODE. ANN. 4-93-101 through -103 (2008) Credit Reporting Disclosure Act of 1989

- **Financial Records**

- ARK. CODE. ANN. § 23-39-512 (2008) - Unless otherwise specified in this section, all information filed with the Securities Commissioner shall be available for public inspection. Ex. Personal information about employees of mortgage brokers, mortgage bankers, mortgage servicers, or loan officers reported to the commissioner under the department's rules concerning registration of those persons are not available for public inspection.
- ARK. CODE. ANN. § 23-46-101 (2008) - Bank examination reports, reports revealing facts about banks or their customers, and personal financial statements submitted the state bank dept are confidential and may be revealed to the public.
- ARK. CODE. ANN. § 23-48-801 (2008) Customer-bank communication terminal", or "CBCT", means any electronic device or facility, other than a point-of-sale terminal, together with all associated equipment, structures, and systems, through or by means of which a customer and a bank may engage in any banking transaction, whether transmitted to the banking institution instantaneously or otherwise. This definition specifically includes automatic teller machines.
- ARK. CODE. ANN. § 23-48-808 (2008) - A bank using customer-bank communication terminals shall establish and maintain reasonable safeguards designed to protect the privacy and confidentiality of account information.

- **Employee Privacy**

- ARK. CODE. ANN. § 11-14-101 through -112 (2008) - voluntary program for a drug free workplace. All information, interviews, reports, statements, memoranda, and drug or alcohol test results, written or otherwise, received by the covered employer through a drug or alcohol testing program are confidential communications and may not be used or received in evidence, obtained in discovery, or disclosed in any public or private proceedings except in accordance with this section or in determining compensability under this chapter or the Workers' Compensation Law.
- ARK. CODE. ANN. § 11-10-314 (2008) Employment Security - except as otherwise provided, information obtained by a director of an employing unit shall be

confidential. This information is not open to public inspection when revealing an individual or unit's identity.

- **Electronic Surveillance**

- ARK. CODE. ANN. § 5-60-120 (2008) - Interception and recording. It is unlawful for a person to intercept a wire, landline, oral, telephonic communication, or wireless communication, and to record or possess a recording of the communication unless the person is a party to the communication or one of the parties to the communication has given prior consent to the interception and recording. Exceptions include telecommunications companies
 - Nothing in this section shall be interpreted to prohibit or restrict a Federal Communications Commission licensed amateur radio operator or anyone operating a police scanner from intercepting a communication for pleasure.
 - Consistent with the provisions of 18 U.S.C. § 2703, as it existed on January 1, 2003, the issuance of a court order for disclosure of a customer communication or record to a governmental entity requiring the information as part of an ongoing criminal investigation is not prohibited by the laws of this state.
 - Consistent with the provisions of 18 U.S.C. §§ 3122 -- 3127, as they existed on January 1, 2003, the issuance of a court order authorizing or approving the installation and use of a pen register or a trap-and-trace device as part of an ongoing criminal investigation is not prohibited by the laws of this state.

- **Computer Statutes**

- ARK. CODE. ANN. § 5-41-103 (2008) Computer fraud. A person commits computer fraud if the person intentionally accesses or causes to be accessed any computer, computer system, computer network, or any part of a computer, computer system, or computer network for the purpose of: (1) Devising or executing any scheme or artifice to defraud or extort; or (2) Obtaining money, property, or a service with a false or fraudulent intent, representation, or promise.
- ARK. CODE. ANN. § 5-41-104 (2008) Computer Trespass. A person commits computer trespass if the person intentionally and without authorization accesses, alters, deletes, damages, destroys, or disrupts any computer, computer system, computer network, computer program, or data.

- **Common Law**

- Dunlap v. McCarty, 678 S.W.2d 361 (Ark. 1984) Recognizes all four common law invasions of privacy: appropriation, false light, disclosure and intrusion.

CALIFORNIA PRIVACY LAW

- **State Constitutional Privacy Rights**
 - **Express**
 - CAL. CONST. art. I, § 1 (2009) - All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy.
 - Hill v. NCAA, 865 P.2d 633 (Cal. 1994) - the constitutional right to privacy is applicable against state and private entities. There must be a legally recognized privacy interest, a reasonable expectation of privacy and conduct that is a serious invasion of privacy.
- **Search and Seizure**
- CAL. CONST. art. I, § 13 (2009) - The right of the people to be secure in their persons, houses, papers and effects against unreasonable searches and seizures may not be violated. Warrants require probable cause.
 - **Auto Exception**
 - People v. Valdez, 671 P.2d 863 (Cal. 1993) - accepts automobile exception. Under the governing authorities, (1) the ready mobility of automobiles, (2) the lesser expectation of privacy in their contents, (3) the significant administrative expense, delay and risk of loss of contents entailed in requiring the police either to secure all automobiles at the scene or to tow all suspected vehicles to a securely maintained depot, and (4) the need for clear guidelines by which police may guide and regulate their conduct, have led to the adoption of a general rule permitting the police to conduct an immediate, on-the-scene warrantless search of an automobile under such circumstances.
 - **Open Fields**
 - People v. Mayoff, 729 P.2d 166 (Cal. 1986) - aerial surveillance of an open field is acceptable without a warrant.
 - **Plain View**
 - In re Deborah C., 635 P.2d 446 (Cal. 1981) - accepts the plain view doctrine if the observer is in a lawful position to view the item in plain view.
- **Statutory Privacy Rights**
 - CAL. CIV. CODE § 1708.7 (2008) - if a person engaged in a pattern of conduct the intent of which was to follow, alarm, or harass the plaintiff. In order to establish this element, the plaintiff shall be required to support his or her allegations of credible threat with independent corroborating evidence. "Credible threat" means a verbal or written threat, including that communicated by means of an electronic communication device, or a threat implied by a pattern of conduct or a combination of verbal, written, or electronically communicated statements and conduct, made with the intent and apparent ability to carry out the threat so as to cause the person who is the target of the threat to reasonably fear for his or her safety or the safety of his or her immediate family.
 - CAL. CIV. CODE § 43 (2008) - Besides the personal rights mentioned or recognized in the Government Code, every person has, subject to the

qualifications and restrictions provided by law, the right of protection from bodily restraint or harm, from personal insult, from defamation, and from injury to his personal relations.

- CAL. CIV. CODE § 3344 (2008) Unauthorized commercial use of name, voice, signature, photograph or likeness is unlawful.
- CAL. PENAL CODE § 646.9 (2008). Stalking. Any person who willfully, maliciously, and repeatedly follows or willfully and maliciously harasses another person and who makes a credible threat with the intent to place that person in reasonable fear for his or her safety, or the safety of his or her immediate family is guilty of the crime of stalking
- **Individually Identifiable Records**
 - CAL. CIV. CODE § 56.10 through .16 (2008) Disclosure of Medical Information by Providers. Prohibited without authorization, but for certain exceptions if the patient has not expressly requested such information not be disclosed.
 - CAL. GOV'T CODE § 27300 through 27307 (2008) Public records must have truncated social security numbers.
 - CAL. CIV. CODE § 1798.42 (2008). Deletion from disclosure of personal information to individual in disclosing information contained in a record to an individual, an agency shall not disclose any personal information relating to another individual which may be contained in the record.
- **Public Records**
 - CAL. GOV. CODE § 6250 (2008) - In enacting this chapter, the Legislature, mindful of the right of individuals to privacy, finds and declares that access to information concerning the conduct of the people's business is a fundamental and necessary right of every person in this state.
 - CAL. GOV. CODE § 6257.5 (2008) - This chapter does not allow limitations on access to a public record based upon the purpose for which the record is being requested, if the record is otherwise subject to disclosure. Examples not permitted for disclosure include personal health records, or health insurance contracts, state employee home telephone or address, corporate financial records, etc.
 - CAL. GOV. CODE § 6254.20 (2008) - Nothing in this chapter shall be construed to require the disclosure of records that relate to electronically collected personal information, as defined by Section 11015.5, received, collected, or compiled by a state agency.
- **Motor Vehicle Records**
 - CAL. VEH. CODE § 1798.26 (2008) -With respect to the sale of information concerning the registration of any vehicle or the sale of information from the files of drivers' licenses, the Department of Motor Vehicles shall, by regulation, establish administrative procedures under which any person making a request for information shall be required to identify himself or herself and state the reason for making the request.
 - CAL. VEH. CODE § 1810.7 (2008) - Except as provided in Sections 1806.5, 1808.2, 1808.4, 1808.5, 1808.6, 1808.7, and 1808.21, the department may authorize, by special permit, any person to access the department's electronic database, as provided for in this section, for the purpose of obtaining information for commercial use. The department shall establish procedures to ensure

confidentiality of any records of residence addresses and mailing addresses as required by Sections 1808.21, 1808.22, 1808.45, 1808.46, and 1810.2. The exceptions include: providing info that would be in contravention of the fair credit reporting act, giving out addresses of peace officers, giving out info on mental or physical conditions, giving out information on DUI intervention programs.

- CAL. VEH. CODE § 1808 (2008) - Except where a specific provision of law prohibits the disclosure of records or information or provides for confidentiality, all records of the department relating to the registration of vehicles, other information contained on an application for a driver's license, abstracts of convictions, and abstracts of accident reports (except for abstracts of accidents where, in the opinion of a reporting officer, another individual was at fault) shall be open to public inspection during office hours. All abstracts of accident reports shall be available to law enforcement agencies and courts of competent jurisdiction.
- CAL. VEH. CODE § 1808.4 and 1808.8 (2008) - For all of the following persons, his or her home address that appears in a record of the department, is confidential if the person requests the confidentiality of that information: includes attorney general, district attorney, directors of the boards of corrections, etc.
- CAL. VEH. CODE § 20012 (2008) All required accident reports, and supplemental reports, shall be without prejudice to the individual so reporting and shall be for the confidential use of the Department of Motor Vehicles and the Department of the California Highway Patrol, except that the Department of the California Highway Patrol or the law enforcement agency to whom the accident was reported shall disclose the entire contents of the reports, including, but not limited to, the names and addresses of persons involved or injured in, etc. Also may be provided to the attorney representing a party.
- **Vehicle Identification Numbers**
 - CAL. VEH. CODE § 4150 (2008) - Application for the original or renewal registration of a vehicle of a type required to be registered under this code shall be made by the owner to the department upon the appropriate form furnished by it and shall contain all of the following: The true, full name, business or residence and mailing address, and driver's license or identification card number, if any, of the owner, and the true, full name and business or residence or mailing address of the legal owner, if any; the name of the county in which the owner resides; description of the vehicle and any other information to show that the vehicle is eligible for registration
 - CAL. VEH. CODE § 2805 (2008) For the purpose of locating stolen vehicles, (1) any member of the California Highway Patrol, or (2) a member of a city police department, a member of a county sheriff's office, or a district attorney investigator, whose primary responsibility is to conduct vehicle theft investigations, may inspect any vehicle of a type required to be registered under this code, or any identifiable vehicle component thereof, on a highway or in any public garage, etc.
- **Consumer Credit**
 - CAL. PENAL CODE § 11149.4 (2008). Action for invasion of privacy. Any vendor or employee of a vendor who intentionally discloses information, not otherwise

public, which that person knows or should reasonably know was obtained from confidential information, shall be subject to a civil action for invasion of privacy by the individual to whom the information pertains.

- CAL. CIV. CODE § 1785.11 (2008) - allows a credit reporting agency to issue credit reports only to the individual, to other recipients that the individual authorizes in writing, under a court order, or to a recipient who intends to use the information to issue credit, as an employment check, to issue a license, or a check before renting a dwelling. A consumer may have his/her name removed from the list.
- CAL. CIV. CODE § 1785.18 (2008) - consumer credit reporting agencies need to state which public record provided the information they report. The agencies may never report for employment purposes any information on the age, marital status, race, color, or creed of any consumer. And any adverse information the agencies report for employment purposes must be kept up to date. The information shall be considered up to date if the current public record status of the item at the time of the report is reported.
- CAL. CIV. CODE § 1785.19.5 (2008) - Every consumer credit reporting agency shall create reasonable procedures to prevent a consumer credit report or information from a consumer's file from being provided to any third party for marketing purposes or for any offer of credit not requested by the consumer.
- CAL. CIV. CODE § 1798.60 (2008) - An individual's name and address may not be distributed for commercial purposes, sold, or rented by an agency unless such action is specifically authorized by law.
- CAL. CIV. CODE § 1798.29 (2008) Disclosure of breach of security by agency that owns or maintains computerized data that contains personally indentifying information.
- CAL. CIV. CODE § 1798.82 (2008) Disclosure of breach in security business maintaining computerized data that includes personal information.
- CAL. GOV'T. CODE § 7493 (2008) Right to obtain credit or consumer credit report. Nothing in this chapter shall be construed to preclude a state or local agency from obtaining a credit report or consumer credit report from anyone other than a financial institution.
- **Financial Records**
 - CAL. GOV'T. CODE §§ 7460 through 7493 - California Right to Financial Privacy Act. Financial records of customers of financial institutions may be obtained by law enforcement personnel only if the records are described with particularity and there is a valid search warrant or subpoena in support of the records request.
 - CAL. FIN. CODE § 4050 through § 4060 (2008) California Financial Information Privacy Act. Contains restrictions on sharing consumer information that are greater than the restrictions contained under federal laws. Contains a provision allowing a consumer to object to (opt-out of) a financial institution's sharing of consumer information with its affiliates.
- **Employee Privacy**
 - Cal Gov Code § 8350 (2008) Drug-Free Workplace Act of 1990. But does not allow drug testing as a condition of employment, only educating employees against the dangers of drugs.

- **Electronic Surveillance**
 - CAL. FAM. CODE § 2022 (2008) - Evidence collected by eavesdropping; admissibility.
 - CAL. PENAL CODE § 629.50 (2008) - Application for order authorizing interception; facsimile copies Electronic Digital Pager, or Electronic Cellular Telephone Communications
 - CAL. PENAL CODE § 629.52 (2008) - Order authorizing interception; required findings; specified offenses
 - CAL. PENAL CODE § 629.53 (2008) - Guidelines for judges; establishment
 - CAL. PENAL CODE § 629.54 (2008) - Contents of order authorizing interception
 - CAL. PENAL CODE § 629.56 (2008) - Oral approval without order; required findings
 - CAL. PENAL CODE § 629.58 (2008) - Period of authorization; extensions; termination; interpreters
 - CAL. PENAL CODE § 629.60 (2008) - Reports to judge issuing order
 - CAL. PENAL CODE § 629.61 (2008) - Report to attorney general; regulations on collection and dissemination of information; disclosure of information
 - CAL. PENAL CODE § 630 (2008) - Invasion of Privacy Declaration of Policy. The Legislature hereby declares that advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society. The Legislature by this chapter intends to protect the right of privacy of the people of this state.
 - CAL. PENAL CODE § 631 (2008) - Wiretapping
 - CAL. PENAL CODE § 632 (2008) - Eavesdropping on or recording confidential communications
 - CAL. PENAL CODE § 632.5 (2008) - Cellular radio telephone interceptions; application of section
 - CAL. PENAL CODE § 632.6 (2008) - Cordless or cellular telephones; interception or receipt of communications without consent; punishment; exceptions
 - CAL. PENAL CODE § 632.7 (2008) - Cordless or cellular radio telephones; intentional recordation of communications without consent; punishment; exceptions
 - CAL. PENAL CODE § 633 (2008) - Law enforcement officers; authorized use of electronic, etc., equipment
 - CAL. PENAL CODE § 633.1 (2008) - Airport law enforcement officer telephone call; recording; admissibility of evidence; application of section
 - CAL. PENAL CODE § 633.5 (2008) - Recording communications relating to commission of extortion, kidnapping, bribery, felony involving violence against the person, or violation of § 653m
 - CAL. PENAL CODE § 633.6 (2008) - Domestic violence restraining order; permission to record prohibited communications by perpetrator
 - CAL. PENAL CODE § 637.7 (2008) Use of electronic tracking device to determine person's location; Consensual use to track vehicle (a) No person or entity in this

state shall use an electronic tracking device to determine the location or movement of a person. (b) This section shall not apply when the registered owner, lessor, or lessee of a vehicle has consented to the use of the electronic tracking device with respect to that vehicle. (c) This section shall not apply to the lawful use of an electronic tracking device by a law enforcement agency. (d) As used in this section, "electronic tracking device" means any device attached to a vehicle or other movable thing that reveals its location or movement by the transmission of electronic signals. (e) A violation of this section is a misdemeanor.

- **Computer Statutes**

- CAL. PENAL CODE § 502 through § 509 (2008) - Anyone who knowingly accesses and without permission alters computer data or without authorization copies any data from any computer system or intentionally causes the disruption of a computer system is subject to criminal penalties.

- **Common Law**

- Diaz v. Oakland Tribune, 139 Cal. App. 3d 118 (1983) - accepts the four invasion of privacy causes of action.

COLORADO PRIVACY LAW

- **State Constitutional Privacy Rights**
 - none
- **Search and Seizure**
 - COLO. CONST. art. II, § 7 (2008) Protects citizens against unreasonable search and seizure and provides for warrants only upon probable cause.
 - Univ. of Colo. v. Derdeyn, 863 P.2d 929 (Colo. 1993). In the absence of voluntary consent, random, suspicionless drug testing programs for intercollegiate athletes are a violation of article II, § 7.
 - People v. Hillman, 834 P.2d 1271 (Colo. 1992) - Colorado construes its constitutional search and seizure protections more stringently than the Fourth Amendment, however because there was no expectation of privacy in the curbside garbage bags, warrantless search of such bags was valid.
 - **Auto Exception**
 - People v. Reyes, 956 P.2d 1254 (Colo. 1998) the court found that the officers' reasonable suspicion that the truck contained controlled substances, coupled with the narcotics canine's two alerts to the vehicle, provided the officers with probable cause to conduct a warrantless search of the passenger compartment of defendant's truck in accordance with the automobile exception to the warrant requirement. Thus, the cocaine found in the truck was the product of a lawful search.
 - **Open Fields**
 - People v. McClaugherty, 566 P.2d 361 (Colo. 1977) - accepting the open fields doctrine.
 - **Plain View**
 - People v. Nefzger, 476 P.2d 995 (Colo. 1970) - accepting the plain view doctrine.
- **Statutory Privacy Rights**
 - COLO. REV. STAT. § 18-9-111 (2008) A person commits stalking if directly, or indirectly through another person, such person knowingly: Makes a credible threat to another person and, in connection with such threat, repeatedly follows, approaches, contacts, or places under surveillance that person, a member of that person's immediate family, or someone with whom that person has or has had a continuing relationship. OR Repeatedly follows, approaches, contacts, places under surveillance, or makes any form of communication with another person.
 - An electronic surveillance device installed on the victim's car "repeatedly" stored information about her movements thereby allowing the defendant to gain information about her on repeated occasions, and therefore satisfying the requirements of this section. People v. Sullivan, 53 P.3d 1181 (Colo. App. 2002).
 - The phrase "under surveillance" includes electronic surveillance that records a person's whereabouts as that person moves from one location to another and allows the stalker to access that information either simultaneously or shortly thereafter. People v. Sullivan, 53 P.3d 1181 (Colo. App. 2002).
- **Individually Identifiable Government Records**

- COLO. REV. STAT. 26-13-102.7 (2008) Child Support Personal Information. In addition to any other confidentiality provisions set forth in this article and section 14-14-113, C.R.S., the child support enforcement agency and the delegate child support enforcement units, when exercising authority pursuant to this article and section 14-14-113, C.R.S., to establish, modify, or enforce support obligations, shall make every effort to preserve the integrity and confidentiality of the informational data obtained from other sources about the support obligor and obligee and the informational data provided to any other source about such individuals.
- COLO. REV. STAT. § 14-14-113 (2008). Recordation of social security numbers in certain family matters. Any commercial driver's license, marriage license, occupational license for the state requires a social security number for the application. An individual can provide a sworn statement as substituting for the social security number. Also, the license card will not contain the social.
- COLO. REV. STAT. § 6-1-715 (2008) - Third parties may not publicly display of SSN and no entry of SSN on a website without encryption and secure connections. BUT, This section shall not prevent the collection, use, or release of a social security number as required, permitted, or authorized by state or federal law or the use of a social security number for internal verification or administrative purposes, including by the department of revenue.
- COLO. REV. STAT. § 25-2-113.5 (2008) Limited access to information upon consent of all parties--voluntary adoption registry.
- **Public Records**
 - COLO. REV. STAT. § 24-72-201; -203 (2008) - It is declared to be the public policy of this state that all public records shall be open for inspection by any person at reasonable times, except as provided in this part 2 or as otherwise specifically provided by law. The official custodian of any public records may make such rules with reference to the inspection of such records as are reasonably necessary for the protection of such records.
 - COLO. REV. STAT. § 24-72-204 (2008) - The records custodian may deny inspection of records for criminal investigations, test questions and answers for administrative licensing, research by state agencies and organizations, real estate appraisals, market analysis by the transportation authority, expenditures of public moneys for security arrangements and investigations, Electronic mail addresses provided by a person to an agency, institution, or political subdivision of the state for the purposes of future electronic communications, medical, mental health, sociological, and scholastic achievement data on individual persons (with some exceptions).
 - COLO. REV. STAT. § 24-72-305.5 (2008) - Records of official actions and criminal justice records and the names, addresses, telephone numbers, and other information in such records shall not be used by any person for the purpose of soliciting business for pecuniary gain.
 - COLO. REV. STAT. § 24-90-119 (2008) Privacy of user records. A publicly-supported library shall not disclose any record or other information that identifies a person as having requested or obtained specific materials or service or as otherwise having used the library. (certain exceptions apply)

- **Motor Vehicle Records**
 - COLO. REV. STAT. § 42-1-206 (2008) - The department or an authorized agent shall require any person, other than a person in interest as defined in section 24-72-202 (4), C.R.S., or a federal, state, or local government agency carrying out its official functions, requesting inspection of a motor vehicle or driver record from the department or agent individually or in bulk, to sign a requestor release form and, under penalty of perjury, an affidavit of intended use prior to providing the record to such person. The department or authorized agent may allow inspection of motor vehicle and driver records only as authorized under section 24-72-204 (7), C.R.S.
 - COLO. REV. STAT. § 42-5-103 (2008). Tampering with a motor vehicle. Any person who with criminal intent, tampers with a motor vehicle or to any part, equipment, attachment, accessory, or appurtenance contained in or forming a part thereof without the knowledge and consent of the owner of such motor vehicle commits a crime.
- **Vehicle Identification Numbers**
 - COLO. REV. STAT. § 42-5-102 (2008). Stolen motor vehicle parts - buying, selling - removed or altered motor vehicle parts. Any person who removes or alters the VIN is subject to criminal penalties.
 - COLO. REV. STAT. § 42-5-202 (2008). Vehicle identification number inspection. The VIN of a bonded title vehicle, homemade vehicle, rebuilt vehicle, reconstructed vehicle, or vehicle assembled from a kit must be inspected in order for those vehicles to be sold in Colorado.
- **Consumer Credit**
 - COLO. REV. STAT. 6-1-716 (2008) Colorado Consumer Protection Act - must notify as soon as possible of an unauthorized breach in security, which is an unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by an individual or a commercial entity.
 - Good faith acquisition of personal information by an employee or agent of an individual or commercial entity for the purposes of the individual or commercial entity is not a breach of the security of the system if the personal information is not used for or is not subject to further unauthorized disclosure.
 - An individual or a commercial entity that conducts business in Colorado and that owns or licenses computerized data that includes personal information about a resident of Colorado shall, when it becomes aware of a breach of the security of the system, conduct in good faith a prompt investigation to determine the likelihood that personal information has been or will be misused.
 - COLO. REV. STAT. § 12-14.3-101 through -109 (2008) Colorado Consumer Credit Reporting Act. Rules for providing personal credit history to consumers and third parties.
 - Note: A consumer reporting agency shall not furnish for employment purposes, or in connection with a credit or insurance transaction or a direct marketing transaction, a consumer report that contains medical

information about a consumer unless the consumer consents to the furnishing of the report.

- **Financial Records**

- COLO. REV. STAT. § 11-102-307 (2008). Access to records. The commissioner shall have access to any record of the division relating to state banks, and the appointive members of the banking board shall have such access upon the affirmative vote of a majority of the members of the banking board.
- COLO. REV. STAT. § 11-102-306 (2008). Banking Information. All employees of the division of banking shall not divulge any information acquired by them in the discharge of their duties except insofar as disclosure may be rendered necessary or authorized by law, including section 11-102-305 (4). The banking board may exchange information with the United States comptroller of the currency, the federal deposit insurance corporation, the board of governors of the Federal Reserve System, the federal home loan bank. Also can exchange information obtained by the banking board relating to: Possible violations of the federal "Employee Retirement Income Security Act of 1974", possible criminal violations of federal law and the activities of money transmitters and foreign capital depositories pertaining to compliance with federal money laundering and other financial crimes laws.
 - Banking Board may disclose any information in the records of the division of banking or acquired by them within the discharge of their duties that is publicly available from the federal deposit insurance corporation, the United States comptroller of the currency, or the Federal Reserve System.
- COLO. REV. STAT. 11-102-305 (2008) - Information from the records of the division of banking shall be revealed only to members of the banking board, with some exceptions including where disclosure is mandated by law.
- COLO. REV. STAT. 26-13-128 (2008) Child Support Disclosure. The purpose of the program authorized by this section shall be to develop and operate, in coordination with such financial institutions and state entities, a data match system, using automated data exchanges, to the maximum extent feasible, in which each such financial institution or state entity is required to provide at least semiannually the name, record address, and social security number, or other taxpayer identification number, of any account holder or customer that maintains an account at such institution or entity and who owes past-due child support, as identified by the state by name and social security number or other taxpayer identification number.
- COLO. REV. STAT. 11-37.5-201 (2008) - The confidential relationship between a foreign capital depository and its customers is to be protected by restrictions on the disclosure of financial records to supervisory agencies and a prohibition against disclosure of financial records to other state and local agencies and to private individuals except under specified conditions.

- **Employee Privacy**

- COLO. REV. STAT. § 22-32-110.7 (2008). Board of education - specific powers - drug testing. The general assembly therefore authorizes school districts to create school safety programs, which may include drug testing of all personnel who apply for, transfer to, or are promoted to safety-sensitive positions. The program

may also include drug testing of personnel in safety-sensitive positions if there is probable cause to believe the person is using illegal drugs.

- *No details on how the testing may be carried out, or the confidentiality of information obtained.*

- **Electronic Surveillance**

- COLO. REV. STAT. § 16-15-101 (2008) Definitions. "Electronic communication" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate or foreign commerce but does not include: (b) Any wire or oral communication; (c) Any communication made through a tone-only paging device; or (d) Any communication from a tracking device.
- COLO. REV. STAT. § 16-15-102 (2008) Ex parte order authorizing the interception of wire, oral, or electronic communications
- COLO. REV. STAT. § 16-15-103 (2008) Order may direct others to furnish assistance
- COLO. REV. STAT. § 16-15-104 (2008) Reports to state court administrator and attorney general
- COLO. REV. STAT. § 18-9-302 (2008) Wiretapping and eavesdropping devices prohibited--penalty. Class 5 felony.
- COLO. REV. STAT. § 18-9-303 (2008) Wiretapping prohibited--penalty
- COLO. REV. STAT. § 18-9-304 (2008) Eavesdropping prohibited--penalty
- COLO. REV. STAT. § 18-9-305 (2008) Exceptions
- COLO. REV. STAT. § 18-9-309 (2008) Telecommunications crime. Commits misdemeanor to felony depending on the number of infractions if a person accesses, uses, manipulates, or damages any telecommunications device without the authority of the owner or person who has the lawful possession or use thereof. Creating cloned devices or intercepts signals between cell phones is also prohibited. Law enforcement and telecommunications services who are properly conducting services are exempt.

- **Computer Statutes**

- COLO. REV. STAT. 18-9-309 (2008) - It is a crime to access any telecommunications device without the authority of the owner. Includes accessing remotely using illegal telecommunications equipment like computer hardware and software.
- COLO. REV. STAT. 18-5.5-102 through -101 (2008). Computer crime (1) A person commits computer crime if the person knowingly: (a) Accesses a computer, computer network, or computer system or any part thereof without authorization; exceeds access; accesses with the intent to defraud, damage, interrupts services, impairs functioning

- **Common Law**

- People v. Home Ins. Co., 591 P.2d 1036 (Colo. 1979) Accepts the four strands of the invasion of privacy common law- intrusion, appropriate, disclosure and false light.

CONNECTICUT PRIVACY LAW

- **State Constitutional Privacy Rights**
 - none
- **Search and Seizure**
 - CONN. CONST. art. I, § 7 - protects against unreasonable search and seizure.
 - State v. Dukes, 547 A.2d 10 (Conn. 1998) - The state constitution provides more personal protection than the federal. However, only unreasonable searches are proscribed by the Connecticut Constitution.
 - State v. Hanna, 191 A.2d 124 (Conn. 1963) - consent to search will waive constitutional protection.
 - **Auto Exception**
 - State v. Smith, 777 A.2d 182 (Conn. 2000) - recognizing the auto exception to the search warrant requirement.
 - **Open Fields**
 - State v. Penna, 241 A.2d 385 (Conn. Cir. Ct. 1967) - accepts open field's exception to warrant requirement.
 - **Plain View**
 - State v. Salz, 512 A.2d 921 (Conn. App. Ct. 1986) accepts plain view exceptions as long as the initial intrusion is lawful and there is probable cause to believe the items viewed are unlawful. Inadvertent discovery is not necessary.
- **Statutory Privacy Rights**
 - CONN. GEN. STAT. § 53a-181c, d, e (2008) - A person is guilty of stalking in the [first, second, third] degree when, with [intent, recklessly] to cause another person to fear for his physical safety, he willfully and repeatedly follows or lies in wait for such other person and causes such other person to reasonably fear for his physical safety. Stalking can be gravitated to the first degree if this is a repeated offense.
 - CONN. GEN. STAT. § 16-262c (2008) - Privacy of individual customer utility usage and billing information.
 - CONN. GEN. STAT. § 42-470 (2008). Restriction on display and use of Social Security number.
- **Individually Identifiable Government Records**
 - CONN. GEN. STAT. § 16-262c (2008) Conviction information shall be available to the public for any purpose. Nonconviction information shall be available to the subject of the information and to the subject's attorney pursuant to this subsection and subsection (e) of this section.
 - CONN. GEN. STAT. § 7-51a (2008) - Copies of vital records. Access to vital records by members of genealogical societies. Marriage licenses. Death certificates. of any records that are over 100 years old.
- **Public Records**
 - CONN. GEN. STAT. § 1-210 (2008) - Except as otherwise provided by any federal law or state statute, all records maintained or kept on file by any public agency, whether or not such records are required by any law or by any rule or regulation, shall be public records and every person shall have the right to (1) inspect such records promptly during regular office or business hours, (2) copy such records in

accordance with subsection (g) of section 1-212, or (3) receive a copy of such records in accordance with section 1-212.

- CONN. GEN. STAT. § 1-211 (2008) Any public agency which maintains public records in a computer storage system shall provide, to any person making a request pursuant to the Freedom of Information Act, a copy of any nonexempt data contained in such records, properly identified, on paper, disk, tape or any other electronic storage device or medium requested by the person, if the agency can reasonably make such copy or have such copy made.
- CONN. GEN. STAT. § 4d-37 (2008) - No contractor or subcontractor, or employee or agent of a contractor or subcontractor, shall sell, market or otherwise profit from the disclosure or use of any public records which are in its possession pursuant to a contract, subcontract or amendment to a contract or subcontract, except as authorized in the contract, subcontract or amendment.
- CONN. GEN. STAT. § 1-210 (2008) - Preliminary drafts or notes provided the public agency has determined that the public interest in withholding such documents clearly outweighs the public interest in disclosure, personnel or health files that would constitute an invasion of privacy, law enforcement investigations, pending claims, trade secrets, answers to test questions for certifying agencies, commercial data given in confidence.
- CONN. GEN. STAT. § 7-232a (2008) municipal utility established under this chapter, or a municipal electric or gas utility owned, leased, maintained, operated, managed or controlled by any unit of local government under the general statutes or a special act, may withhold from public disclosure under the Freedom of Information Act, as defined in section 1-200, any commercially valuable, confidential or proprietary information.
- CONN. GEN. STAT. § 38a-1043 (2008). Access to information. HealthCare. Each managed care organization shall, when presented with the written consent of the consumer or the consumer's guardian or legal representative, provide to the Office of the Healthcare Advocate access to records relating to such consumer.
- *See also Perkins v. Freedom of Information Commn*, 635 A.2d 783 (Conn. 1993)
- *Chairman v. Freedom of Information Commn*, 585 A.2d 96 (Conn. 1991) - If a person has a real expectation of privacy in the documents, and the disclosure would create the potential for embarrassment, they shall not be disclosed.
- **Motor Vehicle Records**
 - CONN. GEN. STAT. § 14-10 (2008) The commissioner may disclose personal information from a motor vehicle record to certain entities including the government and its agencies, for purposes investigating: motor vehicle or driver safety and theft, motor vehicle emissions, motor vehicle product alterations, recalls or advisories, performance monitoring of motor vehicles and dealers by motor vehicle manufacturers, motor vehicle market research activities including survey research, motor vehicle product and service communications and removal of nonowner records from the original; in the normal course of business if only for verification, etc.
- **Vehicle Identification Numbers**
 - *State v. Colon*, 316 A.2d 797 (Conn. Cir. Ct. 1973) - the court held that occupants of a car could not harbor an expectation of privacy concerning the identification

of the vehicle because the number was quasi-public information, obtained by merely looking through the windshield, and a search of the part of the car displaying the number was but a minimal invasion of a person's privacy.

- State v. Conger, 439 A.2d 381 (Conn. 1981) - The police intrusion now complained of amounted to the officers' obtaining the vehicle identification numbers from the three vehicles inspected. We note that the action of a lawfully present police officer peering through a motor vehicle windshield to view its vehicle identification number need not, under all circumstances, be justified by a showing of probable cause.
- CONN. GEN. STAT. § 14-164aa (2008) destroying event data recorder after crash event prohibited. The data is used for the purpose of improving motor vehicle safety, security or traffic management, including the purpose of medical research on physical reaction to motor vehicle accidents, provided the identity of the registered owner, lessee, operator or other occupant of the motor vehicle is not disclosed with respect to the data, except that the disclosure of a vehicle identification number with the last six numbers deleted for such purposes shall not constitute disclosure of the identity of the registered owner.
- **Consumer Credit**
 - CONN. GEN. STAT. § 36a-696 (2008) - No creditor shall take adverse action based wholly or in part on a credit report on any consumer applying to such creditor for credit for personal, family or household purposes without first disclosing to the consumer the name and address of the credit rating agency which issued the report.
 - CONN. GEN. STAT. § 36a-701b (2008) - Breach of security re computerized data containing personal information. Disclosure of breach as soon as possible.
 - "breach of security" means unauthorized access to or acquisition of electronic files, media, databases or computerized data containing personal information when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable.
 - "personal information" means an individual's first name or first initial and last name in combination with any one, or more, of the following data: (1) Social Security number; (2) driver's license number or state identification card number; or (3) account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account. "Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media.
- **Financial Records**
 - CONN. GEN. STAT. § 17b-137 (2008) The Commissioner of Social Services may subpoena the financial records of any financial institution concerning property of any person applying for or presently or formerly receiving aid or care from the state or who is indebted to such applicant or recipient. The Commissioner of Social Services may subpoena such records of any parent or parents of any child applying for or presently or formerly receiving assistance under the aid to families

with dependent children program, the temporary family assistance program or the state-administered general assistance program.

- CONN. GEN. STAT. § 36a-42 (2008). Disclosure of financial records prohibited; exceptions. Subpoena, consent and other limited circumstances are acceptable.
- CONN. GEN. STAT. § 36a-43 (2008). Disclosure of financial records pursuant to lawful authority.
- CONN. GEN. STAT. § 36a-44 (2008). Exceptions are confidential treatment of customer records. For the IRS, employees of the banking institution, etc.
- **Employee Privacy**
 - CONN. GEN. STAT. § 31-48b (2008) - Use of electronic surveillance devices by employers limited. Prohibition on recording negotiations between employers and employees.
 - CONN. GEN. STAT. § 31-128f (2008). Employee's consent required for disclosure. No individually identifiable information contained in the personnel file or medical records of any employee shall be disclosed by an employer to any person or entity not employed by or affiliated with the employer without the written authorization of such employee except where the information is limited to the verification of dates of employment and the employee's title or position and wage or salary.
 - CONN. GEN. STAT. § 31-51w (2008) - No employer or employer representative, agent or designee engaged in a urinalysis drug testing program shall directly observe an employee or prospective employee in the process of producing the urine specimen. Any results of urinalysis drug tests conducted by or on behalf of an employer shall be maintained along with other employee medical records and shall be subject to the privacy protections. And are inadmissible in a criminal proceeding.
 - CONN. AGENCIES REGS. § 31-51x-1 (2009). Designation by the labor commissioner of occupations as high-risk or safety-sensitive occupations subject to random urinalysis drug testing. The Labor Department shall furnish to the employer a notice which states that a written request has been received by the department that an occupation be designated as a high-risk or safety-sensitive occupation for the purpose of random urinalysis drug testing. The employer shall post this notice in a conspicuous location accessible to employees at the worksite affected by the request.
 -
- **Electronic Surveillance**
 - CONN. GEN. STAT. § 53a-187 (2008) - Definitions. Applicability. "Wiretapping" means the intentional overhearing or recording of a telephonic or telegraphic communication or a communication made by cellular radio telephone by a person other than a sender or receiver thereof, without the consent of either the sender or receiver, by means of any instrument, device or equipment.
 - CONN. GEN. STAT. § 53a-188 (2008) - Tampering with private communications: Class A misdemeanor. A person is guilty of tampering with private communications when: (1) Knowing that he does not have the consent of the sender or receiver, he obtains from an employee, officer or representative of a telephone or telegraph corporation, by connivance, deception, intimidation or in any other manner, information with respect to the contents or nature of a

telephonic or telegraphic communication; or (2) knowing that he does not have the consent of the sender or receiver, and being an employee, officer or representative of a telephone or telegraph corporation, he knowingly divulges to another person the contents or nature of a telephonic or telegraphic communication.

- CONN. GEN. STAT. § 53a-189 (2008) - Eavesdropping: Class D felony. One is guilty of eavesdropping when he unlawfully engages in wiretapping or mechanical overhearing of a conversation.
- CONN. GEN. STAT. § 54-41a (2008) - "Electronic, mechanical or other device" means any device or apparatus which can be used to intercept a wire communication other than (A) any telephone or telegraph instrument, equipment or facility, or any component thereof (I) furnished to the subscriber or used by a communications common carrier in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business, or (ii) being used by a communications common carrier in the ordinary course of its business, (B) a hearing aid or similar device being used to correct subnormal hearing to not better than normal.
- CONN. GEN. STAT. § 54-41b (2008) - Application for order authorizing interception
- CONN. GEN. STAT. § 54-41c (2008) - Information in application
- CONN. GEN. STAT. § 54-41d (2008) - Issuance of order
- CONN. GEN. STAT. § 54-41e (2008) - Statement by panel on issuance of order. Contents of order
- CONN. GEN. STAT. § 54-41f (2008) - Execution of order; progress reports
- CONN. GEN. STAT. § 54-41g (2008) - Extensions of order
- CONN. GEN. STAT. § 54-41h (2008) - Privileged wire communications; issuance of order and interception prohibited. If the facilities from which, or the place where, the wire communications are to be intercepted are being used, or are about to be used, or are leased to, listed in the name of, or commonly used by, a licensed physician, an attorney-at-law or a practicing clergyman, no order shall be issued and no wire communications shall be intercepted over such facilities or in such places.
- CONN. GEN. STAT. § 54-41i (2008) - Recording of interception; sealing, custody and destruction
- CONN. GEN. STAT. § 54-41j (2008) - Sealing, custody, storage and destruction of applications and orders
- **Computer Statutes**
 - CONN. GEN. STAT. § 53a-250 through -261 (2008) Computer Crime
 - Unauthorized access to a computer system. (1) A person is guilty of the computer crime of unauthorized access to a computer system when, knowing that he is not authorized to do so, he accesses or causes to be accessed any computer system without authorization. Defenses of good faith applicable.
 - Theft of computer services. A person is guilty of the computer crime of theft of computer services when he accesses or causes to be accessed or

otherwise uses or causes to be used a computer system with the intent to obtain unauthorized computer services.

- Interruption of computer services. A person is guilty of the computer crime of interruption of computer services when he, without authorization, intentionally or recklessly disrupts or degrades or causes disruption of services.
- Misuse of computer system information. A person is guilty of the computer crime of misuse of computer system information when: (1) As a result of his accessing or causing to be accessed a computer system, he intentionally makes or causes to be made an unauthorized display, use, disclosure or copy, in any form, of data residing in, communicated by or produced by a computer system
- Destruction of computer equipment. A person is guilty of the computer crime of destruction of computer equipment when he, without authorization, intentionally or recklessly tampers with, takes, transfers, conceals, alters, damages or destroys any equipment used in a computer system or intentionally or recklessly causes any of the foregoing to occur.
- CONN. GEN. STAT. § 53-451 (2008) Computer Crime. Temporarily or permanently remove, halt or otherwise disable any computer data, computer programs or computer software from a computer or computer network; Cause a computer to malfunction, regardless of how long the malfunction persists; Alter or erase any computer data, computer programs or computer software; Effect the creation or alteration of a financial instrument or of an electronic transfer of funds.
- **Common Law**
 - Foncello v. Amorossi, 931 A.2d 924 (Conn. 2007) - recognizes the four strands of the common law action for invasion of privacy: appropriation, false light, intrusion and disclosure.

DELAWARE PRIVACY LAW

- **State Constitutional Privacy Rights**
 - none
- **Search and Seizure**
 - DEL. CONST. art. I, § 6 (2008) - protects against unreasonable search and seizure
 - DEL. CONST. art. I, § 7 (2008) protects against self incrimination
 - DEL. CODE ANN. tit. 11, § 2308 (2008) - A search warrant shall not authorize the person executing it to search any dwelling house in the nighttime unless the judge, justice of the peace or magistrate is satisfied that it is necessary in order to prevent the escape or removal of the person or thing to be searched for, and then the authority shall be expressly given in the warrant. For purposes of this section the term "nighttime" shall mean the period of time between 10:00 p.m. and 6:00 a.m.
 - **Auto Exception**
 - Dorsey v. State 761 A.2d 807 (Del. 2000) - recognized auto exception to the warrant requirement
 - **Open Fields**
 - State v. Halko, 188 A.2d 100 (Del. Super. Ct. 1962) - recognized the open fields exception and suggests that a roadway may be considered an open field.
 - **Plain View**
 - Boardley v. State, 612 A.2d 150 (Del. 1991) Seizure of evidence under the plain view doctrine is permitted where (1) viewed during lawful police activity, (2) the contact is inadvertent, and (3) the item has immediate evidentiary value.
- **Statutory Privacy Rights**
 - DEL. CODE ANN. tit. 11, § 1311 (2008) - A person is guilty of harassment if that person insults, taunts or challenges another person or engages in any other course of alarming or distressing conduct which serves no legitimate purpose and is in a manner which the person knows is likely to provoke a violent or disorderly response or cause a reasonable person to suffer fear, alarm, or distress. Communicates with a person by telephone, telegraph, mail or any other form of written or electronic communication in a manner which the person knows is likely to cause annoyance or alarm including, but not limited to, intrastate telephone calls initiated by vendors for the purpose of selling goods or services.
 - DEL. CODE ANN. tit. 11, § 1335 (2008) Violation of privacy - Trespasses on property intending to subject anyone to eavesdropping or other surveillance in a private place; Installs in or outside any private place, without consent of the person or persons entitled to privacy there, any device for observing, photographing, recording, amplifying or broadcasting sounds or events in that place; or intercepts without the consent of all parties thereto a message by telephone, telegraph, letter or other means of communicating privately, including private conversation; or Secretly or surreptitiously videotapes, films, photographs or otherwise records another person in an intimate way; or divulges an unlawfully intercepted message.
 - Exceptions include telecommunications carriers, under court order, or lawful activities of police officers.

- **Individually Identifiable Records**

- DEL. CODE ANN. tit. 29 § 4713 (2008) - as a result of a conviction of certain offenses, the person shall have a biological sample taken by the Department of Correction for DNA (deoxyribonucleic acid) law enforcement identification purposes and inclusion in law enforcement identification databases.
- DEL. CODE ANN. tit. 11 § 9403 (2008) - Unless a victim or witness waives confidentiality in writing, neither a law-enforcement agency, the prosecutor, nor the corrections department may disclose, except among themselves or as authorized by law, the residential address, telephone number or place of employment of the victim or a member of the victim's family, or the identity, residential address, telephone number or place of employment of a witness or a member of the witness's family, except to the extent that disclosure is of the site of the crime, is required by law or the Rules of Criminal Procedure, is necessary for law-enforcement purposes, or is permitted by the court for good cause.
- DEL. CODE ANN. tit. 16 § 1006A (2008) Hospital Infections Disclosure Act. It is the express intent of the legislature that a patient's right of confidentiality shall not be violated in any manner. Patient Social Security numbers and any other information that could be used to identify an individual patient shall not be released notwithstanding any other provision of law.

- **Public Records**

- DEL. CODE ANN. tit. 29 § 10003 (2008) - Freedom of Information Act. All public records shall be open to inspection and copying by any citizen of the State during regular business hours by the custodian of the records for the appropriate public body. Reasonable access to and reasonable facilities for copying of these records shall not be denied to any citizen. If the record is in active use or in storage and, therefore, not available at the time a citizen requests access, the custodian shall so inform the citizen and make an appointment for said citizen to examine such records as expediently as they may be made available. Any reasonable expense involved in the copying of such records shall be levied as a charge on the citizen requesting such copy.
- DEL. CODE ANN. tit. 2 § 1328 (2008) - The Transportation Authority and its subsidiaries shall be subject to all applicable provisions of the state Freedom of Information Act. However, Written or recorded information concerning employee addresses, work sites, times of travel, salary and other information of a personal nature, having been provided or to be provided by employers working with the Department to develop transportation programs or projects, shall be treated as confidential and shall not be considered as a public record
- DEL. CODE ANN. tit. 9 § 1184 (2008) Public right of inspection of public records. Except that county records, the disclosure of which would invade a person's right of privacy, hinder law enforcement, endanger the public safety, or breach a legally recognized duty of confidence, or the nondisclosure of which is legally privileged, or which have been prepared for or by the County Attorney for use in actions or proceedings to which the County is or may be a party, shall not be available for public inspection.
- DEL. CODE ANN. tit. 29, § 10402 (2008) - Declares the policy of the Regulatory Flexibility Act and explains: Government information collection has not

adequately weighed the privacy rights of individuals and organizations against the government's need for information because the design of the regulatory process has encouraged regulators to treat information as a free good.

- DEL. CODE ANN. tit. 11, § 925 (2008) videotape distributor may not wrongfully disclose an individual or summary listing of any videotapes purchased or rented by a protected individual [anyone who could be harmed from disclosure] from the videotape distributor.
- DEL. CODE ANN. tit. 7, §§ 7902; 7903 (2008) - Environmental Permit Applications. All information provided under § 7902 is a public record unless it can be shown that disclosure would be an invasion of personal privacy. Confidential information shall not be released to the public or made part of the public record and shall only be released to law enforcement personnel performing the background investigation, authorized representatives of the office of the Attorney General, or sworn law enforcement personnel of other jurisdictions performing similar investigations on the applicant.
 - Applicants for, and holders of, permits to conduct stormwater management, NPDES, oil pollution liability, air, hazardous waste, solid waste, commercial subaqueous, wetlands, coastal zone, storage tank, extremely hazardous substances, hazardous substances cleanup and emergency planning and community right-to-know activities must submit certain information to the authority.
- DEL. CODE ANN. tit. 16, § 2005 (2008). Cancer incidence data. Notwithstanding any provisions in this title to the contrary, the agency shall make available as public records cancer incidence by census tract and by type of cancer. Such released data shall be assigned consensus tract geography from the most recent decennial census. If release of such information by census tract will explicitly or implicitly identify any individual, the agency may combine data among contiguous census tracts, but only insofar as is necessary to protect patient confidentiality.
- **Motor Vehicle Records**
 - DEL. CODE ANN. tit. 21, § 305 (2008). Privacy act governing the release of motor vehicle driving history and license records.
 - Division of Motor Vehicles and any officer, employee or contractor thereof or any other person shall not knowingly disclose or otherwise make available to any person or entity personal information about any individual obtained by the Division in connection with a motor vehicle record.
 - Only driver license and driver performance records which are 3 years old or less shall be made available to authorized persons or agencies, except persons requesting their own records, law enforcement officers, the courts and other motor vehicle jurisdictions may also have access to those records and to vehicle title and registration information which are over 3 years old and are being retained by the Division.
 - Division motor vehicle records can be transmitted to other motor vehicle jurisdictions electronically over authorized networks.

- A person may request to have certain personal information withheld even for some exceptions which include: For use in connection with the operation of private toll transportation facilities, by court order or proceeding, for motor vehicle emissions testing, for use in research activities and for use in producing statistical reports, so long as the personal information is not published, redisclosed or used to contact individuals.
 - DEL. CODE ANN. tit. 21 § 2616 (2008) - specifies limited entities to whom driving records information must be furnished including other state departments of transportation.
- **Vehicle Identification Numbers**
 - DEL. CODE ANN. tit 21, § 6407 (2008) - VIN must be included in written disclosure provided by the transferor of ownership of an vehicle.
 - DEL. CODE ANN. tit 21, § 6812 (2008) - special VIN for off highway vehicles.
- **Consumer Credit**
 - DEL. CODE ANN. tit 6, § 2201 through -2204 (2008) Clean Credit and Identity Theft Prevention Act. Permission for a consumer to request a credit freeze. "Security freeze" means a notice, at the request of the consumer and subject to certain exceptions that prohibits the consumer reporting agency from releasing all or any part of the consumer's credit report or any information derived from it without the express authorization of the consumer. If a security freeze is in place, such a report or information may not be released to a third party without prior express authorization from the consumer.
 - This chapter does not prevent a consumer reporting agency from advising a third party that a security freeze is in effect with respect to the consumer's credit report.
 - DEL. CODE ANN. tit. 11 § 914 (2008) as a condition of accepting a credit card as payment for consumer credit, goods, realty, or services, a person may not write down or request to be written down the address and/or telephone number of the credit card holder on the credit card transaction form. Can use for shipping purposes.
 - DEL. CODE ANN. tit. 11 § 915 (2008) - Use of credit card information. As a condition of accepting a check or other draft as payment for consumer credit, goods, realty or services, a person may not request or record the account number of any credit card of the drawer of the check or other draft. OK to show to prove credit worthiness.
- **Financial Records**
 - DEL. CODE ANN. tit. 5, § 125 (2008) - State Bank Commissioner may examine financial institution records as deemed necessary, but shall keep records and information confidential unless public duty requires otherwise.
- **Employee Privacy**
 - DEL. CODE ANN. tit. 19, § 705 (2008) Notice of monitoring of telephone transmissions, electronic mail, and Internet usage. No employer, nor any agent or any representative of any employer, shall monitor or otherwise intercept any telephone conversation or transmission, electronic mail or transmission, or Internet access or usage of or by a Delaware employee unless the employer

notifies the employee. BUT The provisions of this section shall not apply to processes that are designed to manage the type or volume of incoming or outgoing electronic mail or telephone voice mail or Internet usage, that are not targeted to monitor or intercept the electronic mail or telephone voice mail or Internet usage of a particular individual, and that are performed solely for the purpose of computer system maintenance and/or protection.

- DEL. CODE ANN. tit. 16. § 1146 (2008) Home Health Agencies. All applicants, as defined in § 1145 of this title, with the exception of self-employed healthcare givers seeking employment from a private individual to work in that capacity in a private residence on a private basis, shall submit to mandatory drug testing, as specified by regulations promulgated by DHSS. The requirement for drug tests for healthcare givers seeking employment in a private residence on a private basis is left to the discretion of the employer. Costs for such tests are borne by the employer or the applicant.
- DEL. CODE ANN. tit. 29 § 8922 (2008) - random, conditional and reasonable suspicion drug testing is required for department of corrections employees.
- DEL. CODE ANN. tit. 21 § 2708 (2008) - initial drug test required for all school bus drivers. Refusal to submit to testing, which shall include the provision of a substituted or adulterated test sample, shall be deemed to be a positive test result under this subsection.
- DEL. CODE ANN. tit. 29 § 6908 (2008) - Establish procedures through which all public works contracts, which are paid in whole or in part through public funds, include provisions requiring the contractor, its agents, and employees to implement a mandatory drug testing program for all employees or agents working on the job site in nonclerical positions. Provisions governing mandatory drug testing shall be incorporated into all public works contracts and the rules governing the administration of such tests by the contractor shall be promulgated by the Director pursuant to this subsection.
- *None of these statutes describe whether the drug testing information may be entered as evidence in a criminal proceeding or if the result is confidential.*
- DEL. CODE ANN. tit. 19, § 732 (2008) - employee shall upon request be permitted to inspect their own personnel files, at a reasonable time.
- DEL. CODE ANN. tit. 19, § 733 (2008) - does not require that employees be permitted to leave with or copy files.
- **Electronic Surveillance**
 - DEL. CODE ANN. tit. 11, § 1335 (2008) - Violation of privacy. Trespass on property or to install a device to subject anyone to eavesdropping or other surveillance in a private place. Also cannot unlawfully intercept messages or mail. Knowingly installs an electronic or mechanical location tracking device in or on a motor vehicle without the consent of the registered owner, lessor or lessee of said vehicle. This paragraph shall not apply to the lawful use of an electronic tracking device by a law enforcement officer, nor shall it apply to a parent or legal guardian who installs such a device for the purpose of tracking the location of a minor child thereof. Doesn't apply to third party lines, communication employees, police officers, or by an order of the court.

- DEL. CODE ANN. tit. 11, § 2401 (2008) Definitions. "Electronic communication" means any transfer of signs, signals, writing, images, sounds, data or intelligence of any electromagnetic, photoelectronic or photooptical system. However, "electronic communication" does not include: a. Any wire or oral communication; b. Any communication made through a tone-only paging device; or c. Any communication from a tracking device.
- DEL. CODE ANN. tit. 11, § 2402 (2008) Interception of communications generally; divulging contents of communications, violations of chapter. Intentionally intercept, disclose or use or endeavor to intercept, disclose, use or procure any other person to intercept or endeavor to intercept any wire, oral or electronic communication. BUT it is okay for an operator of a switchboard or an officer, employee or agent of a provider of wire or electronic communication service whose facilities are used in the transmission of wire or electronic communication to intercept, disclose or use such communication in the normal course of employment; law enforcement purposes is acceptable, and so is interception where one person is party to the interception or consents. Also acceptable to intercept radio communication from an authorized frequency.
- DEL. CODE ANN. tit. 11, § 2403 (2008) Manufacture, possession, or sale of intercepting device
- DEL. CODE ANN. tit. 11, § 2404 (2008) Admissibility of evidence
- DEL. CODE ANN. tit. 11, § 2405 (2008) Authorities permitted to apply for order authorizing interception
- DEL. CODE ANN. tit. 11, § 2406 (2008) Lawful disclosure or use of contents of communication
- DEL. CODE ANN. tit. 11, § 2407 (2008) Ex parte order authorizing interception
- DEL. CODE ANN. tit. 11, § 2408 (2008) Reports to President Judge of the Superior Court
- DEL. CODE ANN. tit. 11, § 2409 (2008) Civil liability; defense to civil or criminal action. Any person whose wire, oral or electronic communication is intercepted, disclosed or used in violation of this chapter shall have a civil cause of action against any person who intercepts, discloses, uses, or procures any other person to intercept, disclose or use the communications and be entitled to recover from any person. BUT A good faith reliance on a court order or legislative authorization shall constitute a complete defense to any civil or criminal action brought under this chapter or under any other law.
- **Computer Statutes**
 - DEL. CODE ANN. tit. 11, § 931 through § 941 (2008). Computer Offenses.
 - DEL. CODE ANN. tit. 11, § 932. Unauthorized access
 - DEL. CODE ANN. tit. 11, § 933. Theft of computer services
 - DEL. CODE ANN. tit. 11, § 934. Interruption of computer services
 - DEL. CODE ANN. tit. 11, § 935. Misuse of computer system information
 - DEL. CODE ANN. tit. 11, § 936. Destruction of computer equipment
 - DEL. CODE ANN. tit. 11, § 937. Unrequested or unauthorized electronic mail or use of network or software to cause same
 - DEL. CODE ANN. tit. 11, § 938. Failure to promptly cease electronic communication upon request

- DEL. CODE ANN. tit. 6, § 12B-101; -102 (2008). Computer security breaches. An individual or a commercial entity that conducts business in Delaware and that owns or licenses computerized data that includes personal information about a resident of Delaware shall, when it becomes aware of a breach of the security of the system, conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused. If the investigation determines that the misuse of information about a Delaware resident has occurred or is reasonably likely to occur, the individual or the commercial entity shall give notice as soon as possible to the affected Delaware resident.
 - "Breach of the security of the system" means the unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by an individual or a commercial entity. Good faith acquisition of personal information by an employee or agent of an individual or a commercial entity for the purposes of the individual or the commercial entity is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure;
- **Common Law**
 - **Appropriation**
 - Barbieri v. News Journal Co., 189 A.2d 773 (Del. 1963)
 - **Disclosure**
 - Martin v. Widener Univ. School of Law, No. 91C-03-255, 1992 Del. Super. LEXIS 267 (1992).
 - **False Light**
 - Wyshock v. Malekzadeh, No. 91C-09-22, 1992 Del. Super. LEXIS 247 (1992).
 - **Intrusion**
 - Barker v. Huang, 610 A.2d 1341 (Del. 1992).

DISTRICT OF COLUMBIA PRIVACY LAW

- **State Constitutional Privacy Rights**
 - N/A follows the United States Constitution
- **Search and Seizure**
 - N/A follows the United States Constitution
 - U.S. CONST. amend. IV. Unreasonable searches and seizures. The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.
 - **Auto Exception**
 - The District follows federal law.
 - California v. Acevedo, 500 U.S. 565 (1991).
 - **Open Fields**
 - The District follows federal law.
 - Florida v. Riley, 488 U.S. 445 (1989).
 - **Plain View**
 - The District follows federal law.
 - Kirk v. Louisiana, 536 U.S. 635 (2002).
- **Statutory Privacy Rights**
 - D.C. CODE ANN. § 22-404 (2009) - Any person who on more than one occasion engages in conduct with the intent to cause emotional distress to another person or places another person in reasonable fear of death or bodily injury by willfully, maliciously, and repeatedly following or harassing that person, or who, without a legal purpose, willfully, maliciously, and repeatedly follows or harasses another person, is guilty of the crime of stalking and shall be fined not more than \$ 500 or be imprisoned not more than 12 months, or both.
- **Individually Identifiable Records**
 - D.C. CODE ANN. § 46-226.03 (2009) Authority of IV-D agency to expedite paternity and support processes. Agency may take the following actions relating to paternity establishment or the establishment, modification, or enforcement of support orders without obtaining an order from any judicial or other administrative tribunal:
 - order paternity test
 - Issue an administrative subpoena to an individual or public or private entity (including a financial institution) for financial or other information needed to establish, modify, or enforce a support order, which may include information from a public utility or cable television company, that provides the name and address of a customer or a customer's employer
 - require a public or private entity to provide information on the employment status, number of hours worked, title, employment start date, employment termination date (if applicable), whether the employee ever quit voluntarily, location of work site, compensation, and benefits (including access to health insurance) of any employee of the entity, or of one of its contractors

- Obtain prompt access, including automated access, to information in the following records maintained or possessed by the District government, subject to any applicable privacy provisions under District or federal law including vital records, tax records, etc.
 - D.C. CODE ANN. § 28-3851 (2009) - Consumer Personal Information Security Breach Notification Act of 2006. Any entity that houses personal information must notify such persons as soon as possible if there is a security breach.
 - "Breach of the security of the system" means unauthorized acquisition of computerized or other electronic data, or any equipment or device storing such data, which compromises the security, confidentiality, or integrity of personal information maintained by the person or business.
 - The term "breach of the security system" shall not include a good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business if the personal information is not used improperly or subject to further unauthorized disclosure. Acquisition of data that has been rendered secure, so as to be unusable by an unauthorized third party, shall not be deemed to be a breach of the security of the system.
- **Public Records**
 - D.C. CODE ANN. § 2-531 et seq (2009) - Freedom of Information Act. The public policy of the District of Columbia is that all persons are entitled to full and complete information regarding the affairs of government and the official acts of those who represent them as public officials and employees. To that end, provisions of this subchapter shall be construed with the view toward expansion of public access and the minimization of costs and time delays to persons requesting information.
 - D.C. CODE ANN. § 2-532 (2009) - Any person has a right to inspect, and at his or her discretion, to copy any public record of a public body, except as otherwise expressly provided by § 2-534, in accordance with reasonable rules that shall be issued by a public body after notice and comment, concerning the time and place of access.
 - D.C. CODE ANN. § 2-534 (2009) – Exceptions include invasions of personal privacy, trade secrets and commercial or financial information, investigations for law enforcement purposes, discloses a confidential source, test questions for licensing, pending investigations by the fire marshall or attorney general.
 - D.C. CODE ANN. § 7-220 (2009) - Registrar shall issue a certified copy of all or part of a vital record in his or her custody to any applicant having a direct and tangible interest in the vital record. This includes the registrant, a member of his or her immediate family, his or her guardian, or their respective legal representatives shall be considered to have a direct and tangible interest. Others may demonstrate a direct and tangible interest when information is needed for determination or protection of a personal or property right.
 - D.C. CODE ANN. § 7-201 - "Vital records" means certificates or reports of birth, death, marriage, divorce, annulment, and data related thereto which is permitted to be gathered under this chapter.

- **Motor Vehicle Records**
 - D.C. CODE ANN. § 50-1301.05 (2009) - requires a certified abstract of any person's operating record to be furnished to any person upon request. Certain limitations apply.
 - D.C. CODE ANN. § 50-402 (2009). Uniform classification and commercial driver's license requirements. Randomly generated number or other information to identify the person. The Mayor shall not print the social security number of the person on the license, unless the person requests that their social security number be used as the identification number of the license. The Mayor shall require an applicant for a commercial driver's license to provide a social security number on the application, for the purposes of administering and enforcing the laws of the District of Columbia. Notwithstanding any other law, the social security number shall not be a matter of public record. The social security number shall be kept on file with the issuing agency and the applicant shall be so advised.
 - Wemhoff v. District of Columbia, 887 A.2d 1004 (D.C. 2005) - D.C. Code § 2-534(6) did not authorize the disclosure of personal information from motor vehicle records for the purpose of soliciting clients, as the Driver's Privacy Protection Act (DPPA), 18 U.S.C.S. § 2721 et seq., prohibited such disclosure and use; therefore an attorney was not entitled to information involving persons who were cited as a result of being photographed by a "red light camera" at a certain intersection under the District of Columbia Freedom of Information.
- **Vehicle Identification Numbers**
 - D.C. CODE ANN. § 50-2705 (2009) - An officer of the Metropolitan Police Department or other District of Columbia government employee deemed qualified by the Director shall physically inspect each vehicle for which an application for a scrap title has been submitted and notify the National Insurance Crime Bureau or other national organization identified by the Director that collects data on stolen vehicles of the vehicle identification numbers as part of an effort to verify the accuracy of the vehicle identification numbers of vehicles stored at privately owned tow truck storage lots and to determine whether a stolen vehicle record has been cleared.
 - D.C. CODE ANN. § 50-2421.06 (2009) - Except for vehicles removed after traffic accidents, the Department may, without further notice, dispose of a dangerous vehicle or abandoned vehicle removed from the public space or private property pursuant to any District law or regulation if the vehicle does not display a valid vehicle identification number and recognizable registration.
- **Consumer Credit**
 - D.C. CODE ANN. § 47-3152 (2009) - a credit card may not be required to be shown by the drawer of a check for any reason in connection with acceptance of a check.
 - D.C. CODE ANN. § 47-3153 (2009). Use of consumer identification information in connection with credit card payments. Can't request telephone number or address with the payment, unless necessary for delivery.
- **Financial Records**
 - D.C. CODE ANN. § 26-551.18 (2009) - Investigation, Examination, and Enforcement Powers Of the Commissioner in the Division of Banking.

Confidentiality of Information. Unlawful to disclose personal account information except that the contents of a report or examination of a person or information, including personal information, furnished to or obtained by the Department may be disclosed: (1) To employees, agents, and contractors of the Department in the performance of the duties of the employee, agent, or contractor; (2) To the directors, officers, and other persons authorized by the board of directors of a financial institution or other entity, if the financial institution or other entity furnished the information to the Department; (3) To authorized and appropriate government agencies; or (4) In accordance with a court order.

- **Employee Privacy**

- D.C. CODE ANN. § 1-601.02 (2009) - Merit Personnel System. Assuring, as provided in this chapter, fair treatment of applicants and employees in all aspects of employment without regard to political affiliation, race, color, national origin, sex, religious belief, age, marital status, personal physical appearance, sexual orientation, gender identity or expression, family responsibilities, physical disability, or developmental disability. A proper regard shall be accorded all rights of privacy and other constitutionally protected rights of citizens.
- D.C. CODE ANN. § 1-631.01 (2009) - All official personnel records of the District government shall be established, maintained, and disposed of in a manner designed to ensure the greatest degree of applicant or employee privacy while providing adequate, necessary, and complete information for the District to carry out its responsibilities under this chapter. Such records shall be established, maintained, and disposed of in accordance with rules and regulations issued by the Mayor.
- D.C. CODE ANN. § 32-902; 903 (2009) administering a lie detector test as a condition of employment is an unwarranted invasion of privacy.
 - No employer or prospective employer shall administer, accept or use the results of any lie detector test in connection with the employment, application or consideration of an individual, or have administered, inside the District of Columbia, any lie detector test to any employee, or, in or during any hiring procedure, to any person whose employment, as contemplated at the time of administration of the test, would take place in whole or in part in the District of Columbia.

- **Electronic Surveillance**

- D.C. CODE ANN. § 11-941 (2009) - Issuance of warrants; record. Judges of the Superior Court may, at any time, including Sundays and legal holidays, on complaint or application under oath or actual view, issue warrants for arrest, search or seizure, or electronic surveillance in connection with crimes and offenses committed within the District of Columbia, or for administrative inspections in connection with laws relating to the public health, safety, and welfare. Each proceeding respecting a warrant shall be recorded as prescribed by the court.
- D.C. CODE ANN. § 23-541 (2009) - the term "intercepting device" means any electronic, mechanical, or other device or apparatus which can be used to intercept a wire or oral communication.

- D.C. CODE ANN. § 23-542 (2009) - unlawful to willfully intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept any wire or oral communication. Acceptable for telecommunications employees in the course of their employment, law enforcement or under court order.
- **Computer Statutes**
 - none
- **Common Law**
 - Wolf v. Regardie, 553 A.2d 1213 (D.C. 1980) - D.C. recognizes all four strands for the invasion of privacy, as outlined in the restatement.

FLORIDA PRIVACY LAW

- **State Constitutional Privacy Rights**
 - **Express**
 - FLA. CONST. art. I, § 23 (2009) – Right of Privacy. Every natural person has the right to be let alone and free from governmental intrusion into the person's private life except as otherwise provided herein. This section shall not be construed to limit the public's right of access to public records and meetings as provided by law.
- **Search and Seizure**
 - FLA. CONST. art. I, § 12 (2009) – protection from unreasonable searches and seizures. Specifically states that this section shall be construed with the Fourth Amendment to the US Constitution.
 - State v. Fisher, 591 So.2d 1049 (Fla. Dist. Ct. App. 1991) The Court held that the garbage had not reasonable expectation of privacy and therefore was not protected by the Fourth Amendment.
 - Sarantopoulos v. State, 629 So.2d 121 (Fla. 1993) Defendant's conviction was affirmed because the search predicated on the officer's observations from adjacent private property was legal, even if defendant's property was surrounded by a fence and the officers were on the adjacent property without the owner's permission.
 - **Auto Exception**
 - State v. Hollingshead, 974 So. 2d 1123 (Fla. Dist. Ct. App. 1981).
 - **Open Fields**
 - State v. Brady, 406 So.2d 1093 (Fla. 1981).
 - **Plain View**
 - State v. Brady, 406 So.2d 1093 (Fla. 1981).
- **Statutory Privacy Rights**
 - FLA. STAT. ANN. § 784.048 (2009) - Any person who willfully, maliciously, and repeatedly follows, harasses, or cyberstalks another person commits the offense of stalking
 - "Credible threat" means a threat made with the intent to cause the person who is the target of the threat to reasonably fear for his or her safety. The threat must be against the life of, or a threat to cause bodily injury to, a person.
 - "Harass" means to engage in a course of conduct directed at a specific person that causes substantial emotional distress in such person and serves no legitimate purpose.
 - "Cyberstalk" means to engage in a course of conduct to communicate, or to cause to be communicated, words, images, or language by or through the use of electronic mail or electronic communication, directed at a specific person, causing substantial emotional distress to that person and serving no legitimate purpose.
 - FLA. STAT. ANN. 540.08 (2009) - codifies the common law tort of commercial appropriation.
- **Public Records**
 - FLA. STAT. ANN. § 119.105 (2009) - Police reports are public records except as otherwise made exempt or confidential. Every person is allowed to examine

- nonexempt or nonconfidential police reports. This section does not prohibit the publication of such information to the general public by any news media legally entitled to possess that information or the use of such information for any other data collection or analysis purposes by those entitled to possess that information.
- FLA. STAT. ANN. §§ 119.07(1) (2009) - shall permit the record to be inspected and copied by any person desiring to do so, but exceptions include FLA. STAT. ANN. § 119.071 (2009) - agency test questions for certifications, agency sealed bids or proposals, other agency materials prepared in response to litigation or adverse admin proceedings, criminal investigations, pending discrimination proceedings, security schematics of public buildings, social security numbers of current agency employees, home addresses, telephone numbers of current law enforcement officers and other public servants. In addition, agencies may not collect social security numbers without a legitimate, stated purpose.
 - Any information that would identify or help to locate a child who participates in government-sponsored recreation programs or camps or the parents or guardians of such child, including, but not limited to, the name, home address, telephone number, social security number, or photograph of the child; the names and locations of schools attended by such child; and the names, home addresses, and social security numbers of parents or guardians of such child is exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution. Information made exempt pursuant to this paragraph may be disclosed by court order upon a showing of good cause.
 - Biometric identification information held by an agency before, on, or after the effective date of this exemption is exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution.
 - This paragraph is subject to the Open Government Sunset Review Act in accordance with s. 119.15, and shall stand repealed on October 2, 2013, unless reviewed and saved from repeal through reenactment by the Legislature.
 - FLA. STAT. ANN. § 119.0711 (2009) – no inspection of records concerning allegations of employment discrimination by an agency that are still pending, any eminent domain proceedings cannot be inspected until the sale is complete
 - FLA. STAT. ANN. § 119.0712 (2009) – No inspection of Dept of Health records that contain personal information, no inspection of Dept of Motor Vehicle records that includes, but is not limited to, an individual's social security number, driver identification number or identification card number, name, address, telephone number, medical or disability information, and emergency contact information. For purposes of this subsection, personal information does not include information relating to vehicular crashes, driving violations, and driver's status. This information from the Dept of Motor Vehicles may be released for legitimate purposes including research activities and for use in producing statistical reports, so long as the personal information is not published, redisclosed, or used to contact individuals
 - FLA. STAT. ANN. § 119.0713 (2009) – local government audits cannot be inspected until they are finalized. Worknotes cannot be inspected. Local

government bids for purchasing property and discrimination complaints against the local government are not discoverable until finalized.

- FLA. STAT. ANN. § 1002.22 (2009) - every student has a right to privacy in his/her educational records. These are confidential records.
- FLA. STAT. ANN. § 668.6076 (2009) - Any agency, as defined in s. 119.011, or legislative entity that operates a website and uses electronic mail shall post the following statement in a conspicuous location on its website: Under Florida law, e-mail addresses are public records. If you do not want your e-mail address released in response to a public records request, do not send electronic mail to this entity. Instead, contact this office by phone or in writing.
- FLA. STAT. ANN. § 440.3851 (2009) - Worker's Compensation. The following records of the Florida Self-Insurers Guaranty Association, Incorporated, are confidential and exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution: (a) Claims files, until termination of all litigation and settlement of all claims arising out of the same accident. (b) Medical records that are part of a claims file and other information relating to the medical condition or medical status of a claimant. (c) Minutes of exempt portions of meetings, as provided in subsection (3), until termination of all litigation and settlement of all claims with regard to that claim.
- **Motor Vehicle Records**
 - FLA. STAT. ANN. § 319.17 (2009) The department shall maintain indexes of motor vehicles and mobile homes by name of owner, by title number, and by manufacturer's motor number or vehicle identification number. The department shall keep an electronic record of notices of liens and satisfactions thereof. Such indexes and records shall be open to the inspection of the public at all reasonable times, except as provided in chapter 119.
 - FLA. STAT. ANN. § 320.05 (2009) Upon receipt of an application for the registration of a motor vehicle, vessel, or mobile home, as herein provided for, the department shall register the motor vehicle, vessel, or mobile home under the distinctive number assigned to such motor vehicle, vessel, or mobile home by the department. Electronic registration records shall be open to the inspection of the public during business hours. Information on a motor vehicle or vessel registration may not be made available to a person unless the person requesting the information furnishes positive proof of identification.
 - FLA. STAT. ANN. § 316.066 (2009) Crash reports that reveal the identity, home or employment telephone number or home or employment address of, or other personal information concerning the parties involved in the crash and that are held by any agency that regularly receives or prepares information from or concerning the parties to motor vehicle crashes are confidential and exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution for a period of 60 days after the date the report is filed.
- **Vehicle Identification Numbers**
 - FLA. STAT. ANN. § 319.17 (2009) - index of VINs is a public record.
 - FLA. STAT. ANN. § 319.30 (2009) - unlawful to drive a vehicle without a VIN or sell a vehicle without a VIN. Exceptions apply.
 - FLA. STAT. ANN. § 319.33 (2009) - Offenses involving VINs

- FLA. STAT. ANN. § 320.02 (2009) - requires verification of VIN for all vehicles registered in the state.
- **Consumer Credit**
 - FLA. STAT. ANN. § 817.5681 (2009) - Any person who conducts business in this state and maintains computerized data in a system that includes personal information shall provide notice of any breach of the security of the system, following a determination of the breach, to any resident of this state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The notification shall be made without unreasonable delay, consistent with the legitimate needs of law enforcement but within 45 days
 - notification is not required if, after an appropriate investigation or after consultation with relevant federal, state, and local agencies responsible for law enforcement, the person reasonably determines that the breach has not and will not likely result in harm to the individuals whose personal information has been acquired and accessed. Such a determination must be documented in writing and the documentation must be maintained for 5 years.
 - FLA. STAT. ANN. § 501.005 (2009) - security freeze" means a notice placed in a consumer report that prohibits a consumer reporting agency, as defined in 15 U.S.C. s. 1681a(f), from releasing the consumer report, credit score, or any information contained within the consumer report to a third party without the express authorization of the consumer.
 - FLA. STAT. ANN. § 668.703 (2009) Anti-phishing Act. Person with an intent to engage in conduct involving the fraudulent use or possession of another person's identifying information may not represent oneself, directly or by implication, to be another person without the authority or approval of such other person through the use of a web page or Internet domain name and use that web page, Internet domain name, or a link to that web page or domain name or another site on the Internet to induce, request, or solicit a resident of this state to provide identifying information. Also cannot send email phishing for the same.
- **Financial Records**
 - FLA. STAT. ANN. § 655.059 (2009) The books and records of a financial institution are confidential and shall be made available for inspection and examination only: (a) To the office or its duly authorized representative; (b) To any person duly authorized to act for the financial institution; (c) To any federal or state instrumentality or agency authorized to inspect or examine the books and records of an insured financial institution; (d) With respect to an international banking corporation, to the home-country supervisor of the corporation; (e) As compelled by a court of competent jurisdiction
 - The books and records pertaining to the deposit accounts and loans of depositors, borrowers, members, and stockholders of any financial institution shall be kept confidential by the financial institution and its directors, officers, and employees and shall not be released except upon express authorization of the account holder as to her or his own accounts, loans, or voting rights.

- **Employee Privacy**

- FLA. STAT. ANN. § 440.101 (2009) Drug Free Workplace - an employer implements a drug-free workplace program in accordance with s. 440.102 which includes notice, education, and procedural requirements for testing for drugs and alcohol pursuant to law or to rules developed by the Agency for Health Care Administration
 - One time only, prior to testing, an employer shall give all employees and job applicants for employment a written policy statement that includes the protocol for testing
 - Except as otherwise provided in this subsection, all information, interviews, reports, statements, memoranda, and drug test results, written or otherwise, received or produced as a result of a drug-testing program are confidential and exempt from the provisions of s. 119.07(1) and s. 24(a), Art. I of the State Constitution, and may not be used or received in evidence, obtained in discovery, or disclosed in any public or private proceedings, except in accordance with this section or in determining compensability under this chapter.

- **Electronic Surveillance**

- FLA. STAT. ANN. § 934.01 (2009) - Legislative finding. To safeguard the privacy of innocent persons, the interception of wire or oral communications when none of the parties to the communication has consented to the interception should be allowed only when authorized by a court of competent jurisdiction and should remain under the control and supervision of the authorizing court. Interception of wire and oral communications should further be limited to certain major types of offenses and specific categories of crime with assurance that the interception is justified and that the information obtained thereby will not be misused.
- FLA. STAT. ANN. § 934.02 (2009) Definitions. "Wire communication" means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception including the use of such connection in a switching station furnished or operated by any person engaged in providing or operating such facilities for the transmission of intrastate, interstate, or foreign communications or communications affecting intrastate, interstate, or foreign commerce. "Oral communication" means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation and does not mean any public oral communication uttered at a public meeting or any electronic communication. "Intercept" means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device. "Electronic communication" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects intrastate, interstate, or foreign commerce, but does not include: (a) Any wire or oral communication; (b) Any communication made through a tone-only paging device; (c) Any communication from an electronic or mechanical device which permits the tracking of the movement of a

person or an object; or (d) Electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds.

- FLA. STAT. ANN. § 934.03 (2009) Interception and disclosure of wire, oral, or electronic communications prohibited. Exceptions include law enforcement, telecommunications carriers in the course of employment and by court order.
- FLA. STAT. ANN. § 934.04 (2009) Manufacture, distribution, or possession of wire, oral, or electronic communication intercepting devices prohibited
- FLA. STAT. ANN. § 934.05 (2009) Confiscation of wire, oral, or electronic communication intercepting devices
- FLA. STAT. ANN. § 934.06 (2009) Prohibition of use as evidence of intercepted wire or oral communications; exception. Whenever any wire or oral communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the state, or a political subdivision thereof, if the disclosure of that information would be in violation of this chapter. The prohibition of use as evidence provided in this section does not apply in cases of prosecution for criminal interception in violation of the provisions of this chapter.
- FLA. STAT. ANN. § 934.07 (2009) Authorization for interception of wire, oral, or electronic communications
- FLA. STAT. ANN. § 934.08 (2009) Authorization for disclosure and use of intercepted wire, oral, or electronic communications
- FLA. STAT. ANN. § 934.09 (2009) Procedure for interception of wire, oral, or electronic communications
- FLA. STAT. ANN. § 934.10 (2009) Civil remedies
- FLA. STAT. ANN. § 934.15 (2009) Situations in which law enforcement officer may order telephone line cut, rerouted, or diverted Et seq.
- FLA. STAT. ANN. § 934.22 (2009) - Voluntary disclosure of customer communications or records. Generally not disclosed, but there are exceptions including to law enforcement if the communication pertains to the commission of a crime or if there will be an emergency resulting in death or bodily damage.
- FLA. STAT. ANN. § 944.23 (2009) Comprehensive correctional master plan - one of the purposes of the plan is to assess the use of electronic surveillance in correctional facilities.
- FLA. STAT. ANN. § 944.31 (2009) - General prohibition for pen registers, except upon application by law enforcement. Law enforcement can be authorized to use such devices on emergency basis without court order. In any case, the register must be limited to not capture any more information than the recording or decoding of electronic or other impulses to the dialing, routing, addressing, and signaling information used in processing and transmitting wire or electronic communications provides. The contents of such recording may not be recorded.
- FLA. STAT. ANN. § 944.42 (2009) - An investigative or law enforcement officer may make application to a judge of competent jurisdiction for an order authorizing or approving the installation and use of a mobile tracking device.

- **Computer Statutes**
 - FLA. STAT. ANN. § 815.04 (2009) - Computer Crimes. Willfully or without authorization destroying, altering or destroying data or programs of a computer or computer system is a crime
 - Also data or programs that are trade secrets cannot be public records.
 - FLA. STAT. ANN. § 934.21 (2009) - unlawfully accessing or altering stored communications is crime.
- **Common Law**
 - **Appropriation**
 - The tort of commercial appropriation is FLA. STAT. ANN. 540.08 (2009).
 - Tyne v. Time Warner Entm't Co., 901 So. 2d 802 (Fla. 2005)
 - **Disclosure**
 - Fla. Dep't of Corr. v. Abril, 969 So. 2d 201 (Fla. 2007) - negligent disclosure of HIV test was actionable. Did not have to be intentionally disclosed.
 - **False Light**
 - Jews for Jesus, Inc. v. Rapp, 997 So. 2d 1098 (Fla. 2008) - recognizing that there are four strands to the invasion of privacy tort but explaining that Florida has not accepted all four explicitly yet. This case serves DENY acceptance of the false light tort.
 - **Intrusion**
 - Fla. Dep't of Corr. v. Abril, 969 So. 2d 201 (Fla. 2007) - not exactly held under the intrusion tort, but referenced. Unclear whether Florida will accept intrusion as a cause of action.

GEORGIA PRIVACY LAW

- **State Constitutional Privacy Rights**
 - None
- **Search and Seizure**
 - GA. CONST. art. I, § 1, para. XIII (2008) - The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures shall not be violated; and no warrant shall issue except upon probable cause supported by oath or affirmation particularly describing the place or places to be searched and the persons or things to be seized.
 - **Auto Exception**
 - State v. Menezes, 648 S.E.2d 741 (Ga. Ct. App. 2007) (citing State v. Lejeune, 576 S.E.2d 888 (Ga. 2003)). Recognizes the automobile exception to the warrant requirement. Under the “automobile exception” to the search warrant requirement, when a vehicle is being used on the highways and police officers have probable cause to search the vehicle for evidence of a crime, they may search the vehicle without first obtaining a warrant. Ready mobility and the diminished expectation of privacy in an automobile delineate the circumstances of a permissible warrantless search. When a vehicle is being used on the highways, or if it is readily capable of such use and is found stationary in a place not regularly used for residential purposes - temporary or otherwise - the two justifications for the vehicle exception come into play.
 - **Open Fields**
 - Morse v. State, 655 S.E.2d 217 (Ga. Ct. App. 2007). Recognizes open field’s doctrine, an exception to the warrant requirement. This case applied to a construction site, which did not have the expectancy of privacy.
 - **Plain View**
 - Fair v. State, 664 S.E.2d 227 (Ga. 2008). Recognizes the plain view doctrine, an exception to the warrant requirement. For evidence to be admissible under the plain view doctrine, the officer collecting the evidence must not have violated the Fourth Amendment in arriving at the place from which he or she sees the evidence. The incriminating nature of the object must be immediately apparent.
- **Statutory Privacy Rights**
 - GA. CODE. ANN. § 16-5-90 (2008) - Stalking. A person commits the offense of stalking when he or she follows, places under surveillance, or contacts another person at or about a place or places without the consent of the other person for the purpose of harassing and intimidating the other person. There must be established a pattern of harassing and intimidating behavior, and which serves no legitimate purpose. Includes any communication including without being limited to communication in person, by telephone, by mail, by broadcast, by computer, by computer network, or by any other electronic device; and the place or places that contact by telephone, mail, broadcast, computer, computer network, or any other electronic device. This Code section shall not be construed to require that an overt threat of death or bodily injury has been made.

- **Individually Identifiable Government Records**

- GA. CODE. ANN. § 20-2-740 (2008) – Annual Reports Boards of Education. The Department of Education shall conduct a study for each school year based upon the statistical data filed by local boards pursuant to this Code section for the purpose of determining trends in discipline. The department shall also utilize existing demographic data on school personnel as needed to establish trends in discipline. Nothing in this Code section shall be construed to authorize the public release of personally identifiable information regarding students or school personnel.
- GA. CODE. ANN. § 44-5-158 (2008) Revised Uniform Anatomical Gifts Act. Personally identifiable information on a donor registry about a donor or prospective donor may not be used or disclosed without the express consent of the donor, prospective donor, or person that made the anatomical gift for any purpose other than to determine, at or near death of the donor or prospective donor, whether the donor or prospective donor has made, amended, or revoked an anatomical gift; provided, however, this shall not preclude the use of aggregated demographic information for the purposes of annual reporting, research, or education.
- GA. CODE. ANN. § 10-1-393.8 (2008) - Protection from disclosure of an individual's social security number. Avoid publicly posting or unnecessarily using an individual's social security number.
 - Ga. Comp. R. & Regs. r. 590-6-1-.06 (2009) – The Georgia Archives will flag documents that are otherwise not confidential, but contain confidential elements (like social security numbers) for redacting those confidential elements.
- *See* GA. CODE. ANN. § 50-18-72 (2008) - All state officers and employees shall have a privilege to refuse to disclose the identity or personally identifiable information of any person participating in research on commercial, scientific, technical, medical, scholarly, or artistic issues conducted by the Department of Human Resources or a state institution of higher education whether sponsored by the institution alone or in conjunction with a governmental body or private entity. Personally identifiable information shall mean any information which if disclosed might reasonably reveal the identity of such person including but not limited to the person's name, address, and social security number.
- *See also* Computer Statutes, below.

- **Public Records**

- GA. CODE. ANN. § 49-4-14 (2008) - No person who obtains information by virtue of any regulation made pursuant to subsection (a) of this Code section shall use such information for commercial or political purposes.
- GA. CODE. ANN. § 50-8-39 (2008) - Accounting of funds by [regional developmental] centers. A center shall keep books of account reflecting all funds received, expended, and administered by the center which shall be independently audited at least once in each fiscal year during which a center functions. A copy of the report and of any comments made by the state auditor pursuant to paragraph (2) of subsection (c) of this Code section shall be maintained as a

public record for public inspection during the regular working hours at the principal office of the center.

- GA. CODE. ANN. § 50-18-70 through -102 (2008) - the term "public record" shall mean all documents, papers, letters, maps, books, tapes, photographs, computer based or generated information, or similar material prepared and maintained or received in the course of the operation of a public office or agency. "Public record" shall also mean such items received or maintained by a private person or entity on behalf of a public office or agency which are not otherwise subject to protection from disclosure. Public records shall be open for a personal inspection by any citizen of this state at a reasonable time and place; and those in charge of such records shall not refuse this privilege to any citizen.
- **Exceptions from public inspection** GA. CODE. ANN. § 50-18-72 (2008) – include records that are determined federally confidential, medical/health, law enforcement, motor vehicle accident reports (without specific need), government agency firing/hiring evaluations, certain agricultural or natural resources information, names, addresses, social security numbers, mother's maiden name, credit card information, records that would reveal personal information about public servants, probate court records regarding guardianships or conservatorships, trade secrets, financial information, records of the State Road and Tollway Authority which would reveal the financial accounts or travel history of any individual who is a motorist upon such toll project, records of the Metropolitan Atlanta Rapid Transit Authority or of any other transit system that is connected to that system's TransCard or SmartCard system which would reveal the financial records or travel history of any individual who is a purchaser of a TransCard or SmartCard or similar fare medium.
- **Motor Vehicle Records**
 - GA. CODE. ANN. § 40-3-23 (2008) - maintenance of record of certificates issued; public inspection. The commissioner is required to maintain motor vehicle records that include title numbers, vehicle identification numbers, names of the owners, etc. Not all of these records may be inspected by the public (there are exceptions for car dealers, finding owners of towed/impounded vehicles or tax collectors). BUT motor vehicle records consisting of vehicle description, title status, title brands, last recorded mileage, recorded liens, or recorded security interests can be inspected by the public.
 - Records furnished in accordance with this subsection may be subsequently transferred to third parties.
 - Personal information of any registrant, including name, address, date of birth, or driver's license or social security number, shall not be furnished or transferred by or to any person pursuant to this subsection.
 - Except as otherwise required in the federal Driver's Privacy Protection Act of 1994, 18 U.S.C. Chapter 123, personal information furnished under paragraphs (1), (2), and (3) of subsection (d) of this Code section shall be limited to the natural person's name, address, and driver identification number. The personal information obtained by a business under this Code section shall not be resold or redisclosed for any purposes other than those

- permitted under the federal Driver's Privacy Protection Act of 1994, 18 U.S.C. Chapter 123, without the written consent of the individual.
- GA. CODE. ANN. § 40-3-5 (2008) - Stolen, converted, and recovered vehicles. The commissioner shall maintain appropriately indexed weekly and cumulative public records of stolen, converted, and recovered vehicles reported to him pursuant to this Code section. The commissioner may make and distribute copies of the weekly records so maintained to peace officers upon request without fee and to others for the fee, if any, the commissioner prescribes.
 - GA. CODE. ANN. § 40-14-22 (2008) - Timing of traffic-control signals. Each governing authority using a traffic-control signal monitoring device shall at its own expense test the device for accuracy at regular intervals and record and maintain the results of each test. Such test results shall be public records subject to inspection as provided by Article 4 of Chapter 18 of Title 50.
 - GA. CODE. ANN. § 40-5-2 (2008) - Keeping of records of applications for licenses. The records maintained by the department on individual drivers are exempt from any law of this state requiring that such records be open for public inspection; provided, however, that initial arrest reports, incident reports, and the records pertaining to investigations or prosecutions of criminal or unlawful activity shall be subject to disclosure pursuant to paragraph (4) of subsection (a) of Code Section 50-18-72 and related provisions.
 - Georgia Uniform Motor Vehicle Accident Reports shall be subject to disclosure pursuant to paragraph (4.1) of subsection (a) of Code Section 50-18-72. The department shall not make records or personal information available on any driver except as otherwise provided in this Code section or as otherwise specifically required by 18 U.S.C. Section 2721.
 - The department is specifically authorized to disseminate the following records and information: To the Department of Human Resources, compilations of the names, dates of birth, and most current addresses of licensees or applicants for licenses. Any information provided pursuant to this subsection shall only be used by the Department of Human Resources in connection with the recovery of delinquent child support payments under Article 1 of Chapter 11 of Title 19, known as the "Child Support Recovery Act.
 - It shall be unlawful to disclose, distribute, or sell such records or information to an unauthorized recipient or for an unauthorized purpose. It shall be a violation of this Code section to make a misrepresentation or false statement in order to obtain access to or information from the department's records.
 - GA. CODE. ANN. § 40-5-71 (2008) - Notice of insurance issuance. The minimum liability insurance records which the department is required to maintain under this Code section or any other provision are exempt from the provisions of any law of this state requiring that such records be open for public inspection; provided, however, that the records of any particular motor vehicle may be available for inspection by any law enforcement officer for official law enforcement investigations, the insurer of record, and the owner of the vehicle in the manner prescribed by the commissioner

- GA. CODE. ANN. § 40-13-27 (2008) - A written record is required to be kept of every case made or disposed of under this article [prosecution of traffic violations]. Such record shall be accessible at all times for public inspection and official audit and shall be kept and remain as a part of the permanent records of the court.
 - Under § 40-13-27, municipal traffic records must be accessible for public inspection. 1982 Op. Att'y Gen. No. U82-36.
- GA. CODE. ANN. § 40-2-130 (2008) - Records of certificates of registration. The motor vehicle registration records which the commissioner is required to maintain under this Code section or any other provision are exempt from the provisions of any law of this state requiring that such records be open for public inspection; however, any private person who has met the requirements of Code Section 40-2-25, provided that the information shall be used for the sole purpose of effectuating the registration or renewal of motor vehicles by electronic or similar means, may inspect the following parts of the record: vehicle identification number, the license tag number, the date of expiration of registration, and the amount of tax owed.
- **Vehicle Identification Numbers**
 - GA. CODE. ANN. § 16-8-83 through -84 (2008) - Any person who knowingly alters, counterfeits, defaces, destroys, disguises, falsifies, forges, obliterates, or removes a vehicle identification number with the intent to misrepresent the identity or prevent the identification of a motor vehicle or motor vehicle part shall be guilty of a felony.
 - GA. CODE. ANN. § 40-2-26 (2008) – applications to register a vehicle must include the vehicle identification number. It also states the name, place of residence, and address of the applicant; a brief description of the vehicle to be registered, including its name and model, the name of the manufacturer, the manufacturer's vehicle identification number, and its shipping weight and carrying capacity; from whom, where, and when the vehicle was purchased; the total amount of all liens, if any, thereon, with the name and address of the lien holder; and such other information as the commissioner may require.
 - *See also* GA. CODE. ANN. § 40-2-130 (2008) and GA. CODE. ANN. § 40-3-23 (2008) under motor vehicle records.
- **Consumer Credit**
 - GA. CODE. ANN. § 33-39-8 (2008) – Investigative Consumer Report. No insurance institution, agent, or insurance-support organization may prepare or request an investigative consumer report about an individual in connection with an insurance transaction involving an application for insurance, a policy renewal, a policy reinstatement, or a change in insurance benefits unless the insurance institution or agent informs the individual.
 - GA. CODE. ANN. § 33-39-9 through -10 (2008) - Access to recorded personal information from an insurance institution or agent and the ability to amend or edit such information.
 - GA. CODE. ANN. § 33-39-14 (2008) - An insurance institution, agent, or insurance-support organization shall not disclose any personal or privileged information about an individual collected or received in connection with an

insurance transaction unless the disclosure is: with the written authorization of the individual, or is reasonably necessary for law enforcement, a medical institution or another insurance company to complete a transaction.

- GA. CODE. ANN. § 10-1-910 through -915 (2008) – Identity Theft. Any information broker or data collector that maintains computerized data that includes personal information of individuals shall give notice of any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of this state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
- **Financial Records**
 - *See generally*, public records and computer statutes, above.
- **Employee Privacy**
 - Hall v. State, 574 S.E.2d 610 (Ga. App. 2002) - explicitly held that an employee, lacking a possessory interest in his or her place of employment, has no expectation of privacy in the employer's premises under the Fourth Amendment.
 - Braddock v. State, 194 S.E.2d 317 (Ga. App. 1972) - Holding that the driver of a commercial truck, who was employed by the truck owner, had no reasonable expectation of privacy, under the Fourth Amendment, in the truck's glove compartment, which a federal safety inspector searched. The truck's owner had the authority to consent to the search of the glovebox where the inspector found amphetamines. The employee could not reasonably think of the truck as a personal, private place.
 - GA. CODE. ANN. § 34-9-413 (2008) - Drug-Free Workplace Programs In addition to the requirements of subsection (a) of this Code section, a drug-free workplace program must be implemented in compliance with the confidentiality standards provided in Code Section 34-9-420.
- **Electronic Surveillance**
 - GA. CODE. ANN. § 16-11-60 (2008) - "Device" means an instrument or apparatus used for overhearing, recording, intercepting, or transmitting sounds or for observing, photographing, videotaping, recording, or transmitting visual images and which involves in its operation electricity, electronics, or infrared, laser, or similar beams. Without limiting the generality of the foregoing, the term "device" shall specifically include any camera, photographic equipment, video equipment, or other similar equipment or any electronic, mechanical, or other apparatus which can be used to intercept a wire, oral, or electronic communication.
 - "Trap and trace device" means a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication; provided, however, that such information shall not include the contents of any communication.
 - GA. CODE. ANN. § 16-11-62 (2008) - Eavesdropping, surveillance, or intercepting communication which invades privacy of another. Any person, through the use of any device, without the consent of all persons observed, to observe, photograph, or record the activities of another which occur in any private place and out of

public view. However, there are exceptions for jails, for security purposes, crime prevention, or crime detection (for curtilage or places where there is not expectation of privacy).

- GA. CODE. ANN. § 16-11-64 through -65 (2008) – gives law enforcement officers the ability to use pen registers, trip and trap and other devices for surveillance in the effort to carry out their law enforcement duties, but only with the appropriate warrant or in certain emergency situations.
- GA. CODE. ANN. § 16-11-66 (2008) - Interception of wire, oral, or electronic communication by party thereto. Nothing in Code Section 16-11-62 shall prohibit a person from intercepting a wire, oral, or electronic communication where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception.
- GA. CODE. ANN. § 40-6-20 (2008) - Enforcement by traffic-control signal monitoring devices.
 - "Recorded images" means images recorded by a traffic-control signal monitoring device: (i) On: (I) Two or more photographs; (II) Two or more microphotographs; (III) Two or more electronic images; OR (IV) Videotape; and (ii) Showing a traffic-control signal displaying a CIRCULAR RED or RED ARROW signal along with the rear of a motor vehicle apparently operated in disregard or disobedience of such signal and, on at least one image or portion of tape, clearly revealing the number or other identifying designation of the license plate displayed on the motor vehicle.
 - "Traffic-control signal monitoring device" means a device with one or more motor vehicle sensors working in conjunction with a traffic-control signal to produce recorded images of motor vehicles being operated in disregard or disobedience of a CIRCULAR RED or RED ARROW signal.
 - Recorded images made for purposes of this subsection shall not be a public record for purposes of Article 4 of Chapter 18 of Title 50.
- **Computer Statutes**
 - GA. CODE. ANN. § 16-9-150 through -157 (2008) - Georgia Computer Security Act of 2005. Prohibitions against spyware, email virus distribution and other computer hijackings. Specifically makes illegal the collection, through intentionally deceptive means, personally identifiable information including keystroke-logging function or recording all websites visited. Also prohibits software from being installed without a user's knowledge or automatically reinstalling itself after the user uninstalls the program, or software that disables an antivirus/spyware program.
 - Nothing in this Code section shall apply to any monitoring of, or interaction with, a user's Internet or other network connection or service, or a protected computer, by a telecommunications carrier, cable operator, computer hardware or software provider, or provider of information service or interactive computer service.
 - GA. CODE. ANN. § 16-9-90 through -97 (2008) - Georgia Computer Systems Protection Act. Computer Invasion of Privacy. Any person who uses a computer or computer network with the intention of examining any employment, medical,

salary, credit, or any other financial or personal data relating to any other person with knowledge that such examination is without authority shall be guilty of the crime of computer invasion of privacy. Computer theft, computer trespass are two other crimes under this code section. There has to be intent to access the computer for nefarious means.

- **Common Law**

- Thomas v. Food Lion, 570 S.E.2d 18, 883 (Ga. Ct. App. 2002) - An invasion of privacy claim must fall within one of the following four categories: (1) intrusion upon the plaintiff's seclusion or solitude, or into his private affairs, (2) public disclosure of embarrassing facts about the plaintiff, (3) publicity which places the plaintiff in a false light in the public eye, or (4) appropriation of the plaintiff's name or likeness for the defendant's advantage.

HAWAII PRIVACY LAW

- **State Constitutional Privacy Rights**
 - **Express**
 - HAW. CONST. art. I, § 6 (2008) - Right To Privacy. The right of the people to privacy is recognized and shall not be infringed without the showing of a compelling state interest. The legislature shall take affirmative steps to implement this right.
 - HAW. CONST. art. I, § 7 (2008) - The right of the people to be secure in their persons, houses, papers and effects against unreasonable searches, seizures and invasions of privacy shall not be violated; and no warrants shall issue but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched and the persons or things to be seized or the communications sought to be intercepted.
- **Search and Seizure**
 - HAW. CONST. art. I, § 7 (2008) - prohibits search and seizure and invasions of privacy
 - State v. Kender, 588 P.2d 447 (Haw. 1978) - Extraordinary measures - climbing fence, using binoculars - constitute a search where a person has a reasonable expectation of privacy.
 - State v. Wong, 708 P.2d 825 (Haw. 1985) - using binoculars to observe the inside of a car is not a search if it was in a public parking lot.
 - **Auto Exception**
 - **Open Fields**
 - State v. Stachler, 570 P.2d 1323 (Haw. 1977).
 - **Plain View**
 - State v. Delmondo, 512 P.2d 551 (Haw. 1973).
- **Statutory Privacy Rights**
 - HAW. REV. STAT. § 711-1106.5 (2008) - person commits the offense of harassment by stalking if, with intent to harass, annoy, or alarm another person, or in reckless disregard of the risk thereof, that person engages in a course of conduct involving pursuit, surveillance, or non-consensual contact upon the other person on more than one occasion without legitimate purpose.
 - HAW. REV. STAT. § 711-1110.9 (2008) - A person commits the offense of violation of privacy in the first degree if, except in the execution of a public duty or as authorized by law, the person intentionally or knowingly installs or uses, or both, in any private place, without consent of the person or persons entitled to privacy therein, any device for observing, recording, amplifying, or broadcasting another person in a stage of undress or sexual activity in that place.
 - A person commits the offense of violation of privacy in the second degree if, except in the execution of a public duty or as authorized by law, the person intentionally:
 - Trespasses on property for the purpose of subjecting anyone to eavesdropping or other surveillance in a private place;
 - Peers or peeps into a window or other opening of a dwelling with a lewd or unlawful purpose, under circumstances in which a reasonable person in the dwelling or other structure would not expect to be observed;

- Installs or uses, or both, in any private place, without consent of the person or persons entitled to privacy therein, any means or device for observing, recording, amplifying, or broadcasting sounds or events in that place,
 - Installs or uses outside a private place any device for hearing, recording, amplifying, or broadcasting sounds originating in that place which would not ordinarily be audible or comprehensible outside, without the consent of the person or persons entitled to privacy therein;
Intercepts, without the consent of the sender or receiver, a message or photographic image by telephone, telegraph, letter, electronic transmission, or other means of communicating privately
 - BUT does not apply to any dissemination, distribution, or transfer of images subject to this section by an electronic communication service provider or remote storage service in the ordinary course of its business.
 - HAW. REV. STAT § 711-1111 (2008). Violation of privacy in the second degree. (1) A person commits the offense of violation of privacy in the second degree if, except in the execution of a public duty or as authorized by law, the person intentionally: (a) Trespasses on property for the purpose of subjecting anyone to eavesdropping or other surveillance in a private place; (b) Peers or peeps into a window or other opening of a dwelling or other structure adapted for sojourn or overnight accommodations for the purpose of spying on the occupant thereof or invading the privacy of another person with a lewd or unlawful purpose, under circumstances in which a reasonable person in the dwelling or other structure would not expect to be observed; (c) Trespasses on property for the sexual gratification of the actor; or (d) records without consent individuals where they have an expectation of privacy; (e) intercepts transmissions; (f) disclosing information improperly intercepted.
- **Individually Identifiable Records**
 - HAW. REV. STAT. § 846-35 (2008) Information obtained for civil identification cards is confidential.
 - HAW. REV. STAT. § 846-7 (2008) - direct access to criminal history record information is to be available only to authorized officers or employees of a criminal justice agency and, as necessary, other authorized personnel essential to the proper operation of the criminal history record information system.
 - BUT Nothing in this chapter shall prevent a criminal justice agency from disclosing, to the public, criminal history record information related to the offense for which an individual is currently within the criminal justice system, including the individual's place of incarceration; and, nothing in this chapter shall prevent a criminal justice agency from confirming prior criminal history record information to members of the news media or any other person, upon specific inquiry as to whether a named individual was arrested, detained, indicted, or other formal charge was filed, on a specific date, if the arrest record information or criminal history record information disclosed is based on data excluded by the first paragraph of this section. Nothing in this chapter prohibits the dissemination of criminal history

- record information for purposes of international travel, such as issuing visas and granting of citizenship.
 - HAW. REV. STAT. § 487N-1 through -7(2008) Notification of Security Breaches for entities who maintain databases with personal information.
 - "Security breach" means an incident of unauthorized access to and acquisition of unencrypted or unredacted records or data containing personal information where illegal use of the personal information has occurred, or is reasonably likely to occur and that creates a risk of harm to a person. Any incident of unauthorized access to and acquisition of encrypted records or data containing personal information along with the confidential process or key constitutes a security breach.
 - Good faith acquisition of personal information by an employee or agent of the business for a legitimate purpose is not a security breach; provided that the personal information is not used for a purpose other than a lawful purpose of the business and is not subject to further unauthorized disclosure.
 - HAW. REV. STAT. §§ 487J-1 through -5 (2008) Social Security Protection. Effective July 1, 2009. Applies to businesses and government agencies and states that they may not print social security numbers on any licenses, cards, or receipts. Requesting the number over the internet requires encryption and secure connection.
- **Public Records**
 - HAW. REV. STAT. § 92F-11 (2008) - All government records are open except if disclosure is prohibited by law.
 - HAW. REV. STAT. § 92F-13 (2008) Government records which, if disclosed, would constitute a clearly unwarranted invasion of personal privacy may not be disclosed.
 - HAW. REV. STAT. § 92F-14 (2008) Significant privacy interest; examples include medical records or eligibility for social security or welfare.
 - HAW. REV. STAT. § 92F-22 (2008) - criminal records are private.
- **Motor Vehicle Records**
 - HAW. REV. STAT. § 846-8 (2008) - police blotters, court records, records of traffic offenses maintained for licensing are public.
- **Vehicle Identification Numbers**
 - State v. Moore, 659 P.2d 70 (Haw. 1983) - can inspect VIN only if there is reasonable suspicion.
 - *See also*, State v. Agnasan, 614 P.2d 393 (Haw. 1980) - lifting hood to inspect VIN is a search and therefore requires probable cause.
 - HAW. REV. STAT. § 286-44 (2008) - unlawful to possess a vehicle with a damaged VIN or to alter the VIN
- **Consumer Credit**
 - HAW. REV. STAT. § 708-8105 (2008) - illegal to sell the names of credit card holders without their consent.
 - HAW. REV. STAT. § 489P-1 through -6 (2008) -permits security freeze by consumers to prevent further identity theft.

- **Financial Records**
 - HAW. REV. STAT. § 412:2-603. Disclosures of records of Hawaii financial institutions. Any institution-affiliated party who, without authorization, knowingly discloses, except in the regular course of business, any information derived from a Hawaii financial institution's records shall be guilty of a misdemeanor punishable pursuant to sections 706-663 and 706-640.
- **Employee Privacy**
 - State v. Bonnell, 856 P.2d 1265 (Haw. 1993) - installing a video camera in an employee break room breaches a reasonable expectation of privacy.
 - HAW. REV. STAT. § 329B-1 through -5.5 (2008) The purpose of this chapter is to ensure that appropriate and uniform substance abuse test procedures are employed throughout the State, to protect the privacy rights of persons tested, and to achieve reliable and accurate results. Results are confidential.
- **Electronic Surveillance**
 - HAW. REV. STAT. § 803-41 (2008) Definitions. "Electronic communication" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photo-optical system that affects intrastate, interstate, or foreign commerce. The term "electronic communication" includes, but is not limited to, "display pagers" which can display visual message as part of the paging process, but does not include: **(1)** Any wire or oral communication; **(2)** Any communication made through a tone-only paging device; **(3)** Any communication from a tracking device; or **(4)** Electronic funds transfer information stored by financial institution in a communications system used for the electronic storage and transfer of funds.
 - HAW. REV. STAT. § 803-42 Interception, access, and disclosure of wire, oral, or electronic communications, use of pen register, trap and trace device, and mobile tracking device prohibited. Exceptions for telecommunications employees in the course of employment to intercept, FCC employees, one party to the communication consents, court ordered interception or assistance to the court order, or public available frequency or wavelength
 - Note that a person or entity providing electronic communication service to the public may divulge the contents of any such communication: **(A)** As otherwise authorized by a court order or under this part; **(B)** With the lawful consent of the originator, addressee, or intended recipient of the communication; **(C)** To a person employed or authorized, or whose facilities are used, to forward the communication to its destination; or **(D)** That was inadvertently obtained by the service provider and that appears to pertain to the commission of a crime, if divulged to a law enforcement agency.
 - HAW. REV. STAT. § 803-43 Devices to intercept wire, oral, or electronic communications and advertising of same prohibited; penalty; forfeiture
 - HAW. REV. STAT. § 803-44 Application for court order to intercept wire, oral, or electronic communications
 - HAW. REV. STAT. § 803-44.5 Application. pen register or a trap and trace device

- HAW. REV. STAT. § 803-44.6 Issuance of an order for a pen register or a trap and trace device
- HAW. REV. STAT. § 803-44.7 Application for authorization to install and use a mobile tracking device. A search warrant or court order must be obtained to install such a device. The warrant can't exceed 60 days.
- HAW. REV. STAT. § 803-45 (2008) Authorization for disclosure and use of intercepted wire, oral, or electronic communications
- HAW. REV. STAT. § 803-46 (2008) Procedure for interception of wire, oral, or electronic communication. Only granted for investigations of (A) Murder; (B) Kidnapping; (C) Felony criminal property damage involving the danger of bodily injury; (D) Distribution of dangerous, harmful or detrimental drugs; or (E) Conspiracy to commit one or more of the above. Within 90 days the person intercepted needs to be informed of the interception.
- HAW. REV. STAT. § 803-47 (2008) Reports concerning intercepted wire, oral, or electronic communications. The attorney general and related departments has to report the total number of interceptions and the total number of applications granted and denied.
- **Computer Statutes**
 - HAW. REV. STAT. § 708-891 (2008) person commits the offense of computer fraud in the first degree if the person knowingly, and with intent to defraud, accesses a computer without authorization and, by means of such conduct, obtains or exerts control over the property of another
 - HAW. REV. STAT. § 708-892 (2008) computer damage. Unauthorized access, use or damage is unlawful.
- **Common Law**
 - Mehau v. Reed, 869 P.2d 1320 (Haw. 1994) - accepts the four strands of the common cause of action for an invasion of privacy.

IDAHO PRIVACY LAW

- **State Constitutional Privacy Rights**
 - **Express** - none
 - **Implied**
 - State v. Limberhand, 788 P.2d 857 (Idaho Ct. App. 1990) - Once it is resolved that there is a cognizable expectation of privacy, the invasion of that privacy interest, including a visual one, will be a search subject to constitutional requirements.
- **Search and Seizure**
 - IDAHO CONST. art. I, § 17 - protects against unreasonable search and seizure.
 - **Auto Exception**
 - State v. Yeoumans, 172 P.3d 1146 (Idaho Ct. App. 2007).
 - **Open Fields**
 - State v. Young, 691 P.2d 1286 (Idaho Ct. App. 1984).
 - **Plain View**
 - State v. Limberhand, 788 P.2d 857 (Idaho Ct. App. 1990).
- **Statutory Privacy Rights**
 - IDAHO CODE ANN. § 6-702 (2008) - No person shall have more than one (1) cause of action for damages for libel or slander or invasion of privacy or any other tort founded upon any single publication or exhibition or utterance.
 - IDAHO CODE ANN. § 18-7905 (2008) - person commits the crime of stalking in the second degree if the person knowingly and maliciously: (a) Engages in a course of conduct that seriously alarms, annoys or harasses the victim and is such as would cause a reasonable person substantial emotional distress; OR (b) Engages in a course of conduct such as would cause a reasonable person to be in fear of death or physical injury, or in fear of the death or physical injury of a family or household member. "Nonconsensual contact" includes, but is not limited to: Following the victim or maintaining surveillance, including by electronic means, on the victim.
 - IDAHO CODE ANN. (2008) - The Idaho DNA Database Act of 1996. Any person, including any juvenile tried as an adult, who is convicted of, or pleads guilty to, any of the following crimes, regardless of the form of judgment or withheld judgment, and regardless of the sentence imposed or disposition rendered, shall be required to provide to the Idaho state police, a DNA sample and a right thumbprint impression. Includes 61 crimes including stalking.
 - IDAHO CODE ANN. § 28-52-108 (2008) Protection of personal information. Except as otherwise specifically provided by law, a person shall not intentionally communicate an individual's social security number to the general public.
- **Public Records**
 - IDAHO CODE ANN. § 9-337 through -350 (2008) - Every person has a right to examine and take a copy of any public record of this state and there is a presumption that all public records in Idaho are open at all reasonable times for inspection except as otherwise expressly provided by statute.
 - Exceptions – include law enforcement records, investigatory records of agencies, court files of judicial proceedings (working memoranda), personal records (motor vehicle records, health records, etc), trade secrets,

appraisals, bids, records relating to the uniform securities act, archeological, endangered species, libraries, licensing exams, draft legislation, specific personnel information relating to public officials.

- IDAHO CODE ANN. § 9-341 (2008) - Nonexempt information contained within exempt records, upon request will be separated and made available for disclosure.
- IDAHO CODE ANN. § 9-342 (2008) - A person may inspect and copy the records of a public agency or independent public body corporate and politic pertaining to that person, even if the record is otherwise exempt from public disclosure.
- IDAHO CODE ANN. § 9-348 (2008) - The distribution or sale of mailing addresses or telephone numbers by a state agency is prohibited, unless consent of those on the list is given. Certain exceptions apply.
- **Motor Vehicle Records**
 - IDAHO CODE ANN. § 49-517 (2008) - The state is allowed to create an electronic record of the certificate of title where there is a lien to be recorded.
 - IDAHO CODE ANN. § 49-202 (2008) - All registration and driver's license records in the office of the department shall be public records and open to inspection by the public during normal business hours, except for those records declared by law to be for the confidential use of the department, or those records containing personal information subject to restrictions or conditions regarding disclosure.
 - IDAHO CODE ANN. § 49-203 (2008) - Prohibition on release and use of personal information contained in motor vehicle and driver records, but for some exceptions including consent of the driver, matters of motor vehicle or driver safety and theft, motor vehicle emissions, motor vehicle product alterations, recalls or advisories, performance monitoring of motor vehicles and dealers by motor vehicle manufacturers, and removal of nonowner records from the original owner
- **Vehicle Identification Numbers**
 - IDAHO CODE ANN. § 49-1418 (2008) - Any peace officer or authorized transportation department employee, with or without a warrant, may seize and take possession of any vehicle, trailer, semitrailer, vessel, vessel motor or implement of husbandry, or any part or parts thereof, which the peace officer or authorized employee has probable cause to believe is stolen, or on which any motor number, manufacturer's number, or identification number has been defaced, altered, removed, covered, destroyed or obliterated.
 - IDAHO CODE ANN. § 49-1418 (2008) - Ports of entry or checking stations established -- Motor vehicle investigator activities. Acceptable to set up a road block for investigators to check VIN numbers.
- **Consumer Credit**
 - IDAHO CODE ANN. § 28-52-101 through -107 (2008). Credit Report Protection Act. Allows individuals to place a security freeze on their credit accounts.
 - IDAHO CODE ANN. § 28-51-105 (2008). Disclosure of breach of security of computerized personal information by an agency, individual or a commercial entity. An agency, individual or a commercial entity that conducts business in Idaho and that owns or licenses computerized data that includes personal information about a resident of Idaho shall, when it becomes aware of a breach of the security of the system, conduct in good faith a reasonable and prompt

investigation to determine the likelihood that personal information has been or will be misused. If the investigation determines that the misuse of information about an Idaho resident has occurred or is reasonably likely to occur, the agency, individual or the commercial entity shall give notice as soon as possible to the affected Idaho resident. Notice must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine the scope of the breach, to identify the individuals affected, and to restore the reasonable integrity of the computerized data system.

- **Financial Records**

- IDAHO CODE ANN. § 26-1111 (2008) Banks and Banking. Records not public. The department of finance shall keep proper books and records of all regulatory acts, matters and things done by it under these provisions. Certain communications between the Dept of finance and the institution relating to regulations shall not be made available for disclosure.
- IDAHO CODE ANN. § 26-1112 (2008) - Confidential. Neither the department of finance, its director nor its employees shall disclose to any person or agency any fact or information obtained in the course of business of the department under this act, exceptions including if the dept is directed by law or a criminal proceeding to provide such information
- IDAHO CODE ANN. § 9-340C (2008) Personal bank records compiled by a public depositor for the purpose of public funds transactions conducted pursuant to law are exempt from public disclosure

- **Employee Privacy**

- Idaho Code § 72-1701 through -1717 (2008) - The purpose of this act is to promote alcohol and drug-free workplaces and otherwise support employers in their efforts to eliminate substance abuse in the workplace, and thereby enhance workplace safety and increase productivity. This act establishes voluntary drug and alcohol testing guidelines for employers that, when complied with, will find an employee who tests positive for drugs or alcohol at fault, and will constitute misconduct under the employment security law and result in a denial of unemployment benefits.
 - All information, interviews, reports, statements, memoranda or test results, written or otherwise, received through a substance abuse testing program shall be kept confidential, and are intended to be used only for an employer's internal business use; or in a proceeding related to any action taken by or against an employer

- **Electronic Surveillance**

- IDAHO CODE ANN. § 18-6701 (2008) Definitions. "Electronic communication" means any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system, but does not include: (a) Any wire or oral communication; (b) Any communication made through a tone-only paging device; (c) Any communication from a tracking device, as defined in 18 U.S.C. section 3117; or (d) Electronic fund transfer information stored by a financial

institution in a communications system used for the electronic storage and transfer of funds.

- IDAHO CODE ANN. § 18-6702 (2008) Interception and disclosure of wire, electronic or oral communications prohibited. Willfully intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept any wire, electronic or oral communication. Exceptions for telecommunications and FCC employees acting within the scope of employment, and law enforcement officers under a court order
- IDAHO CODE ANN. § 18-6703 (2008) Manufacture, distribution, possession, and advertising of wire, electronic or oral communication intercepting devices prohibited
- IDAHO CODE ANN. § 18-6704 (2008) Confiscation of wire, electronic or oral communication intercepting devices
- IDAHO CODE ANN. § 18-6705 (2008) Prohibition of use as evidence of intercepted wire, electronic or oral communications
- IDAHO CODE ANN. § 18-6706 (2008) Authorization for interception of wire, electronic or oral communications. Prosecuting attorney can apply for an order authorizing or approving the interception of wire, electronic or oral communications by investigative or law enforcement officers having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of the commission of the offense of murder, kidnapping, gambling, robbery, bribery, extortion, or dealing in narcotic drugs, marijuana or other dangerous drugs, or other crime dangerous to life, limb, or property, and punishable by imprisonment for more than one (1) year, or any conspiracy to commit any of the foregoing offenses.
- IDAHO CODE ANN. § 18-6707 (2008) Authorization for disclosure and use of intercepted wire, electronic or oral communications. Law enforcement officers and others who have legally received the disclosure may disclose to other proper professionals or in a court of law, or use that information for further investigation
- IDAHO CODE ANN. § 18-6708 (2008) Procedure for interception of wire, electronic or oral communications. (a) The identity of the person, if known, whose communications are to be intercepted; (b) The nature and location of the communications facilities as to which, or the place where, authority to intercept is granted; (c) A particular description of the type of communication sought to be intercepted, and a statement of the particular offense to which it relates; (d) The identity of the agency authorized to intercept the communications, and of the person making the application; and (e) The period of time during which such interception is authorized, including a statement as to whether or not the interception shall automatically terminate when the described communication has been first obtained.
- IDAHO CODE ANN. § 18-6709 (2008) Recovery of civil damages authorized. May recover actual and punitive damages from the responsible party.
- IDAHO CODE ANN. § 18-6719 (2008) Definitions. pen registers and trap and trace devices

- IDAHO CODE ANN. § 18-6720 (2008) General prohibition on pen register and trap and trace device use--Exception
- IDAHO CODE ANN. § 18-6721 (2008) Application for an order for a pen register or a trap and trace device
- IDAHO CODE ANN. § 18-6722 (2008) Issuance of an order for a pen register or a trap and trace device
- IDAHO CODE ANN. § 18-6723 (2008) Assistance in installation and use of a pen register or a trap and trace device
- **Computer Statutes**
 - IDAHO CODE ANN. § 26-1220 (2008) - It is unlawful to introduce fraudulent records into the computer system of a bank, or to use without authorization, the computer system of a bank or to obtain valuable services or data from a bank's computer system by unauthorized means.
 - IDAHO CODE ANN. § 18-2201 through -2202 (2008). Any person who knowingly accesses, attempts to access or uses, or attempts to use any computer, computer system, computer network, or any part thereof for the purpose of: devising or executing any scheme or artifice to defraud; obtaining money, property, or services by means of false or fraudulent pretenses, representations, or promises; or committing theft; commits computer crime. Destroying, damaging, accessing or attempting to access the same also commits computer crime.
- **Common Law**
 - Taylor v. KTVB, Inc, 525 P.2d 984 (Idaho 1974) - accepts Prosser's four strands of the tort of the invasion of privacy.

ILLINOIS PRIVACY LAW

- **State Constitutional Privacy Rights**
 - **Express**
 - ILL. CONST. art. I, § 6 (2009) - Searches, Seizures, Privacy and Interceptions. The people shall have the right to be secure in their persons, houses, papers and other possessions against unreasonable searches, seizures, invasions of privacy or interceptions of communications by eavesdropping devices or other means.
- **Search and Seizure**
 - ILL. CONST. art. I, § 6 (2009) - protects against unreasonable search and seizure
 - **Auto Exception**
 - People v. Hoskins, 461 N.E.2d 941 (Ill. 1984)
 - **Open Fields**
 - State v. Schmidt, 552 N.E.2d 1317 (Ill. App. Ct. 1988)
 - **Plain View**
 - People v. Stroud, 546 N.E.2d 293 (Ill. App. Ct. 1989)
- **Statutory Privacy Rights**
 - 720 ILL. COMP. STAT. ANN. 135/1-2 and 3 (2009) Harassment through electronic communications or telephone. Making any comment, request, suggestion or proposal which is obscene with an intent to offend; (2) Interrupting, with the intent to harass, the telephone service or the electronic communication service of any person; (3) Threatening injury to the person or to the property of the person to whom an electronic communication is directed or to any of his or her family or household members.
 - 720 ILL. COMP. STAT. ANN. 110/1 through 3 (2009) Communications Consumer Privacy Act. It shall be unlawful for a communications company to: (1) install and use any equipment which would allow a communications company to visually observe or listen to what is occurring in an individual subscriber's household without the knowledge or permission of the subscriber; (2) provide any person or public or private organization with a list containing the name of a subscriber, unless the communications company gives notice thereof to the subscriber; (3) disclose the television viewing habits of any individual subscriber without the subscriber's consent; or (4) install or maintain a home-protection scanning device in a dwelling as part of a communication service without the express written consent of the occupant.
 - 720 ILL. COMP. STAT. ANN. 145/1 (2009) Telecommunication Line Tapping Act. Any person who shall within this state wrongfully tap or connect a wire with the telegraph or telephone wires of any person, company or association engaged in the transmission of news or telegraph or telephone lines between the states or in this state for the purpose of wrongfully taking or making use of the news dispatches of such person, company or association, or of its customers, shall be deemed guilty of a Class A misdemeanor.
 - 215 ILL. COMP. STAT. ANN. 5/1003 (2009) - Insurance Information and Privacy Protection.
 - 765 ILL. COMP. STAT. ANN. 1075/60 (2009) Right of Publicity Act. Limitations regarding use of an individual's identity. (a) A person may not use an individual's

identity for commercial purposes during the individual's lifetime without having obtained previous written consent from the appropriate person or persons.

- 740 ILL. COMP. STAT. ANN. 7/1 (2009) AntiPhishing Act. It is unlawful for any person, by means of a Web page, electronic mail message, or otherwise through use of the Internet, to solicit, request, or take any action to induce another person to provide identifying information by representing himself, herself, or itself to be a business without the authority or approval of the business.
- 740 ILL. COMP. STAT. ANN. 14/15 (2009) - Biometric Information Privacy Act. No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, unless it first: (1) informs the subject or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored; (2) informs the subject or the subject's legally authorized representative in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and (3) receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative.
 - No private entity in possession of a biometric identifier or biometric information may sell, lease, trade, or otherwise profit from a person's or a customer's biometric identifier or biometric information.
 - No private entity in possession of a biometric identifier or biometric information may disclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information unless there is consent.
- 750 ILL. COMP. STAT. ANN. 50/18.05 (2009). The Illinois Adoption Registry and Medical Information Exchange. Requires voluntary contribution by parties.
- 325 ILL. COMP. STAT. ANN. 17/10 (2009) Children's Privacy Protection And Parental Empowerment Act. Sale or purchase of personal information concerning an individual known to be a child without parental consent is prohibited.
- 815 ILL. COMP. STAT. ANN. 505/2QQ (2009) - can't print social security number on an insurance card.
- **Public Records**
 - ILL. ADMIN. CODE tit. 2, § 701.30 (2009) - Information and public records of the Department are available to any requestor for inspection or copying, unless the public record or information is exempt from inspection or copying pursuant to Section 7 of the FOIA. Requests which violate privacy, further a commercial enterprise or disrupt the duly-undertaken work of any public body (e.g., for the purpose of soliciting business) shall be denied.
 - ILL. ADMIN. CODE tit. 77, § 500.20 (2009) - Any custodian of vital records may furnish, upon the terms or conditions as he or she may prescribe under the Act, the Adoption Act, and this Part, when deemed in the public interest and not for purposes of commercial solicitation or private gain, copies of vital records or data from these records: to public agencies administering health, welfare, safety, law enforcement, or public assistance programs; and to private agencies, approved by

the State Registrar, such as hospitals, public news media, abstract and title companies, and credit bureaus.

- 5 ILL. COMP. STAT. ANN. 140/11(2009) - Any person denied access to inspect or copy any public record by the head of a public body may file suit for injunctive or declaratory relief.
- 5 ILL. COMP. STAT. ANN. 140/7 (2009) specifically exempted from disclosure under the Freedom Of Information Act, which includes information that, if disclosed, would constitute a clearly unwarranted invasion of personal privacy, unless the disclosure is consented to in writing by the individual subjects of the information. The disclosure of information that bears on the public duties of public employees and officials shall not be considered an invasion of personal privacy.
- 5 ILL. COMP. STAT. ANN. 160/1.5 (2009) - (ii) that those records are to be created, maintained, and administered in support of the rights of those citizens and the operation of the State; (iii) that those records are, with very few exemptions, to be available for the use, benefit, and information of the citizens
 - Exceptions include foster parent and adoption information, arrest reports are withheld except to the news media
- 5 ILL. COMP. STAT. ANN. 175/1-101 through 175/99-1 (2009) – Electronic Commerce Security Act creates a way for state agencies to use and maintain the integrity of electronic records.
- 5 ILL. COMP. STAT. ANN. 175/25-101 (2009) - Each State agency shall determine if, and the extent to which, it will send and receive electronic records and electronic signatures to and from other persons and otherwise create, use, store, and rely upon electronic records and electronic signatures
- 5 ILL. COMP. STAT. ANN. 175/25-105 (2009) - The Department of Central Management Services may adopt rules setting forth minimum security requirements for the use of electronic records and electronic signatures by State agencies.
- **Motor Vehicle Records**
 - 625 ILL. COMP. STAT. ANN. 5/2-123 (2009) - Except as otherwise provided in this Section, the Secretary may make the driver's license, vehicle and title registration lists, in part or in whole, and any statistical information derived from these lists available to local governments, elected state officials, state educational institutions, and all other governmental units of the State and Federal Government requesting them for governmental purposes.
 - Commercial purchasers of driver and vehicle record databases shall enter into a written agreement with the Secretary of State that includes disclosure of the commercial use of the information to be purchased. (can't include personal information, unless the use meets one of twelve exceptions including (4) use in research activities and for use in producing statistical reports, if the personally identifying information is not published, redisclosed, or used to contact individuals and (10) or use in connection with the operation of private toll transportation facilities.)
 - Furnish vehicle or driver data to any State or local governmental agency that uses the information provided by the Secretary to transmit data back

- to the Secretary that enables the Secretary to maintain accurate driving records, including dispositions of traffic cases.
 - Can also provide vehicle or driver data to law enforcement, public transit system or authority, public defender, law enforcement agency, a state or federal agency, or an Illinois local intergovernmental association if the effort is to enforce the Code, do a background check, and conduct a criminal investigation.
 - ILL. ADMIN. CODE tit. 92, § 1002.70 (2009) - Subject to the federal Driver's Privacy Protection Act (18 USC 2721 et seq.) and 625 ILCS 5/2-123, the drivers lists, title lists and vehicle lists, and lists of purchasers of these lists, are public records and may be examined and purchased for the appropriate fees for a legitimate and lawful purpose and use.
 - Lists can be organized as by county or counties, age group, zip code groups, make or model of car, restriction codes, license issue data, license expiration data, city, or other governmental or geographic division
 - No listing shall be prepared and sold by the Secretary to any person or organization for commercial solicitation purposes. Lists shall not be available as compiled by any form of driver's license sanction (suspension, revocation, cancellation, or denial)
 - 625 ILL. COMP. STAT. ANN. 5/2-123 (2009) Motor vehicle accident reports confidential subject to limited exceptions for the Motor Vehicle Department and the Secretary of State.
- **Vehicle Identification Numbers**
 - 625 ILL. COMP. STAT. ANN. 5/4-103 (2009) - unlawful to knowingly remove, alter, deface, destroy, falsify, or forge a manufacturer's identification number of a vehicle or an engine number of a motor vehicle or any essential part thereof having an identification number.
 - People v. Anderson, 531 N.E.2d 116 (1988) - No expectation of privacy in a partially visible VIN “Analogizing this case to a search to locate a vehicle identification number (VIN) inside an automobile, held proper in the circumstances present in *New York v. Class* (1986), 475 U.S. 106, the State maintains that the search was proper even if the motivation was to search for marijuana.” Improper, however to open the door to look for the weight of the vehicle in the doorjam.
- **Consumer Credit**
 - 815 ILL. COMP. STAT. ANN. 530/1 through -20 (2009) - Personal Information Protection Act. Requiring notification of security breaches of databases containing personal information to consumers.
 - 815 ILL. COMP. STAT. ANN. 505/2MM (2009) permitting security freezes by consumers to prevent identity theft.
- **Financial Records**
 - 205 ILL. COMP. STAT. ANN. 305/10 (2009) - Credit Union Records. Financial records relating to the member may not be disclosed except to that member, to others that member authorized, pursuant to subpoena or when collecting an obligation owed to the credit union by the consumer.

- **Employee Privacy**

- People v. Neal, 486 N.E.2d 898 (Ill. 1985) - Holding that a state police officer lacked a reasonable expectation of privacy as to the state-owned raincoat pouch he kept in his patrol car. Although the raincoat was issued for the officer's exclusive use, and he put the forged citations in a zipped pocket of the coat, the court held that society was not willing to recognize the officer's expectation of privacy. Additionally the state police had the ability to periodically search the patrol car in accordance with their practices and policies.
- 820 ILL. COMP. STAT. ANN. 55/1 through 20 (2009) - Right to Privacy in the Workplace Act. It shall be unlawful for any employer to inquire, in a written application or in any other manner, of any prospective employee or of the prospective employee's previous employers, whether that prospective employee has ever filed a claim for benefits under the Workers' Compensation Act [820 ILCS 305/1 et seq.] or Workers' Occupational Diseases Act [820 ILCS 310/1 et seq.] or received benefits under these Acts.
- 820 ILL. COMP. STAT. ANN. 40/0.01 thru 13 (2009) Personnel Record Review Act. With certain exceptions.

- **Electronic Surveillance**

- 720 ILL. COMP. STAT. ANN. 720 § 5/14-1 (2009) Definition. An eavesdropping device is any device capable of being used to hear or record oral conversation or intercept, retain, or transcribe electronic communications whether such conversation or electronic communication is conducted in person, by telephone, or by any other means; Provided, however, that this definition shall not include devices used for the restoration of the deaf or hard-of-hearing to normal or partial hearing.
 - "Electronic communication." For purposes of this Article, the term electronic communication means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or part by a wire, radio, pager, computer, electromagnetic, photo electronic or photo optical system, where the sending and receiving parties intend the electronic communication to be private and the interception, recording, or transcription of the electronic communication is accomplished by a device in a surreptitious manner contrary to the provisions of this Article. Electronic communication does not include any communication from a tracking device.
- 720 ILL. COMP. STAT. ANN. 720 § 5/14-2 (2009) Elements of the offense; affirmative defense. person commits eavesdropping when he: (1) Knowingly and intentionally uses an eavesdropping device for the purpose of hearing or recording all or any part of any conversation or intercepts, retains, or transcribes electronic communication unless he does so (A) with the consent of all of the parties to such conversation or electronic communication or (B) in accordance with Article 108A or Article 108B of the "Code of Criminal Procedure of 1963." Other exceptions include:
 - Exceptions for law enforcement acting under a court order to intercept or if the officer overheard the communication or intercepted accidentally but did not disclose.

- 720 ILL. COMP. STAT. ANN. § 5/14-8 (2009) Discovery of eavesdropping device by an individual, common carrier, private investigative agency or non-governmental corporation. Notify state attorney and leverage a fine.
- 720 ILL. COMP. STAT. ANN. § 5/14-9 (2009) Discovery of eavesdropping device by common carrier by wire--Disclosure to subscriber. Notify state attorney and leverage a fine.
- 725 ILL. COMP. STAT. ANN. § 5/108A-1 (2009) Authorization for use of eavesdropping device. The State's Attorney or an Assistant State's Attorney authorized by the State's Attorney may authorize an application to a circuit judge or an associate judge assigned by the Chief Judge of the circuit for installation of an eavesdropping device.
- 725 ILL. COMP. STAT. ANN. § 5/108A-2 (2009) Authorized Disclosure or Use of Information
- 725 ILL. COMP. STAT. ANN. § 5/108A-3 (2009) Procedure for Obtaining Judicial Approval of Use of Eavesdropping Device
- 725 ILL. COMP. STAT. ANN. § 5/108A-4 (2009) Grounds for Approval or Authorization. There is reasonable cause for believing that an individual is committing, has committed, or is about to commit a felony under Illinois law; (c) there is reasonable cause for believing that particular conversations concerning that felony offense will be obtained through such use; and (d) for any extension authorized, that further use of a device is warranted on similar grounds.
- 725 ILL. COMP. STAT. ANN. § 5/108A-5 (2009) Orders Authorizing Use of an Eavesdropping Device
- 725 ILL. COMP. STAT. ANN. § 5/108A-6 (2009) Emergency Exception to Procedures
- 725 ILL. COMP. STAT. ANN. § 5/108A-7 (2009) Retention and Review of Recordings
- 725 ILL. COMP. STAT. ANN. § 5/108A-8 (2009) Notice to Parties Overheard. Within a reasonable time, but not later than 90 days after either the filing of an application for an order of authorization or approval which is denied or not later than 90 days after the termination of the period of an order or extension thereof, the issuing or denying judge shall cause to be served on the persons named in the order or application and such other persons in the recorded conversation as the judge may determine that justice requires be notified
- 725 ILL. COMP. STAT. ANN. § 5/108B-1 through B-14 (2009). Electronic Criminal Surveillance. Same requirements for judicial approval to install these devices as for eavesdropping with the exception that the types of crimes that may be surveyed are not as broad as "any felony," which was permitted for the eavesdropping devices. The types of crimes include: a violation of Section 8-1.1 [720 ILCS 5/8-1.1] (solicitation of murder), 8-1.2 [720 ILCS 5/8-1.2] (solicitation of murder for hire), 9-1 [720 ILCS 5/9-1] (first degree murder), or 29B-1 [720 ILCS 5/29B-1] (money laundering) of the Criminal Code of 1961, Section 401, 401.1 (controlled substance trafficking), 405, 405.1 (criminal drug conspiracy) or 407 of the Illinois Controlled Substances Act or any Section of the Methamphetamine Control and Community Protection Act [720 ILCS 570/401] or conspiracy to commit money laundering or conspiracy to commit first degree murder; (ii) in response to a clear

and present danger of imminent death or great bodily harm to persons resulting from:

- (1) a kidnapping or the holding of a hostage by force or the threat of the imminent use of force; or (2) the occupation by force or the threat of the imminent use of force of any premises, place, vehicle, vessel or aircraft;
 - (iii) to aid an investigation or prosecution of a civil action brought under the Illinois Streetgang Terrorism Omnibus Prevention Act [740 ILCS 147/1 et seq.] when there is probable cause to believe the interception of the private communication will provide evidence that a streetgang is committing, has committed, or will commit a second or subsequent gang-related offense or that the interception of the private communication will aid in the collection of a judgment entered under that Act; or (iv) upon information and belief that a streetgang has committed, is committing, or is about to commit a felony.
 - Note that: "Electronic communication" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or part by a wire, radio, pager, computer, or electromagnetic, photo electronic, or photo optical system where the sending and receiving parties intend the electronic communication to be private and the interception, recording, or transcription of the electronic communication is accomplished by a device in a surreptitious manner contrary to the provisions of this Article. "Electronic communication" does not include: (1) any wire or oral communication; or (2) any communication from a tracking device.
- **Computer Statutes**
 - 720 ILL. COMP. STAT. ANN. § 5/16D-1 through D-7 (2009) - Computer crime. A person accesses or destroys a computer or computer data without authorization.
- **Common Law**
 - Blair v. Nevada Landing Partnership, 859 N.E.2d 1188 (Ill. Ct. App. 2006) After December 31, 1998, the common-law tort of appropriation of one's likeness ceased to exist. The Right of Publicity Act, effective January 1, 1999, completely replaced the common-law tort of appropriation of likeness, although it did not affect the other three common-law privacy torts: Disclosure, False Light, and Intrusion.
 - 735 ILL. COMP. STAT. ANN. § 5/13-201 (2009) Defamation -- Privacy. Actions for slander, libel or for publication of matter violating the right of privacy, shall be commenced within one year next after the cause of action accrued.
 - Cordts v. Chi. Tribune Co., 860 N.E.2d 444 (Ill. Ct. App. 2006) - Specifically accepts the tort of disclosure.

INDIANA PRIVACY LAW

- **State Constitutional Privacy Rights**
 - **Express** - none
 - **Implied**
 - IND. CONST. art. I, § 11 (2009). The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable search, or seizure, shall not be violated; and no warrant shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the person or thing to be seized.
- **Search and Seizure**
 - IND. CONST. art. I, § 11 (2009) no unreasonable search and seizure.
 - Brannon v. State, 142 N.E.2d 215 (Ind. 1957) - right to inspect the exterior of a parked automobile if there is probable cause to believe the car was used in the commission of a felony.
 - **Auto Exception**
 - Campos v. State, 885 N.E.2d 590 (Ind. 2008) - recognized the exception, but found that the officer did not have probable cause to search and therefore the search was illegal.
 - **Open Fields**
 - Sayre v. State, 471 N.E.2d 708 (Ind. Ct. App. 1985)
 - **Plain View**
 - State v. Kitt, 577 N.E.2d 972 (Ind. Ct. App. 1991).
 - Bell v. State, 626 N.E.2d 570 (Ind. Ct. App. 1993) - A person has no reasonable expectation of privacy in garbage left on the curb.
- **Statutory Privacy Rights**
 - IND. CODE ANN. §§ 4-1-6-1 through 4-1-6-9 (2009) – Fair Information Practices Act. Deals with the collection of personal data, rather than the public record, which is understood to be accessible by the public.
 - Personal information may be provided to the individual, his physician or his agent. Agencies may collect personal information, but only as it relates to meeting the statutory purpose of the agency. This information must be kept separate from the information in the public record.
 - IND. CODE ANN. § 4-1-8-1 (2009) No individual may be compelled by any state agency to provide their social security number except for the specified agencies including the Bureau of Motor Vehicles.
 - IND. CODE ANN. § 35-45-10-1 (2009) - Stalking. As used in this chapter, "stalk" means a knowing or an intentional course of conduct involving repeated or continuing harassment of another person that would cause a reasonable person to feel terrorized, frightened, intimidated, or threatened and that actually causes the victim to feel terrorized, frightened, intimidated, or threatened. The term does not include statutorily or constitutionally protected activity.
 - (A) stalks a victim; and (B) makes an explicit or an implicit threat with the intent to place the victim in reasonable fear of: (i) sexual battery (as defined in IC 35-42-4-8); (ii) serious bodily injury; or (iii) death.

- IND. CODE ANN. § 35-46-1-15.1 (2009) - Offenses against the family. Invasion of Privacy. Regarding violations of protective orders, restraining orders, no contact orders.
- IND. CODE ANN. § 24-4.7-1-1 (2009) Telephone Solicitation Act.
- IND. CODE ANN. § 4-1-11-5; -6 (2009) State agency to disclose breach of security that includes personal information -- Notification of owner of licensee of information without unreasonable delay.
- IND. CODE ANN. § 24-4.9-2-4 (2009) "Doing business in Indiana" means owning or using the personal information of an Indiana resident for commercial purposes.
- IND. CODE ANN. § 24-4.9-3-1 (2009) - after discovering or being notified of a breach of the security of a system, the data base owner shall disclose the breach to an Indiana resident whose: (1) unencrypted personal information was or may have been acquired by an unauthorized person; or (2) encrypted personal information was or may have been acquired by an unauthorized person with access to the encryption key; if the data base owner knows, should know, or should have known that the unauthorized acquisition constituting the breach has resulted in or could result in identity deception.
- **Public Records**
 - IND. CODE ANN. § 5-14-3-3 (2009) - any person may inspect and copy the public records of any public agency during the regular business hours of the agency, except as provided in section 4 of this chapter.
 - IND. CODE ANN. § 5-14-3-4 through 6 (2009) – exceptions include records that relate to judicial proceedings, law enforcement job information, the Indiana Economic Development Corporation, certain documents for public negotiations, arrest reports are not all available to the public, certifying agency examinations, trade secrets, patient records, autopsy recordings, social security numbers, attorney work product, diaries/journals, security system information, work product of the legislative assembly, a record that threatens public safety by exposing vulnerability to terrorist attack (planning, risk assessments, certain emergency contact info, etc.)
 - IND. CODE ANN. § 12-15-27-4 (2009) - The office shall keep a file that contains a report showing the name and identification number of each recipient and the amount of medical assistance received each month under the Medicaid program. Report under subsection (a) is a public record open to public inspection at all times during the regular office hours of the office. But cannot utilize information gained from the information for religious, commercial, or political purposes.
 - IND. CODE ANN. § 4-1-10-6 (2009) - must obscure or remove social security numbers before releasing them as public records.
- **Motor Vehicle Records**
 - IND. CODE ANN. 9-14-3-5 (2009) Motor vehicle records are public except that the bureau may not disclose social security number, driver's license number, pictures, signatures or medical or disability information.
 - IND. CODE ANN. 9-14-3-5 (2009) may disclose operating record of each driver which includes insurance lapses, revocation of license and any traffic violation information but the record is not admissible as evidence in any action for damages

arising out of a motor vehicle accident; and may not include voter registration information.

- **Vehicle Identification Numbers**
 - IND. CODE ANN. 9-18-8-12 (2009) unlawful to remove, alter or damage a VIN
- **Consumer Credit**
 - IND. CODE ANN. § 24-4.9-3-1 (2009) - businesses must notify customers of security breaches of their databases that contain personal information
 - IND. CODE ANN. § 4-1-11-5; -6 (2009) State agency to disclose breach of security that includes personal information -- Notification of owner of licensee of information without unreasonable delay.
 - IND. CODE ANN. 24-5-24-1 through -17 (2009). Permits security freezes for consumer reports.
- **Financial Records**
 - IND. CODE ANN. § 28-1-2-30.5 (2009) Financial Institutions Act Personal records -- Keeping, handling, safeguarding, and disposal.
 - IND. CODE ANN. § 28-7-5-39 (2009) - records generated in the course of doing a pawnbroker business are confidential, unless law enforcement needs to intervene to determine ownership.
- **Employee Privacy**
 - IND. CODE ANN. § 4-13-18-6 (2009) - requires public works contractors to have random drug tests at least once per year. There is no explanation whether the results must be confidential.
- **Electronic Surveillance**
 - IND. CODE ANN. 35-33.5-1-1 (2009) Inapplicable to ordinary course of business. This article does not apply to the ordinary course of business pertaining to the operation of a business entity that provides or facilitates electronic communications in accordance with the business entity's tariffs.
 - IND. CODE ANN. 35-33.5-1-3.5 (2009) "Electronic communication" defined. "Electronic communication" means any transfer of signs, signals, writing, images, sounds, data, oral communication, digital information, or intelligence of any nature transmitted in whole or in part by a wire, a radio, or an electromagnetic, a photoelectronic, or a photo-optical system.
 - IND. CODE ANN. 35-33.5-1-5 (2009) Interception defined. "Interception" means the intentional recording or acquisition of the contents of an electronic communication by a person other than a sender or receiver of that communication, without the consent of the sender or receiver, by means of any instrument, device, or equipment under this article. This term includes the intentional recording or acquisition of communication through the use of a computer or a FAX (facsimile transmission) machine.
 - IND. CODE ANN. 3-33.5-2-1 (2009) Application for warrant by prosecuting attorney; coapplicant; interception equipment under control of state police
 - IND. CODE ANN. 3-33.5-2-2 (2009) Application or extension in writing and upon oath of affirmation; information required
 - IND. CODE ANN. 3-33.5-2-3 (2009) Allegations of fact; basis; information required; supporting affidavits

- IND. CODE ANN. § 35-33.5-4-3 (2009) Notice. Within sixty (60) days after the termination of a warrant or an extension, the court shall cause to be served upon each person from whom communication was to be intercepted and upon any other party to an interception whom the court determines it is in the interest of justice to serve, an inventory that includes notice of the following: (1) The date that the application for the warrant or extension was submitted. (2) The date on which the warrant or extension was granted. (3) The time during which the interception was authorized. (4) Whether the type of communication specified in the warrant was intercepted during the authorized time.
- IND. CODE ANN. § 35-33.5-5-1 (2009) Disclosure to parties content of interception evidence. Within 14 days before the evidence is used in a proceeding.
- IND. CODE ANN. 35-33.5-5-2 (2009) Retention of intercepted communications.
- IND. CODE ANN. 35-33.5-5-3 (2009) Legally obtained interceptions by law enforcement may use the communications or disclose them to another law enforcement agency. If the recording is to be transcribed, only the part that is relevant to the proceeding may be transcribed. Note that an otherwise privileged communication that is intercepted in accordance with or in violation of this article does not lose the communication's privileged character.
- **Computer Statutes**
 - IND. CODE ANN. § 35-43-2-3 (2009) - Computer Trespass. Knowingly or intentionally accessing a computer without consent.
 - IND. CODE ANN. § 35-43-1-4 (2009) - Computer Tampering knowingly or intentionally altering or damaging a computer.
- **Common Law**
 - Cullison v. Medley, 570 N.E.2d 27 (Ind. 1991) - recognize all four invasion of privacy categories.

IOWA PRIVACY LAW

- **State Constitutional Privacy Rights**
 - None
- **Search and Seizure**
 - IOWA CONST. art. I, § 8 (2008) - The right of the people to be secure in their persons, houses, papers and effects, against unreasonable seizures and searches shall not be violated; and no warrant shall issue but on probable cause, supported by oath or affirmation, particularly describing the place to be searched, and the persons and things to be seized.
 - IOWA CONST. art. I, § 1 (2008) - All men have certain unalienable rights. Among those is enjoying and defending life and liberty and pursuing safety and happiness.
 - State v. Henderson, 435 N.W. 394, 395 (Iowa Ct. App. 1988) - exposing garbage to the public means there is no reasonable expectation of privacy.
 - **Auto Exception**
 - **Open Fields**
 - State v. Kramer, 231 N.W.2d 874 (Iowa 1975).
 - **Plain View**
 - State v. Davis, 228 N.W.2d 67 (Iowa 1975).
- **Statutory Privacy Rights**
 - IOWA CODE ANN. § 708.11 (2008) - Stalking. The person purposefully engages in a course of conduct directed at a specific person that would cause a reasonable person to fear bodily injury to, or the death of, that specific person or a member of the specific person's immediate family. b. The person has knowledge or should have knowledge that the specific person will be placed in reasonable fear of bodily injury to or the death of, that specific person or a member of the specific person's immediate family by the course of conduct. c. The person's course of conduct induces fear in the specific person of bodily injury to, or the death of, the specific person or a member of the specific person's immediate family.
 - IOWA CODE ANN. § 709.21 (2008) - Invasion of Privacy. A person who knowingly views, photographs, or films another person, for the purpose of arousing or gratifying the sexual desire of any person, commits invasion of privacy if all of the following apply: a. The other person does not have knowledge about and does not consent or is unable to consent to being viewed, photographed, or filmed. b. The other person is in a state of full or partial nudity. c. The other person has a reasonable expectation of privacy while in a state of full or partial nudity.
- **Individually Identifiable Government Records**
 - IOWA CODE ANN. § 22.11 (2008) - Fair information Practices Act. The intent is to require that the information policies of the state agencies are subject to public review and comment.
- **Public Records**
 - IOWA CODE ANN. § 22.11 (2008) - Every person shall have the right to examine and copy a public record and to publish or otherwise disseminate a public record or the information contained in a public record.
 - IOWA CODE ANN. § 22.7 (2008) – lists the exceptions (59 in total) which are not public record, and instead are confidential. Examples include: personal education

records, underage crimes, health records, trade secrets, work product of attorneys, investigations of peace officers, Iowa Dept of Economic Development, criminal identification files (but current and prior arrests are viewable), library information, applications for general assistance, locations of ecologically sensitive areas, gambling addiction programs, certain information on housing assistance forms, certain information about emergency preparedness, information regarding the issuance of a driver's license, etc.

- IOWA CODE ANN. § 144.43 (2008) - access to vital statistics records kept by the state registrar shall be limited to the state registrar and the state registrar's employees, and then only for administrative purposes. Access may be granted if the records are 75 years old. "*Vital statistics*" means records of births, deaths, fetal deaths, adoptions, marriages, dissolutions, annulments, and data related thereto.
- 191 IOWA ADMIN. CODE 54.13 (523C) (2008) – the administrator may keep confidential certain information obtained in the course of an investigation or audit pursuant to IOWA CODE ANN. chapter 22, but generally any application for a license by a service company to the Iowa securities bureau is available for inspection. (Service companies enter into contracts or agreements with residential customers.)
- **Motor Vehicle Records**
 - IOWA CODE ANN. § 516E.18 (2008) - The administrator shall keep a register of all filings and orders which have been entered for contracts or agreements given for consideration over and above the lease or purchase price of a new or used motor vehicle. The register shall be open for public inspection.
 - 191 IOWA ADMIN. CODE 23.6(516E) (2008) - the administrator and the attorney general may keep confidential information obtained during an investigation or audit, but generally must keep all filings and orders of motor vehicle services contracts open for public inspection.
 - IOWA CODE ANN. § 321.24 (2008) Issuance of registration and certificate of title shall be open to public inspection.
 - IOWA CODE ANN. § 321.11 (2008) All records of the department, other than those made confidential or not permitted to be open. Personal information is confidential and means information that identifies a person, including a person's photograph, social security number, driver's license number, name, address, telephone number, and medical or disability information, but does not include information on vehicular accidents, driving violations, and driver's status or a person's zip code.
 - IOWA CODE ANN. § 321.271 (2008) - all accident reports are confidential and only for the use of the department with the exception of those parties involved with the accident and their agents.
- **Vehicle Identification Numbers**
 - IOWA CODE ANN. § 321.92 (2008) - altering or changing VIN with fraudulent intent is a crime.
- **Consumer Credit**
 - IOWA CODE ANN. § 715C.2 (2008) Any person who owns or licenses computerized data that includes a consumer's personal information that is used in the course of the person's business, vocation, occupation, or volunteer activities

and that was subject to a breach of security shall give notice of the breach of security following discovery of such breach of security, or receipt of notification under subsection 2, to any consumer whose personal information was included in the information that was breached. The consumer notification shall be made in the most expeditious manner possible and without unreasonable delay, consistent with the legitimate needs of law enforcement

- **Financial Records**

- IOWA CODE ANN. § 20.25 (2008) - Upon written request of any member of a certified employee organization, the auditor of the state may audit the financial records.
- IOWA CODE ANN. § 527.1 (2008) - Electronic fund transfer systems should provide reliable service with the full protection of privacy for personal financial information.
- IOWA CODE ANN. § 527.10 (2008) - A satellite terminal, data processing center, or central routing unit shall not be operated in any manner to permit any person to obtain information concerning the account of any person with a financial institution, unless such information is essential to complete or prevent the completion of a transaction then being engaged in through the use of that facility.

- **Employee Privacy**

- IOWA CODE ANN. § 730.5 (2008) - Drug Free Workplace. All communications received by an employer relevant to employee or prospective employee drug or alcohol test results, or otherwise received through the employer's drug or alcohol testing program, are confidential communications and shall not be used or received in evidence, obtained in discovery, or disclosed in any public or private proceeding, except as otherwise provided or authorized by this section. Exceptions include disclosure in arbitration under a collective bargaining agreement, if employment is based on a government contract.
 - Positive test results from an employer drug or alcohol testing program shall not be used as evidence in any criminal action against the employee or prospective employee tested.
- IOWA CODE ANN. § 91B.1 (2008) An employee, as defined in section 91A.2, shall have access to and shall be permitted to obtain a copy of the employee's personnel file maintained by the employee's employer, as defined in section 91A.2, including but not limited to performance evaluations, disciplinary records, and other information concerning employer-employee relations. However, an employee's access to a personnel file is subject to all of the following: the employer and employee shall agree on the time the employee may have access to the employee's personnel file, and shall not review employment references written for the employee.

- **Electronic Surveillance**

- IOWA CODE ANN. § 727.8 (2008). Electronic and mechanical eavesdropping. Any person, having no right or authority to do so, who taps into or connects a listening or recording device to any telephone or other communication wire, or who by any electronic or mechanical means listens to, records, or otherwise intercepts a conversation or communication of any kind, commits a serious misdemeanor; provided, that the sender or recipient of a message or one who is openly present

and participating in or listening to a communication shall not be prohibited hereby from recording such message or communication; and further provided, that nothing herein shall restrict the use of any radio or television receiver to receive any communication transmitted by radio or wireless signal.

- IOWA CODE ANN. § 808B.1 (2008) Definitions. "*Electronic communication*" means any transfer of signals, signs, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects intrastate, interstate, or foreign commerce, but excludes the following: a. Wire or oral communication. b. Communication made through a tone-only paging device. c. Communication from a tracking device.
- IOWA CODE ANN. § 808B.2 (2008) Unlawful acts--penalty. Willfully intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, a wire, oral, or electronic communication. b. Willfully uses, endeavors to use, or procures any other person to use or endeavor to use an electronic, mechanical, or other device to intercept any oral communication.
 - Ok to intercept if a party to the communication, if a telecommunications employee in the course of employment (however, communications common carriers shall not use service observing or random monitoring except for mechanical or service quality control checks) or under court order.
- IOWA CODE ANN. § 808B.3 (2008) Court order for interception by special agents. The attorney general shall authorize and prepare any application for an order authorizing the interception of wire, oral, or electronic communications. Only can be granted if the interception is aimed at getting information about: a felony offense involving dealing in controlled substances, as defined in section 124.101. or a felony offense involving money laundering in violation of chapter 706B.
- IOWA CODE ANN. § 808B.4 (2008) Permissible disclosure and use. To another law enforcement officer or agency in performance of their duties or in a court of law.
- IOWA CODE ANN. § 808B.5 (2008) Application and order
- IOWA CODE ANN. § 808B.6 (2008) Reports to state court administrator
- IOWA CODE ANN. § 808B.7 (2008) Contents of intercepted wire, oral, or electronic communication as evidence. Can't be admitted unless in accordance with this chapter.
- IOWA CODE ANN. § 808B.8 (2008) Civil damages authorized--civil and criminal immunity-- injunctive relief. Against the person who intercepted unlawfully.
- IOWA CODE ANN. § 808B.10 (2008) Restrictions on use and installation of a pen register or a trap and trace device. Need to have a court order.
- IOWA CODE ANN. § 808B.11 (2008) Application and order to install and use a pen register or trap and trace device.
- **Computer Statutes**
 - IOWA CODE ANN. § 692.8; 692.10 (2008) - intelligence data from the department of public safety or criminal justice agency may be placed in computer storage as long as access is restricted to employees of the department
 - IOWA CODE ANN. § 715.1 through 715.8 (2008) - Computer Spyware And Malware Protection. It is the intent of the general assembly to protect owners and

operators of computers in this state from the use of spyware and malware that is deceptively or surreptitiously installed on the owner's or the operator's computer.

- IOWA CODE ANN. § 716A.2 (2008) - transmission of unsolicited bulk email is unlawful. Uses a computer or computer network with the intent to falsify or forge electronic mail transmission information or other routing information in any manner in connection with the transmission of unsolicited bulk electronic mail through or into the computer network of an electronic mail service provider or its subscribers.
- IOWA CODE ANN. § 716.6B (2008) - person who knowingly and without authorization accesses a computer, computer system, or computer network is committing a crime. It aggravates the crime if data is destroyed, copied or altered.
- **Common Law**
 - Stessman v. American Black Hawk Broadcasting Co, 416 N.W.2d 685 (Iowa 1987) - accepts the four invasion of privacy common law torts - intrusion, false light, disclosure and appropriation.

KANSAS PRIVACY LAW

- **State Constitutional Privacy Rights**
 - none
- **Search and Seizure**
 - KAN. CONST. Bill of Rights, § 15 (2007) - The right of the people to be secure in their persons and property against unreasonable searches and seizures, shall be inviolate; and no warrant shall issue but on probable cause, supported by oath or affirmation, particularly describing the place to be searched and the persons or property to be seized.
 - **Auto Exception**
 - State v. Ibarra, 147 P.3d 842 (Kan. 2006)
 - **Open Fields**
 - State v. Tinsley, 823 P.2d 205 (Kan. Ct. App. 1991)
 - **Plain View**
 - State v. Marks, 602 P.2d 1344 (Kan. 1979)
- **Statutory Privacy Rights**
 - KAN. STAT. ANN. § 21-4002 (2007) - Breach of privacy is knowingly and without lawful authority: (1) Intercepting, without the consent of the sender or receiver, a message by telephone, telegraph, letter or other means of private communication; or (2) Divulging, without the consent of the sender or receiver, the existence or contents of such message if such person knows that the message was illegally intercepted, or if such person illegally learned of the message in the course of employment with an agency in transmitting it. Shall not apply to messages overheard through a regularly installed instrument on a telephone party line or on an extension.
 - KAN. STAT. ANN. § 60-31a02 (2007) - Protection From Stalking Act."Stalking" means an intentional harassment of another person that places the other person in reasonable fear for that person's safety. A person may seek relief under the protection from stalking act by filing a verified petition with the district judge or clerk of the court in the county where the stalking occurred. The judge may issue a restraining order.
- **Individually Identifiable Government Records**
 - KAN. STAT. ANN. § 22-4704 (2007) - requires procedures to insure security of all criminal history information and to allow inspection of such information.
 - KAN. STAT. ANN. § 22-4709 (2007) - criminal history information may not be disseminated except in strict accordance with the law, and non criminal justice persons may only receive the information in accordance with the law.
 - KAN. STAT. ANN. § 50-7a01; -02 (2007) If there is a security breach of personal information, the person or government, governmental subdivision or agency shall give notice as soon as possible to the affected Kansas resident without reasonable delay if there has been a misuse of information or is reasonably likely to occur,
 - "Security breach" means the unauthorized access and acquisition of unencrypted or unredacted computerized data that compromises the security, confidentiality or integrity of personal information maintained by an individual or a commercial entity and that causes, or such individual or entity reasonably believes has caused or will cause, identity theft to any

consumer. Good faith acquisition of personal information by an employee or agent of an individual or a commercial entity for the purposes of the individual or the commercial entity is not a breach of the security of the system, provided that the personal information is not used for or is not subject to further unauthorized disclosure.

- "Personal information" means a consumer's first name or first initial and last name linked to any one or more of the following data elements that relate to the consumer, when the data elements are neither encrypted nor redacted.

- KAN. STAT. ANN. § 45-230 (2007) Unlawful use of names derived from public records. No person shall knowingly sell, give or receive, for the purpose of selling or offering for sale any property or service to persons listed therein, any list of names and addresses contained in or derived from public records. Certain exceptions apply including: Lists of names and addresses from public records of the division of vehicles under § 74-2012.

- **Public Records**

- KAN. STAT. ANN. § 39-709b (2007) - Information concerning applicants for and recipients of social welfare assistance from the secretary shall be confidential and privileged and shall only be available to the secretary and the officers and employees of the secretary except as set forth in this section.
- KAN. STAT. ANN. § 45-218 (2007) - All public records shall be open for inspection by any person, except as otherwise provided by this act.
- KAN. STAT. ANN. § 45-221 (2007) – Lists 47 exceptions including information about safehouses, criminal investigations, other security-related investigations, market research of managed care third party, records that would invade personal privacy, information regarding victims of the sex offender registration act, work product of a legislative agency, testing or examination materials for a licensing test, library information drug dependency treatment; however, a record that is over 70 years old may be open for public inspection.
- KAN. STAT. ANN. § 45-230 (2007) - No person shall knowingly sell, give or receive, for the purpose of selling or offering for sale any property or service to persons listed therein, any list of names and addresses contained in or derived from public records except: Lists of names and addresses from public records of the division of vehicles obtained under K.S.A. 74-2012; lists of names and addresses of persons licensed, registered or issued certificates or permits to practice a profession or vocation, if for purposes related to the profession; names from voter registration may be given for election purposes.

- **Motor Vehicle Records**

- KAN. STAT. ANN. § 74-2012 (2007) - All motor vehicle records shall be subject to the provisions of the open records act, except as otherwise provided under the provisions of this section and by K.S.A. 74-2022.
 - However all motor vehicle records which relate to the physical or mental condition of any person have been expunged, or are photographs or digital images maintained in connection with the issuance of drivers' licenses shall be confidential.

- Lists of persons' names and addresses contained in or derived from motor vehicle records shall not be sold, given or received for the purpose of commercial gain, but may be given to assisting manufacturers of motor vehicles in compiling statistical reports or in notifying owners of vehicles believed to have defects.
 - Motor vehicle names and addresses may also be disclosed for use in assisting a governmental agency and for other reasons including: assisting an employer or an employer's authorized agent in monitoring the driving record of the employees required to drive in the course of employment to ensure driver behavior, performance, or safety.
- **Vehicle Identification Numbers**
 - KAN. STAT. ANN. § 74-2135 (2007) The superintendent of the Kansas highway patrol may adopt rules and regulations relating to the manner in which checks for verification of vehicle identification numbers shall be made under K.S.A. 8-116a [check of VINs by highway patrol] and amendments thereto. Concerning motor vehicles upon which such checks are made, such rules and regulations may provide for tests and procedures to detect evidence of possible fraud or other improper conduct relating to certificates of title, odometers.
 - KAN. STAT. ANN. § 8-116A (2007) When an application is made for a vehicle which has been assembled, reconstructed, reconstituted or restored from one or more vehicles, or the proper identification number of a vehicle is in doubt, the procedure in this section shall be followed. The owner of the vehicle shall request the Kansas highway patrol to check the vehicle and the highway patrol shall within a reasonable period of time perform such vehicle check.
 - State v. Morlock, 190 P.3d 1002 (Kan. 2008) - Noting with approval that in New York v. Class, 475 U.S. 106 (1986), the Court held that an officer could check the vehicle identification number (VIN) during a traffic stop in part because VINs are used to check for stolen vehicles, which also are more likely to be involved in accidents. 475 U.S. at 111. Despite the fact that VINs have nothing to do with the purpose of the typical traffic stop.
- **Consumer Credit**
 - KAN. STAT. ANN. § 50-701 (2007) Fair Credit Reporting Act. The purpose of the Act is to ensure consumer reporting agencies adopt reasonable procedures for meeting the needs of commerce for consumer credit, personnel, insurance, and other information in a manner which is fair and equitable to the consumer, with regard to the confidentiality, accuracy, relevancy, and proper utilization of such information in accordance with the requirements of such sections of this act.
 - KAN. STAT. ANN. § 50-703 (2007). A consumer reporting agency may furnish a consumer report under the following circumstances and no other: In response to the order of a court having jurisdiction to issue such an order; in accordance with the written instructions of the consumer to whom it relates; and to a person which it has reason to believe is issuing credit to the consumer.
 - KAN. STAT. ANN. § 50-704 (2007). Obsolete information not to be included in the credit report, ex. bankruptcies more than 14 years old.
 - KAN. STAT. ANN. § 50-707 (2007). Disclosures to governmental agencies. Notwithstanding the provisions of K.S.A. 50-703, a consumer reporting agency

may furnish identifying information respecting any consumer, limited to name, address, former addresses, places of employment, or former places of employment, to a governmental agency.

- KAN. STAT. ANN. § 50-708 (2007). Disclosures to consumers. Every consumer reporting agency shall, upon request and proper identification of any consumer, clearly and accurately disclose to the consumer: The nature and substance of all information (except medical information) in its files on the consumer at the time of the request; the sources of information and who else requested the report.
- KAN. STAT. ANN. § 50-723 (2007) - permits consumers to place a security freeze on their records.
- **Financial Records**
 - KAN. STAT. ANN § 9-1712 (2007) - Examination records of commissioner confidential; disclosure, when, procedure. All information the state bank commissioner generates in making an investigation or examination of a state bank or trust company shall be confidential information. All confidential information shall be the property of the state of Kansas and shall not be subject to disclosure except upon the written approval of the state bank commissioner.
- **Employee Privacy**
 - State v. Cruz, 809 P.2d 1233 (Ka. Ct. App. 1991) - held that an employee, lacking a possessory interest in his or her place of employment, has no expectation of privacy in the employer's premises under the Fourth Amendment.
- **Electronic Surveillance**
 - KAN. STAT. ANN. § 21-4001 (2007) Eavesdropping - entering a private place or installing a device that aids in listening surreptitiously to private conversations or to observe the personal conduct. Exception for telecommunications operator in the course of employment.
 - KAN. STAT. ANN. § 22-2514 (2007) Authorized interception of wire, oral or electronic communications; definitions. (11) "electronic communication" means any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photo-optical system but does not include: (a) Any wire or oral communication; (b) any communication made through a tone-only paging device; or (c) any communication from a tracking device, as defined in section 3117, chapter 205 of title 18, United States Code.
 - KAN. STAT. ANN. § 22-2515 (2007) - lists the 20 crimes that can justify eavesdropping warrants. Includes terrorism, murder, racketeering, etc.
 - KAN. STAT. ANN. § 22-2516 (2007) Application for order, form and contents; issuance of order; contents; duration; extension; recordation of intercepted communications; custody of application and order, disclosure; inventory, notice to certain persons; evidentiary status of intercepted communications; motion to suppress, appeal
 - Within a reasonable time but not later than 90 days after the termination of the period of an order or extensions thereof the issuing or denying judge shall cause to be served on the persons named in the order or the application and, in the interest of justice, such other parties to intercepted communications as the judge may determine, an inventory which shall

include notice of: (i) the fact of the entry of the order or the application; (ii) the date of the entry and the period of authorized, approved or disapproved interception, or the denial of the application; and (iii) the fact that during the period wire, oral or electronic communications were or were not intercepted.

- KAN. STAT. ANN. § 22-2517 (2007) Unlawful interception of wire or oral communication; evidentiary status of contents.
- KAN. STAT. ANN. § 22-2518 (2007) Civil action for damages; defense available in civil and criminal actions.
- KAN. STAT. ANN. § 22-2519 (2007) Reports by judges and prosecutors to administrative office of federal courts.
- KAN. STAT. ANN. § 22-2525 (2007) Authorized installation or use of pen register or a trap and trace device; court order required, exception. Exceptions are consent or if the telecommunications provider needs to install the register for operation and maintenance.
 - “pen register” means a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached but shall not include any device used by a provider or customer of an electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device used by a provider or customer of an electronic communication service for cost accounting or other like purposes in the ordinary course of its business;
 - "trap and trace device" means a device which captures the incoming electronic or other impulses which identify the originating number of an instrument or device from which a wire or electronic communication was transmitted.
- KAN. STAT. ANN. § 22-2526 (2007) Order, contents of pen register or trap and trace.
- KAN. STAT. ANN. § 22-2527 (2007) Order; issuance; specifications required; duration; extensions; disclosure.
- KAN. STAT. ANN. § 22-2528 (2007) responsibilities of and assistance to authorities by provider, landlord, custodian or other person; compensation; immunity.
- **Computer Statutes**
 - KAN. STAT. ANN. § 21-3755 (2007) Computer crime; computer password disclosure; computer trespass. Intentionally and without authorization accessing and damaging, modifying, altering, destroying, copying, disclosing or taking possession of a computer, computer system, computer network or any other property; using a computer, computer system, computer network or any other property for the purpose of devising or executing a scheme or artifice with the intent to defraud or for the purpose of obtaining money, property, services or any other thing of value by means of false or fraudulent pretense or representation; or intentionally exceeding the limits of authorization and damaging, modifying, altering, destroying, copying, disclosing or taking possession of a computer, computer system, computer network or any other property

- **Common Law**
 - Dotson v. McLaughlin, 531 P.2d 1 (Kan. 1975) - adopts the four strands of the invasion of privacy as set out in the Restatement.

KENTUCKY PRIVACY LAW

- **State Constitutional Privacy Rights**
 - none
- **Search and Seizure**
 - KY. CONST. Bill of Rights § 10 (2009) - Security from search and seizure -- Conditions of issuance of warrant. The people shall be secure in their persons, houses, papers and possessions, from unreasonable search and seizure; and no warrant shall issue to search any place, or seize any person or thing, without describing them as nearly as may be, nor without probable cause supported by oath or affirmation.
 - **Auto Exception**
 - Lynn v. Commonwealth, 257 S.W.3d 596 (Ky. Ct. App. 2008)
 - **Open Fields**
 - Smith v. Commonwealth, 424 S.W.2d 835 (Ky. Ct. App. 1967)
 - **Plain View**
 - Commonwealth v. Johnson, 777 S.W.2d 876 (Ky. 1989)
- **Statutory Privacy Rights**
 - KY. REV. STAT. ANN. § 526.050 (2009) - Tampering with private communications. (1) A person is guilty of tampering with private communications when knowing that he does not have the consent of the sender or receiver, he unlawfully: (a) Opens or reads a sealed letter or other sealed private communication; or (b) Obtains in any manner from an employee, officer or representative of a communications common carrier information with respect to the contents or nature of a communication. (2) The provisions of this section do not apply to the censoring of sealed letters or sealed communications for security purposes in official detention or penal facilities.
 - KY. REV. STAT. ANN. §§ 508.140 and 508.150 (2009) - Stalking. A person makes an explicit or implicit threat with the intent to place that person in reasonable fear of: a. Sexual contact as defined in KRS 510.010; b. Serious physical injury; or c. Death; and there is a protective order issued by the court to protect the same victim.
 - KY. REV. STAT. ANN § 391.170 (2009). Commercial rights to use of names and likenesses of public figures. The General Assembly recognizes that a person has property rights in his name and likeness which are entitled to protection from commercial exploitation. The General Assembly further recognizes that although the traditional right of privacy terminates upon death of the person asserting it, the right of publicity, which is a right of protection from appropriation of some element of an individual's personality for commercial exploitation, does not terminate upon death.
- **Public Records**
 - KY. REV. STAT. ANN. § 61.872 (2009) - All public records shall be open for inspection by any person, except as otherwise provided by KRS 61.870 to 61.884.
 - KY. REV. STAT. ANN. § 61.878 (2009) - exceptions include unwarranted invasions of personal privacy, law enforcement records, investigatory and work product records of agencies, court files of judicial proceedings (working memoranda), personal name/address records (motor vehicle records, health records, etc.), trade

secrets, appraisals, bids, infrastructure or hazardous chemical storage information, archeological, endangered species, libraries, licensing exams, draft legislation, personnel files containing social security information, and information that, if disclosed, would give a reasonable likelihood of threatening the public safety by exposing a vulnerability in preventing, protecting against, mitigating, or responding to a terrorist act.

- No exemption in this section shall be construed to prohibit disclosure of statistical information not descriptive of any readily identifiable person.
 - KY. REV. STAT. ANN. § 61.884 (2009) - Any person shall have access to any public record relating to him or in which he is mentioned by name, upon presentation of appropriate identification, subject to the provisions of KRS 61.878.
 - KY. REV. STAT. ANN. § 61.874 (2009) - It shall be unlawful for a person to obtain a copy of any part of a public record for a: commercial purpose, without stating the commercial purpose if a certified statement from the requestor was required by the public agency.
 - Note that a newspaper, periodical, radio or television station shall not be held to have used or knowingly allowed the use of the public record for a commercial purpose merely because of its publication or broadcast.
 - KY. REV. STAT. ANN. § 133.047 (2009) - the property tax roll, or a copy of the property tax roll, shall be retained in the office of the property valuation administrator for maintenance as an open public record for five (5) years.
 - Personal property tax returns, accompanying documents, and assessment records, with the exception of the certified personal property tax roll, shall be considered confidential under the provisions of KRS 131.190.
 - KY. REV. STAT. ANN. § 131.190 (2009) – In general, information gathered in tax administration shall not be disclosed. However there are exceptions including: Statistics of tax-paid gasoline gallonage reported monthly to the Department of Revenue under the gasoline excise tax law may be made public by the department.
 - KY. REV. STAT. ANN. § 17.150 (2009) - Intelligence and investigative reports are subject to public inspection if the matter is completed. Personal information will be omitted unless of specific importance.
 - KY. REV. STAT. ANN. §65.030 (2009). Record-keeping by computer or other rapid-access data collection system. Notwithstanding any provision of law to the contrary, any unit of state, county or municipal government, or any court, may maintain any records by computer or other rapid-access data collection system, provided that those records which are public records shall be kept in a manner which will allow the public unlimited and speedy access to them.
- **Motor Vehicle Records**
 - KY. REV. STAT. ANN. § 61.878 (2009) (citing Opinion of the Attorney General 95-ORD-151) - Where a private investigator, who was retained by a driver involved in an accident to locate the other driver involved in the collision, requested copies of motor vehicle registration records and records reflecting insurance coverage, the Transportation Cabinet did not violate the Open Records Act by partially denying the private investigator's commercial request since the strong privacy

interest outweighed the nominal public interest which would be served by disclosing the owner's address, birthdate and social security number.

- KY. REV. STAT. ANN. § 61.878 (2009) (citing Opinion of the Attorney General 05-ORD-129) - The Motor Vehicle Enforcement Division of the Justice and Public Safety Cabinet violated the Open Records Act in denying a request for "names, addresses and violation information of all CDL class A drivers that have had out of service violations"; the requester is entitled to a copy of the entire database containing the requested information in standard format, and, in the event the Cabinet elects to redact protected information of a personal nature per KRS 61.878(1)(a), it, rather than the requester, must bear the cost of redaction pursuant to KRS 61.878(4).
- KY. REV. STAT. ANN. § 187.310 (2009) - a certified abstract of the operating record of any person shall be furnished upon request to any person. Accidents reported and traffic offenses within the last three years will be included. The abstracts shall not be admissible as evidence in any action for damages or criminal proceedings arising out of a motor vehicle accident.
- KY. REV. STAT. ANN. § 281A.100 (2009) Commercial driving history may be requested by employers or prospective employers of commercial drivers.
- **Vehicle Identification Numbers**
 - KY. REV. STAT. ANN. § 186A.305 (2009) - Alteration or removal of motor vehicle identification number prohibited.
- **Consumer Credit**
 - KY. REV. STAT. ANN. § 367.310 (2009) Consumer reporting agency records restriction. No consumer reporting agency shall maintain any information in its files relating to any charge in a criminal case, in any court of this Commonwealth, unless the charge has resulted in a conviction.
 - KY. REV. STAT. ANN. § 367.365 (2009) - consumers may put a security freeze on their credit report.
- **Financial Records**
 - KY. REV. STAT. ANN. § 286.6-185 (2009) A credit union has a special obligation of confidentiality to its members; therefore, any contrary provisions of KRS Chapter 271B notwithstanding, a credit union shall be obligated to provide a shareholder only names and addresses of its member shareholders.
 - KY. REV. STAT. ANN. § 286.5-271 (2009) - Every member shall have the right to inspect such books and records of an association as pertain to his loan or savings account. Otherwise, the right of inspection and examination of the books and records shall be limited: (a) To the executive director or his duly authorized representatives as provided in this subtitle; (b) To persons duly authorized to act for the association; and (c) To any federal instrumentality or agency authorized to inspect or examine the books and records of an insured association.
- **Employee Privacy**
 - KY. REV. STAT. ANN. § 351.185 (2009) Confidentiality of drug and alcohol test results -- Exceptions -- Use of results in criminal proceeding against applicant prohibited.
- **Electronic Surveillance**

- KY. REV. STAT. ANN. § 526.010 (2009) Definition. "Eavesdrop" means to overhear, record, amplify or transmit any part of a wire or oral communication of others without the consent of at least one (1) party thereto by means of any electronic, mechanical or other device.
- KY. REV. STAT. ANN. § 526.020 (2009) Eavesdropping. A person is guilty of eavesdropping, a felony, when he intentionally uses any device to eavesdrop.
- KY. REV. STAT. ANN. § 526.030 (2009) Installing eavesdropping device
- KY. REV. STAT. ANN. § 526.040 (2009) Possession of eavesdropping device
- KY. REV. STAT. ANN. § 526.060 (2009) Divulging illegally obtained information
- KY. REV. STAT. ANN. § 526.070 (2009) Eavesdropping; exceptions. Inadvertently overhears the communication through a regularly installed telephone party line or on a telephone extension but does not divulge it; or (2) Is an employee of a communications common carrier who, while acting in the course of his employment, intercepts, discloses or uses a communication transmitted.
- **Computer Statutes**
 - KY. REV. STAT. ANN. § 434.845 (2009) - A person is guilty of unlawful access to a computer in the first degree when he or she, without the effective consent of the owner, knowingly and willfully, directly or indirectly accesses, causes to be accessed, or attempts to access any computer software, computer program, data, computer, computer system, computer network, or any part thereof, for the purpose of: (a) Devising or executing any scheme or artifice to defraud; or (b) Obtaining money, property, or services for themselves or another by means of false or fraudulent pretenses, representations, or promises.
 - KY. REV. STAT. ANN. § 434.850 (2009) a person is guilty of unlawful access to a computer in the second degree when he or she, without the effective consent of the owner, knowingly and willfully, directly or indirectly accesses, causes to be accessed, or attempts to access any computer software, computer program, data, computer, computer system, computer network, or any part thereof, which results in the loss or damage of three hundred dollars (\$300) or more.
 - KY. REV. STAT. ANN. § 434.855 (2009) Misuse of computer information. (1) A person is guilty of misuse of computer information when he or she: (a) Receives, conceals, or uses, or aids another in doing so, any proceeds of a violation of KRS 434.845; or (b) Receives, conceals, or uses or aids another in doing so, any books, records, documents, property, financial instrument, computer software, computer program, or other material, property, or objects, knowing the same to have been used in or obtained from a violation.
- **Common Law**
 - McCall v. Courier-Journal & Louisville Times, 623 S.W.2d 882 (Ky. 1981) - accepts the four strands of the invasion of privacy as set out by the Restatement.

LOUISIANA PRIVACY LAW

- **State Constitutional Privacy Rights**
 - **Express**
 - LA. CONST. art. I, § 5 (2008) - Right to privacy. Every person shall be secure in his person, property, communications, houses, papers, and effects against unreasonable searches, seizures, or invasions of privacy.
 - **Implied**
 - Parish Nat'l Bank v. Lane, 397 So. 2d 1282 (La. 1981) - The Louisiana Constitution protects against private as well as government actions that infringe privacy.
- **Search and Seizure**
 - LA. CONST. art. I, § 5 (2008) - protections against unreasonable searches or seizures.
 - State v. Jackson, 764 So. 2d 64 (La. 2000) - DWI roadblocks are a valid law enforcement tool when conducted pursuant to neutral guidelines that limit the discretion of the officer in the field
 - **Auto Exception**
 - State v. Fearheiley, 979 So. 2d 487(La. 2008)
 - **Open Fields**
 - State v. Stokes, 511 So.2d 1317 (La. Ct. App. 1987)
 - **Plain View**
 - State v. Cunningham, 511 So.2d 1317 (La. Ct. App. 1987)
- **Statutory Privacy Rights**
 - LA. REV. STAT. ANN. § 14:40.2 (2008) - Stalking is the intentional and repeated following or harassing of another person that would cause a reasonable person to feel alarmed or to suffer emotional distress. Stalking shall include but not be limited to the intentional and repeated uninvited presence of the perpetrator at another person's home, workplace, school, or any place which would cause a reasonable person to be alarmed, or to suffer emotional distress as a result of verbal or behaviorally implied threats of death, bodily injury, sexual assault, kidnapping, or any other statutory criminal act to himself or any member of his family or any person with whom he is acquainted.
 - LA. REV. STAT. ANN. § 51:2021 (2008) Louisiana Anti-phishing Act. A person may not, with the intent to engage in conduct involving the fraudulent use or possession of another person's identifying information: (1) Create a Web page or Internet domain name that is represented as a legitimate online business without the authorization of the registered owner of the business. (2) Use that Web page or a link to the Web page, that domain name, or another site on the Internet to induce, request, or solicit another person to provide identifying information for a purpose that the other person believes is legitimate.
 - LA. REV. STAT. ANN. § 51:2033 (2008). Unlawful requests by misrepresentation. It shall be unlawful for any person, by means of a web page, electronic mail message, or otherwise through use of the Internet, to solicit, request, or take any action to induce another person to provide identifying information by representing itself to be a business without the authority or approval of the business.
- **Individually Identifiable Government Records**

- LA. REV. STAT. ANN. § 15:578 (2008) Criminal history records are confidential.
- LA. REV. STAT. ANN. § 23:1293 (2008) Medical records and worker's compensation payment records are confidential.
- **Public Records**
 - LA. REV. STAT. ANN. § 44:1 (2008) - All records are open unless specifically provided by law. Exceptions are provided in § 44:2 through 44:23 and include hospital records and trade secret information, arrest records and pending litigation issues.
 - Webb v. City of Shreveport, 371 So.2d 316 (La. Ct. App. 1979) All records are public unless excepted by law or if someone has a reasonable expectation of privacy in the documents.
- **Motor Vehicle Records**
 - LA. REV. STAT. ANN. § 32:393.1 (2008) - Records of traffic offenses and license records are public.
 - LA. REV. STAT. ANN. § 32:398 (2008) The state police, any local police department, or any sheriff's office shall provide copies of crash reports to any interested person upon request and may charge a fee, not to exceed the sum of five dollars per report that does not exceed two pages, and seven dollars and fifty cents per report that exceeds two pages. The state police, any local police department, or any sheriff's office shall provide copies of photographs of accidents or other photographs required of the investigating agency, video tapes, audio tapes, and any extraordinary-sized documents, or documents stored on electronic media, to any interested person upon request and may charge a reasonable fee for such copies.
- **Vehicle Identification Numbers**
 - State v. Reed, 483 So.2d 1278 (La. Ct. App. 1986) Lifting the hood to view the VIN was not a search.
 - LA. REV. STAT. ANN. § 14:207 (2008) No person shall cover, remove, deface, alter, or destroy the manufacturer's number or any other distinguishing number or identification mark on any motor vehicle or motor vehicle part for the purpose of concealing or misrepresenting its identity; nor shall any person buy, sell, receive, dispose of, conceal, or knowingly have in his possession any motor vehicle or motor vehicle part from or on which the manufacturer's number or any other distinguishing number or identification mark has been covered, removed, defaced, altered, or destroyed for the purpose of concealing or misrepresenting its identity.
- **Consumer Credit**
 - LA. REV. STAT. ANN. § 9:3571 (2008). A savings bank, a savings and loan association, a company issuing credit cards, or a business offering credit shall disclose financial records of its customers only pursuant to R.S. 6:333.
 - LA. REV. STAT. ANN. § 9:3571.1 (2008). Every consumer has the right to receive a copy of his credit report and the agency must comply with the request.
 - LA. REV. STAT. ANN. § 51:3074 (2008) Any person that conducts business in the state or that owns or licenses computerized data that includes personal information, or any agency that owns or licenses computerized data that includes personal information, shall, following discovery of a breach in the security of the system containing such data, notify any resident of the state whose personal

electromagnetic, photoelectronic, or photo-optical system, but does not include any of the following: (i) Any oral communication. (ii) Any communication made through a tone-only paging device. (iii) Any communication from a tracking device used to locate a mobile object by emission of a sound signal.

- LA. REV. STAT. ANN. § 15:1303 (2008) Interception and disclosure of wire, electronic, or oral communications. Ok for FCC and telecommunications employees to intercept in accordance with their jobs, or if one party has consented to the interception. Law enforcement if acting under a court order may use and transfer such information to other law enforcement officers. No otherwise privileged wire, oral, or electronic communication intercepted in accordance with, or in violation of, the provisions of this Chapter shall lose its privileged character.
- LA. REV. STAT. ANN. § 15:1304 (2008) Manufacture, distribution, or possession of wire or oral communication intercepting devices prohibited.
- LA. REV. STAT. ANN. 15:1305 (2008) Confiscation of wire or oral communication intercepting devices.
- LA. REV. STAT. ANN. 15:1307 (2008) Prohibition of use as evidence of intercepted wire or oral communications.
- LA. REV. STAT. ANN. 15:1308 (2008) Authorization for interception of wire or oral communications. The attorney general can apply for and order to intercept, but can only do so for certain enumerated crimes such as terrorism, money laundering and drug crimes.
- LA. REV. STAT. ANN. 15:1309 (2008) Authorization for disclosure and use of intercepted wire or oral communications.
- LA. REV. STAT. ANN. 15:1310 (2008) Procedure for interception of wire or oral communications.
- **Computer Statutes**
 - LA. REV. STAT. ANN. § 14:73.2 (2008). Offenses against intellectual property. An offense against intellectual property is the intentional: (1) Destruction, insertion, or modification, without consent, of intellectual property; or (2) Disclosure, use, copying, taking, or accessing, without consent, of intellectual property.
- **Common Law**
 - Taylor v. State, 617 So. 2d 1198 (La. Ct. App. 1993) - recognizes the four strands of the common law tort of invasion of privacy. The right to privacy embraces four different interests: (1) an invasion takes place by the appropriation of an individual's name or likeness for the use or benefit of another; (2) an invasion occurs when the defendant unreasonably intrudes upon the plaintiff's physical solitude or seclusion; (3) an invasion of privacy occurs through publicity which unreasonably places the plaintiff in a false light before the public; and (4) an invasion of privacy takes place by the unreasonable public disclosure of embarrassing private facts.

MAINE PRIVACY LAW

- **State Constitutional Privacy Rights**
 - none
 - **Implied**
 - ME. CONST. art. I, § 6 (2008) - right against self incrimination
- **Search and Seizure**
 - ME. CONST. art. I, § 5 (2008) - Security from search and seizure -- Conditions of issuance of warrant. The people shall be secure in their persons, houses, papers and possessions, from unreasonable search and seizure; and no warrant shall issue to search any place, or seize any person or thing, without describing them as nearly as may be, nor without probable cause supported by oath or affirmation.
 - State v. Philbrick, 436 A.2d 844 (Me. 1981) - abandoned property may be searched without a warrant. *But see* State v. Chapman, 250 A.2d 203 (Me. 1969) where something is placed in a trash barrel in a certain position, it will not constitute abandonment.
 - **Auto Exception**
 - State v. Melvin, 955 A.2d 245 (Me. 2008)
 - **Open Fields**
 - State v. Pease, 520 A.2d 698 (Me. 1987).
 - **Plain View**
 - State v. Cloutier, 544 A.2d 1277 (Me. 1988).
 - State v. Cote, 518 A.2d 454 (Me. 1986) Stating that the VIN may be checked by an officer standing outside the car because it is in plain view. The United States Supreme Court recently held in New York v. Class, 475 U.S. 106 (1986), that there is no reasonable expectation of privacy in a VIN because it is in plain view of someone standing outside the automobile. The court stated it is "unreasonable to have an expectation of privacy in an object required by law to be located in a place ordinarily in plain view from the exterior of the automobile" and ". . . to examine it does not constitute a search." *Id.* Fearon
- **Statutory Privacy Rights**
 - ME. REV. STAT. ANN. tit. 17-A, § 210-A (2008) - A person is guilty of stalking if: The actor intentionally or knowingly engages in a course of conduct directed at a specific person that would in fact cause both a reasonable person and that other specific person: 1) To suffer intimidation or serious inconvenience, annoyance or alarm; 2) To fear bodily injury or to fear bodily injury to a member of that person's immediate family; or 3) To fear death or to fear the death of a member of that person's immediate family.
 - ME. REV. STAT. ANN. tit. 24, §§ 2202 through 2220 (2008) - Insurance Information and Privacy Protection Act. The purpose of this chapter is to establish standards for the collection, use and disclosure of information gathered in connection with insurance transactions; to maintain a balance between insurance carriers' need for information and the public's need for fair information practices that respect privacy; to establish a regulatory mechanism to enable insurance consumers to ascertain what information is being collected about them and to verify its accuracy; to limit the distribution of information collected in connection

with insurance transactions; and to enable consumers to obtain the reasons for adverse underwriting decisions.

- ME. REV. STAT. ANN. tit. 35-A, § 114 (2008) - Materials prepared for and used specifically in the examination or evaluation of applicants for positions with a public utility, including working papers, research materials, records and examinations; and personnel records containing certain private material.
- ME. REV. STAT. ANN. tit. 35-A, § 7101-A (2008) - Telecommunications privacy; policy. The Legislature declares and finds the following. 1. Privacy Right. Telephone subscribers have a right to privacy and the protection of this right to privacy is of paramount concern to the State. 2. Exercise of Right. To exercise their right to privacy, telephone subscribers must be able to limit the dissemination of their telephone numbers to persons of their choosing.
- ME. REV. STAT. ANN. tit. 5, § 4612 (2008) - Confidentiality of 3rd-Party Records. The Legislature finds that persons who are not parties to a complaint under this chapter [unlawful discrimination] as a complainant or a person accused of discrimination have a right to privacy. Any records of the commission which are open to the public under Title 1, chapter 13, shall be kept in such a manner as to ensure that data identifying these 3rd parties is not reflected in the record.
- ME. REV. STAT. ANN. tit. 17-A, § 511 (2008) - person is guilty of violation of privacy if, except in the execution of a public duty or as authorized by law, that person intentionally: A. Commits a civil trespass on property with the intent to overhear or observe any person in a private place; B. Installs or uses in a private place without the consent any device for observing, photographing, recording, amplifying or broadcasting sounds or events in that place; C. Installs or uses outside a private place without the consent any device for hearing, recording, amplifying or broadcasting sounds originating in that place that would not ordinarily be audible or comprehensible outside that place; or D. Engages in visual surveillance in a public place by means of mechanical or electronic equipment with the intent to observe any part of a person concealed from public view under clothing.
- **Individually Identifiable Records**
 - ME. REV. STAT. ANN. tit. 10, § 1346 though § 1350-A (2008) - Notification of security breach of personal information. If an information broker that maintains computerized data that includes personal information becomes aware of a breach of the security of the system, the information broker shall conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused and shall give notice of a breach of the security of the system following discovery or notification of the security breach to a resident of this State whose personal information has been, or is reasonably believed to have been, acquired by an unauthorized person.
- **Public Records**
 - ME. REV. STAT. ANN. tit. 1, §§ 401 through 412 (2008) - The state declares a policy that legislative actions and records are open to inspection.
 - The term "public records" means any written, printed or graphic matter or any mechanical or electronic data compilation from which information can be obtained, directly or after translation into a form susceptible of visual

or aural comprehension, that is in the possession or custody of an agency or public official of this State or any of its political subdivisions, or is in the possession or custody of an association, the membership of which is composed exclusively of one or more of any of these entities, and has been received or prepared for use in connection with the transaction of public or governmental business or contains information relating to the transaction of public or governmental business.

- Exemptions which include any confidential information stated by statute, records in preparation for a pending litigation, negotiations of the state in making contracts, medical records, social security records etc.

- **Motor Vehicle Records**

- ME. REV. STAT. ANN. tit. 29-A § 2251 (2008) Disclosure of accident reports. An accident report made by an investigating officer or a 48-hour report made by an operator as required by former subsection 5 is for the purposes of statistical analysis and accident prevention. A report or statement contained in the accident report, or a 48-hour report as required by former subsection 5, a statement made or testimony taken at a hearing before the Secretary of State held under section 2483, or a decision made as a result of that report, statement or testimony may not be admitted in evidence in any trial, civil or criminal, arising out of the accident. A report may be admissible in evidence solely to prove compliance with this section. The Chief of the State Police may disclose the date, time and location of the accident and the names and addresses of operators, owners, injured persons, witnesses and the investigating officer. On written request, the chief may furnish a photocopy of the investigating officer's report at the expense of the person making the request.
- ME. REV. STAT. ANN. tit. 29-A § 2521 (2008) - implied consent to chemical tests if there is probable cause.

- **Vehicle Identification Numbers**

- ME. REV. STAT. ANN. tit. 29-A, § 751 (2008) illegal to sell or exchange, offer to sell or exchange, or give away a certificate of title, certificate of salvage, certificate of lien, or vehicle identification number plate.

- **Consumer Credit**

- ME. REV. STAT. ANN. tit. 10, §§ 1311 through 1330 (2008) - Fair Credit Reporting Act. There is a need to ensure that consumer reporting agencies exercise their grave responsibilities with fairness, impartiality and a respect for the consumer's right to privacy. Act includes rules on consumer disclosure, procedures for correcting information, permission for a consumer to institute a security freeze on an account, prohibition from furnishing reports that contain medical information, and permissible parties to release information to including for employment purposes.
- ME. REV. STAT. ANN. tit. 9-A, § 8-304 (2008) it is unlawful for a person, business, corporation, partnership, agency, financial institution, credit card registration service or other entity to rent, sell, exchange or otherwise disclose or make available to another person or entity a list containing the names, addresses and account numbers of credit card holders without the express, written permission of the credit card holders. Some exceptions apply including to a parent company.

- **Financial Records**
 - ME. REV. STAT. ANN. tit. 9-B, §§ 161 through 164 (2008) - A financial institution authorized to do business in this State or credit union authorized to do business in this State or its affiliates may not disclose to any person, except to the customer or the customer's duly authorized agent, any financial records relating to that customer of that financial institution or credit union unless the request is from certain parties including the owner of the record, a legal proceeding, the dept of labor, or to human services in suspicion of financial exploitation.
- **Employee Privacy**
 - ME. REV. STAT. ANN. tit. 26, § 681 through § 690 (2008) - The purpose of this chapter is to protect the privacy rights of individual employees in the State from undue invasion by employers through the use of substance abuse tests while allowing the use of tests when the employer has a compelling reason to administer a test. Results are confidential and may not be released except to the employee unless he consents. Exceptions to release information under state or federal law, or in a grievance procedure.
- **Electronic Surveillance - Doesn't specifically discuss Electronic Communications**
 - ME. REV. STAT. ANN. tit. 15, §§ 710, 712 (2008) - Interception of wire and oral communication is a crime unless by a common carrier in the course of employment or by law enforcement.
- **Computer Statutes**
 - ME. REV. STAT. ANN. tit. 17-A, §§ 432, 433 (2008) - Criminal investigation of computer privacy occurs when a person intentionally accesses any computer resource without authorization. It becomes an aggravated crime if the computer software or programs or hardware is copied, damaged, or altered, or if a virus is introduced.
- **Common Law**
 - **Appropriation**
 - Equifax Svcs. v. Cohen, 420 A.2d 189 (Me. 1980).
 - **Disclosure**
 - Loe v. Town of Thomaston, 600 A.2d 1090 (Me. 1991).
 - **False Light**
 - Estate of Berthiaume v. Pratt, 365 A.2d 792 (Me. 1976).
 - **Intrusion**
 - Estate of Berthiaume v. Pratt, 365 A.2d 792 (Me. 1976).

MARYLAND PRIVACY LAW

- **State Constitutional Privacy Rights**
 - none
- **Search and Seizure**
 - MD. CONST. Declaration of Rights. art. 26. Warrants to search and seize may only be granted if there is a name or description of the place or person.
 - **Auto Exception**
 - Nathan v. State, 805 A.2d 1086 (Md. Ct. App. 2003).
 - **Open Fields**
 - Brown v. State, 540 A.2d 143 (Md. Ct. Spec. App. 1988).
 - **Plain View**
 - Liichowv. State, 419 A.2d 1041 (Md. 1980).
- **Statutory Privacy Rights**
 - MD. CODE ANN., CRIM. LAW [§ 3-801 through -806 \(2008\)](#) - Stalking means a malicious course of conduct that includes approaching or pursuing another where the person intends to place or knows or reasonably should have known the conduct would place another in reasonable fear of death, rape or serious bodily injury. Includes contacts through electronic mail and the telephone.
 - MD. CODE ANN., CRIM. LAW § 8-301 (2008) Identity fraud is a crime.
- **Individually Identifiable Records**
 - MD. CODE ANN., STATE GOV'T § 10-624 (2008) - Personal records defined, and administrative procedure for correcting and ensuring correct information.
 - MD. CODE ANN., COM. LAW § 14-3401 through 3402 (2008) - Social Security Protection Act. Public display is prohibited.
- **Public Records**
 - MD. CODE ANN., STATE GOV'T § 10-612 (2008) public inspection of records allowed.
 - MD. CODE ANN., STATE GOV'T § 10-626 through 10-628 (2008) - unlawful disclosure of public records if the record contains a personally identifying factor.
 - MD. CODE ANN., STATE GOV'T § 10-616 (2008). Specific records that the records custodian must deny access to including: adoption records, welfare records, certain police records, motor vehicle records containing personal information (except for certain narrow purposes in connection with emissions, safety and theft of vehicles), etc.
 - MD. CODE ANN., STATE GOV'T § 10-617 (2008) - certain records containing specific information must be denied disclosure, including personnel information, medical records, trade secrets and financial information. Names, addresses and telephone numbers of professionally qualified license holders will be disclosed. Possible to petition for the release of more information if there is a compelling reason for the public purpose.
- **Motor Vehicle Records**
 - MD. CODE ANN., STATE GOV'T § 10-616 (2008) - cannot disclose motor vehicle records containing personal information. Some narrow exceptions apply.
 - MD. CODE ANN., TRANSP. § 13-107 (2008) - Certificates of title shall contain VIN.
- **Vehicle Identification Numbers**

- MD. CODE ANN., TRANSP. § 13-107 (2008) - Certificates of title shall contain VIN.
- MD. CODE ANN., TRANSP. § 14-107 (2008) - illegal to use or transfer a vehicle with a removed or damaged VIN.
- State v. Sedacca, 249 A.2d 456 (Md. 1969) - routine checks of VIN are permissible during traffic stops because the number is visible.
- **Consumer Credit**
 - MD. CODE ANN., COM. LAW § 14-1202 (2008) Permissible uses of consumer reports. Under court order, or if the consumer requests to use the report for certain purposes. May request the reporting agency to not provide the information to any marketing or mailing firm.
 - MD. CODE ANN., COM. LAW § 14-1204 (2008) Investigative consumer reports may not be prepared or disclosed unless for employment purposes. Any entity making this request must inform the consumer.
 - MD. CODE ANN., COM. LAW § 14-1206 (2008) - must disclose to the consumer a copy of any file about the consumer. May not contain medical information. The consumer reporting agency may delete the sources of information acquired solely for use in an investigative report and used for no other purpose.
 - MD. CODE ANN., COM. LAW § 14-1207 (2008) - Except as provided in § 14-1213 of this subtitle, no consumer may bring any action or proceeding in the nature of defamation, invasion of privacy, or negligence with respect to the reporting of information against any consumer reporting agency, any user of information, based on information disclosed pursuant to this section. Unless false information is maliciously or intentionally reported.
 - MD. CODE ANN., COM. LAW § 14-1212 (2008) - must inform consumer if credit is denied due to information the reporting agency provided.
 - MD. CODE ANN., COM. LAW § 1213; 1216 (2008) - causes of action.
 - MD. CODE ANN., COM. LAW §§ 14-3501 through -3508 (2008) Maryland Personal Information Protection Act. Requires notification to the consumer if an entity that maintains personal information data has a security breach without delay.
 - MD. CODE ANN., COM. LAW § 14-1212.1 (2008) Permits Maryland residents to put a security freeze by placing a restriction on a consumer's consumer report at the request of the consumer that prohibits a consumer reporting agency from releasing the consumer's consumer report or any information derived from the consumer's consumer report without the express authorization of the consumer.
- **Financial Records**
 - MD. CONST. art. III, § 39 (2008) - The books, papers and accounts of all banks shall be open to inspection under such regulations as may be prescribed by law.
 - MD. CODE ANN., FIN INST. § 1-302 (2008) - Unless otherwise permitted, a financial institution may not disclose any financial record relating to a customer.
 - MD. CODE ANN., FIN INST. § 1-303 (2008) enumerates permissible disclosures including consent and between bank employees.
 - MD. CODE ANN., FIN INST. § 1-305 (2008) crime to disclose such information
- **Employee Privacy**
 - MD. CODE ANN., HEALTH-GEN. § 17-214 (2008) - Confidentiality. Except as provided in paragraphs (2) and (3) of this subsection, in the course of obtaining

information for, or as a result of, conducting job-related alcohol or controlled dangerous substance testing for an employer under this section, a laboratory, a physician, including a physician retained by the employer, or any other person may not reveal to the employer information regarding: (i) The use of a nonprescription drug, excluding alcohol, that is not prohibited under the laws of the State; or (ii) The use of a medically prescribed drug, unless the person being tested is unable to establish that the drug was medically prescribed under the laws of the State. But, if the test operator notifies the applicant that if the preliminary test is positive, the applicant may voluntarily disclose and provide documentation to the operator that the applicant is taking a legally prescribed medication.

- **Electronic Surveillance**

- MD. CODE ANN., CTS. & JUD. PROC. § 10-401 (2008) Definitions. (i) "Electronic communication" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system. (ii) "Electronic communication" does not include: 1. Any wire or oral communication; 2. Any communication made through a tone-only paging device; or 3. Any communication from a tracking device.
- MD. CODE ANN., CTS. & JUD. PROC. § 10-402 (2008) Wiretapping generally. Unlawful to Willfully intercept, endeavor to intercept, or procure any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication unless a telecommunications carrier acting in the course of business, a law enforcement officer with an order listening for an enumerated crime including gambling, murder, fraudulent insurance act, etc.
- MD. CODE ANN., CTS. & JUD. PROC. § 10-403 (2008) Wiretapping device; prohibited acts.
- MD. CODE ANN., CTS. & JUD. PROC. § 10-404 (2008) Confiscation of prohibited device.
- MD. CODE ANN., CTS. & JUD. PROC. § 10-405 (2008) Wiretapped communications not admissible. Unless conducted lawfully.
- MD. CODE ANN., CTS. & JUD. PROC. § 10-406 (2008) Authorized interception; to whom granted. Attorney general, state prosecutor, etc., may apply for an order allowing interception to a judge in the appropriate jurisdiction.
- MD. CODE ANN., CTS. & JUD. PROC. § 10-407 (2008) Legal uses of intercepted communication
- MD. CODE ANN., CTS. & JUD. PROC. § 10-408 (2008) Permitted interception; ex parte order
- MD. CODE ANN., CTS. & JUD. PROC. § 10-409 (2008) Authorized interceptions; submission of reports
- MD. CODE ANN., CTS. & JUD. PROC. § 10-410 (2008) Wrongful interception; civil liability; defenses
- MD. CODE ANN., CTS. & JUD. PROC. § 10-4A-03 (2008) - Except as provided, it is unlawful for a person providing an electronic communication service to divulge to any other person the contents of a communication while the communication is in electronic storage by that service.

- MD. CODE ANN., CTS. & JUD. PROC. § 10-4A-04 (2008) - Lawful to communicate contents of recordings among law enforcement officers. Telecommunications employees may disclose to law enforcement only under a subpoena.
- MD. CODE ANN., CTS. & JUD. PROC. § 10-4B-01 through -05 (2008) - Process for using a pen register or a trap and trace device.
- **Computer Statutes**
 - MD. CODE ANN., CRIM. LAW § 7-302 (2008) - unauthorized access to computers and related material is a crime
- **Common Law**
 - Lawrence v. Abell Co., 475 A.2d 448 (Md. 1984) accepts the four strands of common law tort of invasion of privacy.

MASSACHUSETTS PRIVACY LAW

- **State Constitutional Privacy Rights**
 - none
- **Search and Seizure**
 - MASS. CONST. Pt. 1, art. XIV, § 43 - right of search and seizure regulated.
 - **Auto Exception**
 - Commonwealth v. Bostock, 880 N.E.2d 759 (Mass. 2008).
 - **Open Fields**
 - Commonwealth v. Ortiz, 380 N.E.2d 669 (Mass. 1978).
 - **Plain View**
 - Commonwealth v. Young, 416 N.E.2d 944 (Mass. 1981).
- **Statutory Privacy Rights**
 - MASS. GEN. LAWS ANN. ch. 272, § 43 (2009) - Whoever (1) willfully and maliciously engages in a knowing pattern of conduct or series of acts over a period of time directed at a specific person which seriously alarms or annoys that person and would cause a reasonable person to suffer substantial emotional distress, and (2) makes a threat with the intent to place the person in imminent fear of death or bodily injury, shall be guilty of the crime of stalking and shall be punished by imprisonment in the state prison for not more than five years or by a fine of not more than one thousand dollars, or imprisonment in the house of correction for not more than two and one-half years or both. Such conduct, acts or threats described in this paragraph shall include, but not be limited to, conduct, acts or threats conducted by mail or by use of a telephonic or telecommunication device including, but not limited to, electronic mail, internet communications and facsimile communications.
 - MASS. GEN. LAWS ANN. ch. 214, § 1B (2009) - A person shall have a right against unreasonable, substantial or serious interference with his privacy. The superior court shall have jurisdiction in equity to enforce such right and in connection therewith to award damages.
- **Public Records**
 - MASS. GEN. LAWS ANN. ch. 66, § 10 (2009) - Records open for public inspection. Custodian must make records available.
 - MASS. GEN. LAWS ANN. ch. 4, § 7 (2009) - definition of public record. Exemptions include personal information, listings of named individuals and anything that would constitute an unwarranted invasion of privacy.
 - MASS. REGS. CODE tit. 950, § 32.05 (2009) - A custodian of a public record shall permit all public records within his or her custody to be inspected or copied by any person during regular business hours. In governmental entities which do not have daily business hours, a written notice shall be posted in a conspicuous location listing the name, position, address and telephone number of the person to be contacted to obtain access to public records. There is a prohibition of Custodial Requests for Background Information, so the custodian cannot ask why the person wants the record.
- **Motor Vehicle Records**
 - MASS. GEN. LAWS ANN. ch. 90, § 8 (2009) - information requirements to obtain licenses and junior licenses.

- Doe v. Registrar of Motor Vehicles, 528 N.E.2d 880 (Mass App. Ct. 1988) - information required by the Dept of Motor Vehicles may not be sold to anyone unless disclosure is not an unwarranted invasion of privacy.
- **Vehicle Identification Numbers**
 - MASS. GEN. LAWS ANN. ch. 90, § 7R (2009) All motor vehicles, and all trailers and semi-trailers manufactured for the model year nineteen hundred and seventy-nine and thereafter and registered under the provisions of sections two to five, inclusive, shall be equipped with and display a vehicle identification number, in accordance with such minimum requirements and design as the registrar may prescribe under rules and regulations made by him.
 - MASS. GEN. LAWS ANN. ch. 175, § 113S (2009) - Motor vehicle liability coverage shall not be provided for theft unless inspections have included taking a physical imprint or recording of the VIN.
- **Consumer Credit**
 - MASS. GEN. LAWS ANN. ch. 93, § 53 (2009) - cannot cause investigation report of any consumer unless disclosed to that consumer.
 - MASS. GEN. LAWS ANN. ch. 93, § 55 (2009) - consumer report may furnish certain personally identifying information about a consumer to a government agency including name, address, etc.
 - MASS. GEN. LAWS ANN. ch. 93, § 62A (2009) - permits a consumer to request a security freeze.
 - MASS. GEN. LAWS ANN. ch. 9-H, § 1 through 6(2009) - Notification of Security Breach to consumers where personal information was likely acquired.
 - "Breach of security", the unauthorized acquisition or unauthorized use of unencrypted data or, encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information, maintained by a person or agency that creates a substantial risk of identity theft or fraud against a resident of the commonwealth.
 - A good faith but unauthorized acquisition of personal information by a person or agency, or employee or agent thereof, for the lawful purposes of such person or agency, is not a breach of security unless the personal information is used in an unauthorized manner or subject to further unauthorized disclosure.
- **Financial Records**
 - MASS. GEN. LAWS ANN. 62E, § 14 (2009) - Commissioner may request information on account holders and the bank shall not disclose to a depositor or an account holder that the name of such person has been received from or furnished to the commissioner; provided, however, that an institution may disclose to its depositors or account holders that under the financial institution match system the commissioner has the authority to request certain identifying information on certain depositors or account holders.
 - MASS. GEN. LAWS ANN. ch. 119A, § 14 (2009). Agency Authorized to Obtain Certain Information to Assist in Administration of Child Support Enforcement. Certain records held by private entities with respect to individuals who owe or are owed support (or against or with respect to whom a support obligation is sought),

consisting of the names and addresses of such individuals and the names and addresses of the employers of such individuals as appearing in customer records of public utilities and cable television companies, pursuant to an administrative subpoena authorized by section 15; and information (including information on assets and liabilities) on such individuals held by financial institutions.

- **Employee Privacy**
 - none
- **Electronic Surveillance**
 - MASS. GEN. LAWS ANN. ch. 272, § 99 (2009) - Interception of wire and oral communications. Unlawful to willfully commit an interception, attempts to commit an interception, or procures any other person to commit an interception or to attempt to commit an interception of any wire or oral communication. Or to improperly disclose the interception. Exceptions for law enforcement, communications carriers, and for a financial institution to record telephone communications with its corporate or institutional trading partners in the ordinary course of its business.
 - The general court further finds that the uncontrolled development and unrestricted use of modern electronic surveillance devices pose grave dangers to the privacy of all citizens of the commonwealth. Therefore, the secret use of such devices by private individuals must be prohibited. The use of such devices by law enforcement officials must be conducted under strict judicial supervision and should be limited to the investigation of organized crime.
- **Computer Statutes**
 - MASS. GEN. LAWS ANN. ch. 266, § 33A (2009) - Fraudulent Obtaining of Commercial Computer Service
 - MASS. GEN. LAWS ANN. ch. 266, § 120F (2009) - Unauthorized Accessing of Computer Systems; Penalty; Password Requirement as Notice
 - MASS. GEN. LAWS ANN. ch. 266, § 30 (2009) in terms of larceny, property includes electronically processed or stored data, either tangible or intangible, data while in transit, telecommunications services
- **Common Law**
 - **Appropriation**
 - Tropeano v. Atlantic Monthly Co., 400 N.E.2d 847(Mass. 1980).
 - **Disclosure**
 - Jones v. Taibbi, 512 N.E.2d 260 (Mass. 1987).
 - **False Light**
 - Ayash v. Dana-Farber Cancer Inst., 822 N.E.2d 667(Mass. 1989) - evaluating the false light common law claim in the backdrop of MASS. GEN. LAWS ANN. ch. 214, § 1B (2009). Ultimately held there was no invasion of privacy. Probably doesn't accept the common law version of this tort.
 - **Intrusion**
 - Schlesinger v. Merrill Lynch, 567 N.E.2d 912 (Mass. 1991)

MICHIGAN PRIVACY LAW

- **State Constitutional Privacy Rights**
 - none
- **Search and Seizure**
 - MICH. CONST. art. I, § 11 Protects against unreasonable search and seizure.
 - State v. Thivierge, 435 N.W.2d 446 (Mich. Ct. App. 1988) - searches of curbside trash is permissible.
 - **Auto Exception**
 - People v. King, 612 N.W.2d 159 (Mich. 2000)
 - **Open Fields**
 - People v. Rotar, 357 N.W.2d 885 (Mich. Ct. App. 1984).
 - **Plain View**
 - People v. Secrest, 321 N.W.2d 368 (Mich. Ct. App. 1984).
- **Statutory Privacy Rights**
 - MICH. COMP. LAWS. ANN. § 750.411h (2009) "Stalking" means a willful course of conduct involving repeated or continuing harassment of another individual that would cause a reasonable person to feel terrorized, frightened, intimidated, threatened, harassed, or molested and that actually causes the victim to feel terrorized, frightened, intimidated, threatened, harassed, or molested.
- **Public Records**
 - MICH. COMP. LAWS. ANN. § 15.231 (2009) Freedom of Information Act.
 - MICH. COMP. LAWS. ANN. § 15.233 (2009) - except as provided public records are open to the public for inspection and copying.
 - MICH. COMP. LAWS. ANN. § 15.243 (2009) Freedom of Information Act Exemptions from disclosure including social security numbers, financial records, trade secrets and pending criminal investigation and other unwarranted invasions of personal privacy.
 - MICH. COMP. LAWS. ANN. § 400.64 (2009) The Social Welfare Act. applications and records concerning an applicant for or recipient of aid or relief under the terms of this act, except medical assistance, shall be considered public records and shall be open to inspection by persons authorized by the federal or state government, the state department of social services, or the officials of the county, city, or district involved, in connection with their official acts and by the general public as to the names of recipients and the amounts of aid or relief granted.
 - MICH. COMP. LAWS. ANN. § 445.85 (2009). Exemption from disclosure. All or more than 4 sequential digits of a social security number contained in a public record are exempt from disclosure under the Freedom of Information Act.
- **Motor Vehicle Records**
 - Michigan courts have held that the disclosure of traffic reports can constitute an unwarranted invasion of personal privacy and therefore government entities are not required to make these reports public. Mich. Rehab. Clinic Inc., P.C. v City of Detroit, 310 F Supp 2d 867 (E.D. Mich 2004) (interpreting state law)
 - MICH. COMP. LAWS. ANN. § 257.232 (2009) Upon request, the secretary of state may furnish a list of information from the records of the department maintained under this act to a federal, state, or local governmental agency for use in carrying

out the agency's functions, or to a private person or entity acting on behalf of a governmental agency for use in carrying out the agency's functions.

- The secretary of state may contract for the sale of lists of driver and motor vehicle records and other records maintained under this act in bulk for purposes permitted by and described in section 208c(3). The secretary of state shall fix a market-based price for the sale of such lists or other records maintained in bulk, which may include personal information.
 - The secretary of state or any other state agency shall not sell or furnish any list of information under subsection (2) for the purpose of surveys, marketing, and solicitations. The secretary of state shall ensure that personal information disclosed in bulk will be used, rented, or sold solely for uses permitted under this act.
 - MICH. COMP. LAWS. ANN. § 257.208c (2009). Disclosure of personal information; uses. Examples include use in connection with matters of motor vehicle and driver safety or auto theft; motor vehicle emissions; motor vehicle product alterations, recalls, or advisories; performance monitoring of motor vehicles; motor vehicle market research activities, including survey research; and the removal of nonowner records from the original records of motor vehicle manufacturers; in legal proceedings, or for use by the agency.
- **Vehicle Identification Numbers**
 - People v. Brooks, 274 N.W.2d 430 (Mich 1979) - There is no reasonable expectation of privacy with respect to a VIN.
 - MICH. COMP. LAWS. ANN. § 257.217 (2009) - must submit VIN to state in order to register a vehicle.
- **Consumer Credit**
 - MICH. COMP. LAWS. ANN. § 445.72 (2009) Identity Theft Protection Act. Unless the person or agency determines that the security breach has not or is not likely to cause substantial loss or injury to, or result in identity theft with respect to, 1 or more residents of this state, a person or agency that owns or licenses data that are included in a database that discovers a security breach, or receives notice of a security breach under subsection (2), shall provide a notice of the security breach to each resident of this state who meets 1 or more of the following:(a) That resident's unencrypted and unredacted personal information was accessed and acquired by an unauthorized person. (b) That resident's personal information was accessed and acquired in encrypted form by a person with unauthorized access to the encryption key.
- **Financial Records**
 - MICH. COMP. LAWS. ANN. § 488.12 (2009) - To protect the privacy of customers using funds transfer services, a person providing services of a funds transfer facility and a financial institution providing services by means of a funds transfer facility, except as provided by law or with the consent of the customer, shall not provide to an outside party information about a customer's deposit account or a customer's transaction obtained through use of a funds transfer facility.
- **Employee Privacy**
 - MICH. COMP. LAWS. ANN. § 423.508 (2009) An employer shall not gather or keep a record of an employee's associations, political activities, publications, or

communications of nonemployment activities, except if the information is submitted in writing by or authorized to be kept or gathered, in writing, by the employee to the employer. This prohibition on records shall not apply to the activities that occur on the employer's premises or during the employee's working hours with that employer that interfere with the performance of the employee's duties or duties of other employees.

- **Electronic Surveillance**

- MICH. COMP. LAWS. ANN. § 750.539 (2009) Divulging of contents of message, refusal or delay in transmission of message, etc. It is illegal for any person connected with a telegraph, telephone or messenger company to divulge contents of message.
- MICH. COMP. LAWS. ANN. § 750.539a (2009) Offenses relating to eavesdropping or surveillance; definitions
- MICH. COMP. LAWS. ANN. § 750.539b (2009) Trespassing for purpose of eavesdropping or surveillance
- MICH. COMP. LAWS. ANN. § 750.539c (2009) Eavesdropping upon private conversation. Prohibited without a warrant or consent of all parties to the communication.
- MICH. COMP. LAWS. ANN. § 750.539d (2009) Installation, placement, etc., of recording, transmitting, etc., device in private place; distribution, dissemination, or transmission of recording, photograph, or visual image obtained in violation of section; other offenses. The installation of devices for observing, photographing or eavesdropping in private places is prohibited, unless there is consent of the persons entitled to privacy.
- MICH. COMP. LAWS. ANN. § 750.539e (2009) Use or divulgence of information. Telecommunications employees may not intentionally divulge the contents of messages to any unauthorized person.
- MICH. COMP. LAWS. ANN. § 750.539f (2009) Unlawful manufacture, possession or transfer of eavesdropping devices
- MICH. COMP. LAWS. ANN. § 750.539g (2009) Eavesdropping or surveillance permitted under §§ 750.539a to 750.539f. Acceptable for peace officers of the state or the federal government, by correctional facilities, in the course of communication by a common carrier.
- MICH. COMP. LAWS. ANN. § 750.539h (2009) Civil remedies of parties subject to unlawful eavesdropping
- MICH. COMP. LAWS. ANN. § 750.539i (2009). Prima facie evidence of violation of § 750.539d In any criminal or civil action, proof of the installation in any private place of any device which may be used for the purposes of violating the provisions of this act shall be prima facie evidence of a violation of section 539d.

- **Computer Statutes**

- MICH. COMP. LAWS. ANN. §§ 752.791; 752.793; 752.794; 752.797 (2009) - Fraudulent Access to Computer or Computer networks. A person shall not intentionally access or cause access to be made to a computer program, computer, computer system, or computer network to devise or execute a scheme or artifice with the intent to defraud or to obtain money, property, or a service by a false or fraudulent pretense, representation, or promise.

- person shall not intentionally and without authorization or by exceeding valid authorization do any of the following: Access or cause access to be made to a computer program, computer, computer system, or computer network to acquire, alter, damage, delete, or destroy property or otherwise use the service of a computer program, computer, computer system, or computer network.
 - Insert or attach or knowingly create the opportunity for an unknowing and unwanted insertion or attachment of a set of instructions or a computer program into a computer program, computer, computer system, or computer network, that is intended to acquire, alter, damage, delete, disrupt, or destroy property or otherwise use the services of a computer program, computer, computer system, or computer network.
- **Common Law**
 - Beaumont v. Brown, 257 N.W.2d 522 (Mich. 1977) - accepts the four strands of invasion of privacy under common law.

MINNESOTA PRIVACY LAW

- **State Constitutional Privacy Rights**
 - none
- **Search and Seizure**
 - MINN. CONST. art. I, § 10 Unreasonable search and seizure prohibited. Identical to the Fourth Amendment.
 - State v. Krech, 403 N.W.2d 634 (Minn. 1987) - there is no reasonable expectation of privacy in garbage.
 - **Auto Exception**
 - State v. Ture, 632 N.W.2d 621 (Minn. 2001)
 - **Open Fields**
 - State v. Sorenson, 430 N.W.2d 231 (Minn. Ct. App. 1988).
 - **Plain View**
 - State v. Hoven, 269 N.W.2d 849 (Minn. 1978)
- **Statutory Privacy Rights**
 - MINN. STAT. ANN. § 504B.211 (2008) - Residential Tenant's Right to Privacy. Landlord may enter the premises rented by a residential tenant only for a reasonable business purpose and after making a good faith effort to give the residential tenant reasonable notice under the circumstances of the intent to enter. A residential tenant may not waive and the landlord may not require the residential tenant to waive the residential tenant's right to prior notice of entry under this section as a condition of entering into or maintaining the lease. Some exceptions for emergency purposes apply.
 - MINN. STAT. ANN. § 609.746 (2008) - Interference with privacy. Surreptitious intrusion; observation device with the intent to view places where persons have an expectation of privacy is a gross misdemeanor.
 - MINN. STAT. ANN. § 609.748; 609.749 (2008) Harassment and stalking crimes. (a) A person who harasses another by committing any of the following acts is guilty of a gross misdemeanor: (1) directly or indirectly manifests a purpose or intent to injure the person, property, or rights of another by the commission of an unlawful act; (2) stalks, follows, monitors, or pursues another, whether in person or through technological or other means; (3) returns to the property of another if the actor is without claim of right to the property or consent of one with authority to consent; (4) repeatedly makes telephone calls, or induces a victim to make telephone calls to the actor, whether or not conversation ensues; (5) makes or causes the telephone of another repeatedly or continuously to ring; (6) repeatedly mails or delivers or causes the delivery by any means, including electronically, of letters, telegrams, messages, packages, or other objects; or (7) knowingly makes false allegations against a peace officer concerning the officer's performance of official duties with intent to influence or tamper with the officer's performance of official duties.
- **Individually Identifiable Government Records**
 - MINN. STAT. ANN. § 13.82 (2008) defines law enforcement public and nonpublic data and requires the department to make the public data available for inspection. ex. Response or incident data is public, while personal details of domestic abuse data is not.

- MINN. STAT. ANN. § 260C.171 (2008) The records from proceedings or portions of proceedings involving a child in need of protection or services, permanency, or termination of parental rights are accessible to the public as authorized by the Minnesota Rules of Juvenile Protection Procedure.
 - None of the records relating to an appeal from a nonpublic juvenile court proceeding, except the written appellate opinion, shall be open to public inspection or their contents disclosed except by order of a court.
 - The records of juvenile probation officers are records of the court for the purposes of this subdivision. This subdivision applies to all proceedings under this chapter, including appeals from orders of the juvenile court. The court shall maintain the confidentiality of adoption files and records in accordance with the provisions of laws relating to adoptions. In juvenile court proceedings any report or social history furnished to the court shall be open to inspection by the attorneys of record and the guardian ad litem a reasonable time before it is used in connection with any proceeding before the court.
- **Public Records**
 - MINN. STAT. ANN. § 13.03 (2008) - All government data is public unless otherwise restricted as confidential. All government data collected, created, received, maintained or disseminated by a government entity shall be public unless classified by statute, or temporary classification pursuant to section 13.06, or federal law, as nonpublic or protected nonpublic, or with respect to data on individuals, as private or confidential.
 - MINN. STAT. ANN. § 13.06 (2008) the responsible authority of a government entity may apply to the commissioner for permission to classify data or types of data on individuals as private or confidential, or data not on individuals as nonpublic or protected nonpublic, for its own use and for the use of other similar government entities on a temporary basis until a proposed statute can be acted upon by the legislature. The application for temporary classification is public.
 - Demers v. Minneapolis, 468 N.W.2d 71 (Mich. 1991). Information identifying complainant on nonpending, noncurrent police department data is public. The section classified some data as private in order to protect the privacy of government employees, not the privacy of the individuals who filed the complaints. There was no evidence to indicate that disclosure of the identity of complainants to researchers or other interested persons deterred the filing of complaints.
- **Motor Vehicle Records**
 - MINN. STAT. ANN. § 168.346 (2008) - Data on an individual provided to register a vehicle shall be treated as provided by United States Code, title 18, section 2721, as in effect on May 23, 2005, and shall be disclosed as required or permitted by that section, but owner of vehicle may request that the owner's address or name be confidential. Some exceptions for the commissioner to disclose in connection with public safety or security of drivers, vehicles, pedestrians, or property.
 - MINN. STAT. ANN. § 168.09 (2008) All reports and supplemental information required under this section must be for the use of the commissioner of public safety and other appropriate state, federal, county, and municipal governmental

agencies for accident analysis purposes, except for some acts by the commissioner of public safety. Accident reports and data contained in the reports are not discoverable under any provision of law or rule of court. May be disclosed to those in the accident.

- MINN. STAT. ANN. § 171.12 (2008) Data on individuals provided to obtain a driver's license or Minnesota identification card shall be treated as provided by United States Code, title 18, section 2721, as in effect on May 23, 2005, and shall be disclosed as required or permitted by that section, but the driver may request that address information be confidential.
- **Vehicle Identification Numbers**
 - State v. Brown, No. C8-90-1740, 1991 Minn. App. LEXIS 111 (1991) - inspecting a VIN through the window is acceptable under the search and seizure rules of the state.
- **Consumer Credit**
 - MINN. STAT. ANN. § 13C.01 (2008) - A consumer is entitled to receive a copy of a consumer report once every 12 month period. A consumer reporting agency or any other business entity may not sell to, or exchange with, a third party, unless the third party holds an existing mortgage loan on the property, the existence of a credit inquiry arising from a consumer mortgage loan application when the sale or exchange is triggered by an inquiry made in response to an application for credit.
 - MINN. STAT. ANN. § 13C.016 (2008) - A consumer is entitled to put a security freeze on their credit report.
 - MINN. STAT. ANN. § 325E.61 (2008) - Any person or business that conducts business in this state, and that owns or licenses data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of this state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in paragraph (c), or with any measures necessary to determine the scope of the breach, identify the individuals affected, and restore the reasonable integrity of the data system
- **Financial Records**
 - MINN. STAT. ANN. § 47.69 (2008) - To protect the privacy of customers using electronic financial terminals, including any supporting equipment, structures or systems, information received by or processed through such terminals, supporting equipment, structures or systems shall be treated and used only in accordance with applicable law relating to the dissemination and disclosure of such information. The person establishing and maintaining an electronic financial terminal, including any supporting equipment, structures or systems, shall take such steps as are reasonably necessary to restrict disclosure of information to that necessary to complete the transaction and to safeguard any information received or obtained about a customer or that customer's account from misuse by any person staffing an electronic financial terminal, including any supporting equipment, structures or systems.

- MINN. STAT. ANN. § 47.61 (2008) "Electronic financial terminal" means an electronic information processing device that is established to do either or both of the following: (1) capture the data necessary to initiate financial transactions; or (2) through its attendant support system, store or initiate the transmission of the information necessary to consummate a financial transaction. (b) "Electronic financial terminal" does not include: (1) a telephone; (2) an electronic information processing device that is used internally by a financial institution to conduct the business activities of the institution; (3) or a personal computer.
- **Employee Privacy**
 - State v. Huseth, 375 N.W.2d 846 (Minn. Ct. App. 1985) - held that an employee, lacking a possessory interest in his or her place of employment, has no expectation of privacy in the employer's premises under the Fourth Amendment.
 - Minn. Stat. § 181.950 through 181.957 (2008) - results of an employee drug test may not be used in a criminal proceeding, but may be (1) used in an arbitration proceeding pursuant to a collective bargaining agreement, an administrative hearing under chapter 43A or other applicable state or local law, or a judicial proceeding, provided that information is relevant to the hearing or proceeding; (2) disclosed to any federal agency or other unit of the United States government as required under federal law, regulation, or order, or in accordance with compliance requirements of a federal government contract; and (3) disclosed to a substance abuse treatment facility for the purpose of evaluation or treatment of the employee.
- **Electronic Surveillance**
 - MINN. STAT. ANN. § 609.4975 (2008) Warning subject of surveillance or search. Electronic communication. Whoever, having knowledge that an investigative or law enforcement officer has been authorized or has applied for authorization under chapter 626A to intercept a wire, oral, or electronic communication, and with intent to obstruct, impede, or prevent interception, gives notice or attempts to give notice of the possible interception to a person, may be sentenced to imprisonment for not more than five years
 - MINN. STAT. ANN. § 626A.02 (2008) Interception And Disclosure Of Wire Or Oral Communications Prohibited. Intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, electronic, or oral communication. Or uses such interception, or discloses such information unlawfully is prohibited. Exceptions include law enforcement, telecommunications or FCC operators in the course of their employment; one party has consented to the communication, also acceptable to intercept radio frequencies available to the public.
 - MINN. STAT. ANN. § 626A.03 (2008) - It is illegal to manufacture, possess, assemble or sell the devices in this section to a non-authorized person.
 - MINN. STAT. ANN. § 626A.05 (2008) - Authorization for interception. The attorney general or county attorney may apply for an order to intercept if for the following offenses: a felony offense involving murder, manslaughter, assault in the first, second, and third degrees, aggravated robbery, kidnapping, criminal sexual conduct in the first, second, and third degrees, prostitution, bribery, perjury, escape from custody, theft, receiving stolen property, embezzlement,

burglary in the first, second, and third degrees, forgery, aggravated forgery, check forgery, or financial transaction card fraud.

- MINN. STAT. ANN. § 626A.06 (2008) - Procedure for interception
- MINN. STAT. ANN. § 626A.65 (2008) - Emergency interception. A law enforcement officer can use due diligence and judgment to determine that surveillance is necessary, but cannot wait for a warrant.
- MINN. STAT. ANN. § 626A.08 (2008) Preservation Of Material Obtained, Applications And Orders; Destruction. Every part of any wire, oral, or electronic communication intercepted pursuant to this chapter shall be completely recorded on tape or wire or other comparable device and shall be done in such manner as will protect the recording from editing or other alterations. Immediately upon the expiration of the period of the order, or extensions thereof, such recordings shall be made available to the judge issuing such order and sealed under the judge's directions. Custody of the recordings shall be wherever the judge orders. They shall not be destroyed except upon an order of the issuing or denying judge or a successor and in any event shall be kept for ten years.
- MINN. STAT. ANN. § 626A.10 (2008) - Notice of order. Within a reasonable time but not later than 90 days after the termination of the period of a warrant or extensions thereof, the issuing or denying judge shall cause to be served, on the persons named in the warrant and the application, and such other parties to intercepted communications as the judge may determine that is in the interest of justice.
- MINN. STAT. ANN. § 626A.35 (2008) - It is illegal to use a pen register, trap or trace device or mobile tracker without first obtaining a court do so, unless there is consent by the owner of the object to do so.
- **Computer Statutes**
 - MINN. STAT. ANN. § 609.87 through 609.8913 (2008) - Computer access, theft, damage and criminal use of encryption, and facilitating access to a computer security system.
- **Common Law**
 - Lake v. Wal-mart Stores, Inc., 582 N.W.2d 231 (Minn. 1998) (recognizing for the first time a tort for invasion of privacy). The right to privacy exists in the common law of Minnesota, including causes of action in tort for intrusion upon seclusion, appropriation, and publication of private facts. The tort of false light publicity is not included in the right to privacy.

MISSISSIPPI PRIVACY LAW

- **State Constitutional Privacy Rights**
 - none
- **Search and Seizure**
 - MISS. CONST. art. III, § 23 - privacy protection is extended through the limitation of unreasonable searches and seizures.
 - **Auto Exception**
 - Smith v. State, 724 So. 2d 280 (Miss. 1998)
 - **Open Fields**
 - Arnett v. State, 532 So.2d 1003 (Miss. 1988)
 - **Plain View**
 - Franklin v. State, 587 So.2d 905 (Miss. 1991)
- **Statutory Privacy Rights**
 - MISS. CODE ANN. § 97-3-107 (2008) - Any person who willfully, maliciously and repeatedly follows or harasses another person, or who makes a credible threat, with the intent to place that person in reasonable fear of death or great bodily injury is guilty of the crime of stalking.
 - MISS. CODE ANN. § 77-3-703 (2008) - Mississippi Telephone Solicitation Act. The use of the telephone to make all types of solicitations to consumers is pervasive. This article gives consumers a tool by which to object to telemarketing calls as these communications can amount to a nuisance, an invasion of privacy, and can create a health and safety risk for certain consumers who maintain their phone service primarily for emergency medical situations.
 - MISS. CODE ANN. § 45-27-1 (2008) - Mississippi Justice Information Center will control the collection, storage, dissemination and use of criminal offender record information. These improvements in the organization and control of criminal offender record keeping are imperative both to strengthen the administration of criminal justice and to assure appropriate protection of rights of individual privacy. The purposes of this chapter are (a) to control and coordinate criminal offender record keeping within this state; (b) to assure periodic reporting to the Governor and Legislature concerning such record keeping; and (c) to establish a more effective administrative structure for the collection, maintenance, retrieval and dissemination of criminal history record information described in this chapter, consistent with those principles of scope and security prescribed by this chapter, and to facilitate the practical use of criminal offender record information within the criminal justice system.
 - MISS. CODE ANN. § 97-45-19 (2008) - prohibition against identity theft. A person shall not obtain or attempt to obtain personal identity information of another person with the intent to unlawfully use that information for any of the following purposes without that person's authorization including to obtain credit or employment.
- **Individually Identifiable Government Records**
 - MISS. CODE ANN. § 41-9-23 (2008) Hospital records and information confidential
 - MISS. CODE ANN. § 41-75-19 (2008) Medical records confidential
 - MISS. CODE ANN. § 41-91-11 (2008) Patient records confidential
- **Public Records**

- MISS. CODE ANN. § 25-61-1 through -17 (2008) Public Records Act.
- MISS. CODE ANN. § 25-61-5 (2008). Public access to records; form and retention of denials
- MISS. CODE ANN. § 25-61-9 (2008). Trade secrets and confidential commercial or financial information is not public
- MISS. CODE ANN. § 25-61-10 (2008). Access to records stored, manipulated or retrieved by sensitive software; acquisition, modification,
- MISS. CODE ANN. § 25-61-11 (2008). Records exempted or privileged by law shall not be made public.
- MISS. CODE ANN. § 25-61-12 (2008). Exemption for private information of law enforcement, judicial and prosecutorial personnel; victim statements exceptions
- MISS. CODE ANN. § 25-53-53 (2008) Mississippi Department Of Information Technology Services (MDITS) Information Confidentiality: Information and data shall be considered public record information and data and receive normal handling and processing unless designated as "confidential information" by the agency and institution originating the data. Information and data designated as "confidential information" will receive special handling based on procedures agreed to by the executive director and the agency or institution head and shall be handled in accordance with the oath subscribed to by the confidentiality officer.
- MISS. CODE ANN. § 41-57-2 (2008) - Records in the possession of the Mississippi Department of Health, Bureau of Vital Statistics, which would be of no legitimate and tangible interest to a person making a request for access to such records, shall be exempt from the provisions of the Mississippi Public Records Act of 1983; provided, however, nothing in this section shall be construed to prohibit any person with a legitimate and tangible interest in such records from having access thereto.
- **Motor Vehicle Records**
 - MISS. CODE ANN. § 63-3-417 (2008) - All required accident reports and supplemental reports shall be without prejudice to the individual so reporting and, except as otherwise provided in this section, shall be for the confidential use of the department; however, the department may, upon written request of any person involved in an accident, the spouse or next of kin of any such person, or any person against whom a claim is made as a result of the accident or upon written request of the representative of his estate, disclose to such requester or his legal counsel or a representative of his insurer any information contained in such report except the parties' version of the accident as set out in the written report filed by such parties, or may disclose the identity of a person involved in an accident when such identity is not otherwise known or when such person denies his presence at such accident.
 - MISS. CODE ANN. § 63-13-21 (2008) Members of the Mississippi Highway Safety Patrol may at any time, upon reasonable cause to believe that a vehicle is unsafe or not equipped as required by law, or that its equipment is not in proper adjustment or repair, require the driver of such vehicle to stop and submit such vehicle to an inspection and such test with reference thereto as may be reasonably appropriate. No person driving a vehicle shall refuse to submit such vehicle to an

inspection and test when required to do so by a member of the Mississippi Highway Safety Patrol.

- Such authority, however, shall be limited to the inspection of said vehicle for mechanical defects and shall not authorize the search of the vehicle or the occupants thereof for any other purpose without due process of law.

- **Vehicle Identification Numbers**

- MISS. CODE ANN. § 63-13-7 (2008) - periodic inspection of motor vehicles requires checking VIN for accuracy.

- **Consumer Credit**

- MISS. CODE ANN. § 75-24-201 through -211 (2008) - permits a consumer to put a security freeze on his report, but allows the reporting agency to notify any entity seeking information of the freeze.

- **Financial Records**

- MISS. CODE ANN. § 13-1-245 (2008) Bank expenses related to disclosure of customer's financial records in connection with a judicial proceeding.
- MISS. CODE ANN. § 79-23-1 (2008). Commercial and financial information exempt from provisions of public access; application of Trade Secrets Act.

- **Employee Privacy**

- MISS. CODE ANN. § 71-3-66 (2008) - workers compensation records are confidential.
- MISS. CODE ANN. § 71-3-121 (2008) - Drug Testing and worker's compensation. Under such policy, if the employer has probable cause to suspect that an employee's injury was occasioned primarily by the intoxication of the employee or by the illegal use of any controlled substances that affected the employee to the extent that the employee's normal faculties were impaired, the employer may require the employee to submit to a test for the presence of any controlled substances or alcohol in his system. The results of the employer-administered tests shall be considered admissible evidence solely on the issue of causation in the determination of intoxication of an employee at the time of injury for workers' compensation purposes under Section 71-3-7.
- MISS. CODE ANN. § 71-7-1 through -33 (2008) - Drug Testing of Employees. All information, interviews, reports, statements, memoranda and test results, written or otherwise, received by the employer through its drug and alcohol testing program are confidential communications and may not be used or received in evidence, obtained in discovery, or disclosed in any public or private proceedings, except in accordance with this chapter. The confidentiality provisions provided for in this section shall not apply to other parts of an employee's or job applicant's personnel or medical files.

- **Electronic Surveillance**

- MISS. CODE ANN. § 41-29-501 (2008) Definitions. Interception of wire or oral communications. Doesn't specifically include electronic.
- MISS. CODE ANN. § 41-29-503 (2008) Admission of evidence. If obtained by illegal surveillance, not admissible.
- MISS. CODE ANN. § 41-29-505 (2008) Authorization by judge. judge of competent jurisdiction in the circuit court district of the location where the interception of wire, oral or other communications is sought, or a circuit court district contiguous

to such circuit court district, may issue an order authorizing interception of wire, oral or other communications only if the prosecutor applying for the order shows probable cause to believe that the interception will provide evidence of the commission of a felony under the Uniform Controlled Substances Law.

- MISS. CODE ANN. § 41-29-507 (2008) Authorized possession or use of devices
- MISS. CODE ANN. § 41-29-509 (2008) Procedures before applying to court
- MISS. CODE ANN. § 41-29-511 (2008) Disclosure and use of information
- MISS. CODE ANN. § 41-29-513 (2008) Application for authority to intercept
- MISS. CODE ANN. § 41-29-515 (2008) Orders authorized; disqualification of judge. Upon receipt of an application, the judge may enter an ex parte order, as requested or as modified, authorizing interception of wire, oral or other communications if the judge determines from the evidence submitted by the applicant that there is probable cause and the surveillance will be fruitful.
- MISS. CODE ANN. § 41-29-517 (2008) Recordings; sealing, custody and preservation
- MISS. CODE ANN. § 41-29-519 (2008) Handling of applications and orders
- MISS. CODE ANN. § 41-29-523 (2008) - Notice to persons named in order or application; inspection of intercepted communications; postponement of notice (1) Within a reasonable time but not later than ninety (90) days after the date an application for an order is denied or after the date an order or the last extension, if any, expires, the judge who granted or denied the application shall cause to be served upon the persons named in the order or the application and any other parties to intercepted communications deemed appropriate by the issuing judge, if any, an inventory.
- **Computer Statutes**
 - MISS. CODE ANN. § 97-45-1 through -9 (2008) - computer crimes
 - MISS. CODE ANN. § 97-45-3 (2008). Computer fraud; penalties
 - MISS. CODE ANN. § 97-45-5 (2008). Offense against computer users; penalties
 - MISS. CODE ANN. § 97-45-7 (2008). Offense against computer equipment; penalties
 - MISS. CODE ANN. § 97-45-9 (2008). Offense against intellectual property; penalties. Destruction, copying, taking of computers and computer equipment.
- **Common Law**
 - Deaton v. Delta Democrat Publishing Co., 326 So. 2d 471 (Miss. 1976)
Mississippi has by implication judicially recognized the common law right to privacy. Although the law of privacy has developed along divergent lines and amid a welter of confusing judicial pronouncements, four distinct theories of the cause of action are generally recognized: (1) The intentional intrusion upon the solitude or seclusion of another; (2) the appropriation of another's identity for an unpermitted use; (3) the public disclosure of private facts; and (4) holding another to the public eye in a false light.

MISSOURI PRIVACY LAW

- **State Constitutional Privacy Rights**
 - none
- **Search and Seizure**
 - MO. CONST. art. I, § 15 - protects against unreasonable search and seizure.
 - **Auto Exception**
 - State v. Lane, 937 S.W.2d 721 (Mo. 1997).
 - **Open Fields**
 - State v. Schweitzer, 879 S.W.2d 594 (Mo. Ct. App. 1994).
 - **Plain View**
 - State v. Peters, 695 S.W.2d 140 (Mo. Ct. App. 1985).
- **Statutory Privacy Rights**
 - MO. REV. STAT. § 565.225 (2009) - A person commits the crime of stalking if he or she purposely, through his or her course of conduct, harasses or follows with the intent of harassing another person; aggravated stalking requires making a credible threat, harasses a minor, or is violating parole, or other protective order.
 - MO. REV. STAT. § 565.250 through .257 (2009) - Invasion of Privacy. Knowingly photographs or films another person, without the person's knowledge and consent, while the person being photographed or filmed is in a state of full or partial nudity and is in a place where one would have a reasonable expectation of privacy, and the person subsequently distributes the photograph or film to another or transmits the image contained in the photograph or film in a manner that allows access to that image via a computer.
- **Individually Identifiable Records**
 - MO. REV. STAT. § 565.250 (2009) Governmental Bodies And Records. Arrest Records. All incident reports and arrest reports shall be open records, but if any portion of a record or document of a law enforcement officer or agency, other than an arrest report, which would otherwise be open, contains information that is reasonably likely to pose a clear and present danger to the safety of any victim, witness, undercover officer, or other person; or jeopardize a criminal investigation, including records which would disclose the identity of a source wishing to remain confidential or a suspect not in custody; or which would disclose techniques, procedures or guidelines for law enforcement investigations or prosecutions, that portion of the record shall be closed and shall be redacted from any record.
 - MO. REV. STAT. § 407.1355 (2009) - person or entity must redact social security numbers from public documents, cannot request a person to send SSN over the internet unless the connection is secure. This section does not prevent the collection, use, or release of a Social Security number as required by state or federal law or the use of a Social Security number for internal verification or administrative purposes.
- **Public Records**
 - MO. REV. STAT. § 610.011 (2009) - It is the public policy of this state that meetings, records, votes, actions, and deliberations of public governmental bodies be open to the public unless otherwise provided by law. This shall be liberally construed and their exceptions strictly construed to promote this public policy.

- MO. REV. STAT. § 610.024 (2009). Public records containing exempt and nonexempt materials, nonexempt to be made available--deleted exempt materials to be explained, exceptions:
 - If a public record contains material which is not exempt from disclosure as well as material which is exempt from disclosure, the public governmental body shall separate the exempt and nonexempt material and make the nonexempt material available for examination and copying.
 - When designing a public record, a public governmental body shall, to the extent practicable, facilitate a separation of exempt from nonexempt information. If the separation is readily apparent to a person requesting to inspect or receive copies of the form, the public governmental body shall generally describe the material exempted unless that description would reveal the contents of the exempt information and thus defeat the purpose of the exemption.
- **Motor Vehicle Records**
 - MO. REV. STAT. § 301.116 (2009). Records required to be kept by service agents, time period--records open for inspection. Motor vehicle registration and licensing shall be open to inspection by any authorized representative of the department, member of the Missouri highway patrol or any authorized peace officer during reasonable business hours.
 - MO. REV. STAT. § 301.225 (2009). Licensees to maintain records--inspection of premises. Every person licensed or required to be licensed shall maintain for three years on vehicles not more than seven years old a record of: (1) Every vehicle or used transmission, rear end, cowl, frame, body, front end assembly or engine of or for a vehicle received or acquired by him, its description and identifying number, if any, the date of its receipt or acquisition, and the name and address of the person from whom received or acquired (2) every vehicle wrecked by him
 - Every such record shall be retained by the person licensed or required to be licensed at his principal place of business and shall be open to inspection by any representative of the department, member or authorized or designated employee of the Missouri highway patrol, or any police officer during reasonable business hours.
 - MO. REV. STAT. § 300.025 (2009). Records of traffic violations are kept for prior five years and are available for inspection by the public.
 - MO. REV. STAT. § 300.040 (2009). Traffic accident reports. The traffic division shall maintain a suitable system of filing traffic accident reports. Accident reports or cards referring to them shall be filed alphabetically by location. Such reports shall be available for the use and information of the city traffic engineer.
- **Vehicle Identification Numbers**
 - MO. REV. STAT. § 301.190 (2009) - Every application of ownership shall contain a VIN. The certificate shall be manufactured to prevent forgery.
- **Consumer Credit**
 - MO. REV. STAT. § 407.1382 (2009) - consumers are allowed to place a security freeze on their accounts and necessitate notification if any entity tries to access their credit report.
- **Financial Records**

- MO. REV. STAT. § 408.677 (2009) - Right to Financial Privacy Act. No government authority may have access to or obtain copies of the information contained in the financial records of any customer unless the financial records are reasonably described and the consumer consents or they are disclosed in response to a subpoena or specific written request.
- MO. REV. STAT. § 408.690 (2009). Lists nonprohibited disclosure activities including exchange of records between financial institutions, if the records have no identifying information.
- MO. REV. STAT. § 198.032 (2009). Nothing contained in sections 198.003 to 198.186 shall permit the public disclosure by the department [public health and welfare] of confidential medical, social, personal or financial records of any resident in any facility, except when disclosed in a manner which does not identify any resident, or when ordered to do so by a court of competent jurisdiction.
- MO. REV. STAT. § 610.225 (2009). Tax credit records and documents deemed closed records.
- **Employee Privacy**
 - MO. REV. STAT. § 36.420 (2009). Records open for public inspection. The records of the personnel division of the state government, except such records as the regulations may require to be held confidential for reasons of public policy, shall be public records and shall be open to public inspection, subject to regulations as to the time and manner of inspection which may be prescribed by the board.
 - MO. REV. STAT. § 105.959 (2009). Public Officers and Officials. All investigations by the executive director shall be limited to the information contained in the reports or statements. The commission shall notify the complainant or the person under investigation, by registered mail, within five days of the decision to conduct such investigation. Revealing any such confidential investigation information shall be cause for removal or dismissal of the executive director or a commission member or employee.
 - MO. REV. STAT. § 288.045 (2009) - random drug testing of employees is permissible as long as the employee is given notice in their employee handbook. There is no information whether the result is confidential or may be entered into evidence in a criminal proceeding.
- **Electronic Surveillance**
 - MO. REV. STAT. § 542.400 (2009) Definitions. Not specifically included is electronic communication, but does include electronic devices as prohibited.
 - MO. REV. STAT. 542.402 (2009) Penalty for illegal wiretapping, permitted activities. Knowingly intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire communication, or uses or discloses such communication. Exceptions include law enforcement, common carriers in the course of employment, where one party has given consent.
 - MO. REV. STAT. 542.404 (2009) Application for an order--authorization by attorney general--approval by judge, probable cause required. An attorney general may apply to a judge in the jurisdiction if there is probable cause to believe that the interception may provide evidence of a felony which involves the manufacture or distribution of a controlled substance, as the term is defined by section

195.016, RSMo, or the felony of murder, arson, or kidnapping, or a terrorist threat as defined in section 574.115, RSMo, or any conspiracy to commit any of the foregoing.

- MO. REV. STAT. 542.406 (2009) Disclosure of contents--privileged communications
- MO. REV. STAT. 542.408 (2009) Application, contents--ex parte order issued, when, contents, extensions granted, when--reports, court may require, when--pen registers, who may request--communication common carriers may provide aid, immunity from suit, compensation.
- MO. REV. STAT. 542.410 (2009) Recording of contents, required, how, custody of, duplication, destruction of--applications and orders sealed by court, disclosure, when, destruction of--penalty--notice to persons named in order, when, right to inspect and copy contents
- MO. REV. STAT. 542.412 (2009) Contents may be used as evidence, when--disclosure of additional evidence to defendant
- MO. REV. STAT. 542.414 (2009) Suppression of contents, grounds--right of state to appeal suppression motion
- MO. REV. STAT. 542.416 (2009) Reports to state courts administrator required, when, contents, who must report--state courts administrator to report to general assembly, when--rules and regulations
- MO. REV. STAT. 542.418 (2009) Use of contents of wiretap in civil action, limitations on-- illegal wiretap, cause of action, damages, attorney fees and costs--good faith reliance on court order a prima facie defense
- **Computer Statutes**
 - MO. REV. STAT. §§ 569.095; 569.097 (2009). Tampering with computer data includes modifying, destroying data or programs on a computer or computer network. Tampering with computer equipment involves physically damaging the hardware.
 - MO. REV. STAT. § 569.099 (2009) - A person commits the crime of tampering with computer users if he knowingly and without authorization or without reasonable grounds to believe that he has such authorization: (1) Accesses or causes to be accessed any computer, computer system, or computer network; or (2) Denies or causes the denial of computer system services to an authorized user of such computer system services, which, in whole or in part, is owned by, under contract to, or operated for, or on behalf of, or in conjunction with another.
- **Common Law**
 - Sullivan v. Pulitzer Broadcasting Co., 709 S.W.2d 475 (Mo. 1986) - Recognizes appropriation, intrusion and public disclosure.
 - State v. BP Prods, 163 S.W.3d 922 (Mo. 2005) - suggests that false light is recognized in Missouri, but not totally clear and the court did not decide the case on this issue. "In that case, the plaintiff attempted to bring a claim for false light invasion of privacy more than four years after his claim accrued. Although no false light invasion of privacy claim was recognized in Missouri at that time, the plaintiff urged the Court to allow him to evade the two-year statute of limitations for defamation by denominating his claim as one for "false light invasion of privacy."

MONTANA PRIVACY LAW

- **State Constitutional Privacy Rights**
 - **Express**
 - MONT. CONST. art. II, § 10 (2007) - Right of privacy. The right of individual privacy is essential to the well-being of a free society and shall not be infringed without the showing of a compelling state interest.
 - Great Falls Tribune Co. v. Cascade County Sheriff, 775 P.2d 1267 (Mont. 1989) Supreme Court of Montana has used a two-part test in determining whether a person has a constitutionally-protected privacy interest. First, a court determines whether the person has a subjective or actual expectation of privacy. Next, it evaluates whether society is willing to recognize that expectation as reasonable.
 - **Implied**
 - State v. Sierra, 692 P.2d 1273 (Mont. 1985) - Montana's privacy right is more extensive than the Fourth Amendment; if there is a less intrusive method, it must be used.
- **Search and Seizure**
 - MONT. CONST. art. II, § 11 - Prohibits unreasonable search and seizure.
 - State v. Emerson, 546 p.2d 509 (Mont. 1976) - if there is no intent to find, then there can be no search.
 - **Auto Exception**
 - State v. Pierce, 116 P.3d 817 (Mont. 2005) "we have since rejected the "automobile exception" and demands that "a warrantless search of an automobile requires the existence of probable cause as well as a generally applicable exception to the warrant requirement such as a plain view search, a search incident to arrest, or exigent circumstances."
 - **Open Fields**
 - State v. Bullock, 901 P.2d 61 (Mont. 1995). In Montana a person may have an expectation of privacy in an area of land that is beyond the curtilage which the society of this state is willing to recognize as reasonable, and that where that expectation is evidenced by fencing, "No Trespassing," or similar signs, or by some other means which indicates unmistakably that entry is not permitted, entry by law enforcement officers requires permission or a warrant. This requirement does not apply to observations of private land from public property.
 - **Plain View**
 - State v. O'Neill, 679 P.2d 760 (Mont. 1984).
- **Statutory Privacy Rights**
 - MONT. CODE ANN. § 45-5-220 (2007) - person commits the offense of stalking if the person purposely or knowingly causes another person substantial emotional distress or reasonable apprehension of bodily injury or death by repeatedly: (a) following the stalked person; or (b) harassing, threatening, or intimidating the stalked person, in person or by mail, electronic communication.
 - MONT. CODE ANN. § 33-19-410 (2007) An individual or a business that, by means of a website, an electronic mail message, or otherwise through the internet, solicits, requests, or takes an action to induce another individual or business to

provide personal information by purporting to be a licensee or insurance-support organization that conducts business in Montana without the authority or approval of the represented licensee or insurance-support organization that conducts business in Montana, is guilty of a theft of identity, as provided in 45-6-332(1). This crime of fraudulent electronic misrepresentation is commonly known as "phishing".

- **Individually Identifiable Government Records**

- MONT. CODE ANN. § 33-19-301; -306 (2007) Insurance information. May be disclosed to prevent criminal acts in connection with insurance transaction. Person also has access to insurance information recorded about himself.
- MONT. CODE ANN. § 44-5-213 (2007) - Collection methods of criminal information must be accurate and the person may inspect his own records.
- MONT. CODE ANN. § 44-5-302; -303 (2007) Confidential criminal history information must be identified as such and its release limited to those authorized.
- MONT. CODE ANN. § 44-5-304 (2007) If an agency wants to use criminal information for statistical purposes, it must first sign an agreement with the criminal justice agency.
- MONT. CODE ANN. § 44-5-504 (2007) Standards and procedures must be adopted for dealing with criminal history information and must include safeguards for individual privacy rights.

- **Public Records**

- MONT. CODE ANN. § 2-6-102 (2007) All public writings except those protected by statute are public and may be inspected.
- MONT. CODE ANN. § 7-1-4144 (2007) Personal records, medical records, and other records which relate to matters in which the right to individual privacy exceeds the merits of public disclosure shall not be available to the public unless the person they concern requests they be made public.
- MONT. CODE ANN. § 31-3-126 (2007) A consumer reporting agency which furnishes a consumer report for employment purposes and which for that purpose compiles and reports items of information on consumers which are matters of public record and are likely to have an adverse effect upon a consumer's ability to obtain employment shall: at the time such public record information is reported to the user of such consumer report, notify the consumer of the fact that public record information is being reported by the consumer reporting agency, together with the name and address of the person to whom such information is being reported.
- MONT. CODE ANN. § 39-71-224 (2007) Worker's compensation board records are confidential.
- MONT. CODE ANN. § 22-1-1103 (2007) Library records may not be disclosed except in response to a written request of the person identified in the record, on court order, or to collect overdue fines.
- MONT. CODE ANN. § 53-3-111 (2007) Information obtained by the welfare department is confidential.
- Denny Driscoll Boys Home v. State, 737 P.2d 1150 (Mont. 1987) No libel action can exist if letter is of public record written in official capacity.

- Bozeman Daily Chronicle v. City of Bozeman Police Dept., 859 P.2d 435 (Mont. 1993) - In general the public's right to know of any misbehavior by police outweighs the right to privacy. Investigative reports have to be released as well.
- **Motor Vehicle Records**
 - MONT. CODE ANN. § 61-3-101 (2007) Motor vehicle records maintained by the department must be open to inspection during reasonable business hours, and the department shall furnish any information from the records, except personal information and highly restricted personal information [Highly restricted personal information means an individual's photograph or image, social security number, or medical or disability information].
 - MONT. CODE ANN. § 61-7-114 (2007) Accident reports are confidential, but may be revealed to identify a party or due to a court order.
- **Vehicle Identification Numbers**
 - State v. Amaya, 739 P.2d 955 (Mont. 1987) VIN numbers may be examined without a warrant in an abandoned car.
 - MONT. CODE ANN. § 61-3-604 (2007) Penalty for altering identification number. Any person who willfully removes or falsifies an identification number of a motor vehicle, trailer, semitrailer, pole trailer, or motor vehicle engine is punishable by a fine of not more than \$ 5,000 or imprisonment in the state prison for a period of not more than 10 years, or both.
- **Consumer Credit**
 - MONT. CODE ANN. § 31-3-131 (2007) Consumer has to be advised if credit is denied based on a report by the reporting agency.
 - MONT. CODE ANN. § 30-14-1727 (2007) - Impediment to Identity Theft. A consumer may elect to place a security freeze on the consumer's own credit report.
 - MONT. CODE ANN. § 30-14-1704 (2007) Computer security breach. Any person or business that conducts business in Montana and that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the data system following discovery or notification of the breach to any resident of Montana whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person. The disclosure must be made without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection (3), or consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.
 - MONT. CODE ANN. § 31-3-113 (2007) Investigative reports can only be prepared if a consumer is informed or if they will be used for employment purposes.
 - MONT. CODE ANN. § 31-3-111 (2007) - A consumer reporting agency may furnish a consumer report under the following circumstances and no other: (1) in response to the order of a court having jurisdiction to issue such an order; (2) in accordance with the written instructions of the consumer to whom it relates; (3) to a person who intends to use the information in a legitimate credit transaction.
- **Financial Records**
 - MONT. CODE ANN. § 32-6-105 (2007) No information relating to any transaction by electronic funds transfer, or application therefore, between a financial

institution and its customer or prospective customer may be disclosed by the financial institution to any person or government entity without: (a) the consent of the customer; or (b) a subpoena issued by a court of record.

- MONT. CODE ANN. § 32-1-339 (2007) Right of examination by stockholder. A stockholder of a bank incorporated under the laws of this state who is not a director may not inspect the books and records of the bank showing its transactions with a customer. A stockholder may inspect the books and records of the bank as provided otherwise.
- **Employee Privacy**
 - MONT. CODE ANN. § 39-2-205 through -213 (2007) Drug Testing. (1) Except as provided in subsection (2) and except for information that is required by law to be reported to a state or federal licensing authority, all information, interviews, reports, statements, memoranda, or test results received by an employer through a qualified testing program are confidential communications and may not be used or received in evidence, obtained in discovery, or disclosed in any public or private proceeding. (2) Material that is confidential under subsection (1) may be used in a proceeding related to: (a) legal action arising out of an employer's implementation of 39-2-205 through 39-2-211; or (b) inquiries relating to a workplace accident involving death, physical injury, or property damage in excess of \$ 1,500 when there is reason to believe that the tested employee may have caused or contributed to the accident.
 - MONT. CODE ANN. § 39-71-224 (2007) Worker's compensation board records are confidential.
 - MONT. CODE ANN. § 39-2-304 (2007) - A person, firm, corporation, or other business entity or its representative may not require a person to take a polygraph test or any form of a mechanical lie detector test as a condition for employment or continuation of employment.
- **Electronic Surveillance**
 - MONT. CODE ANN. § 45-8-213 (2007). Privacy in communications. Unlawful to knowingly or purposely communicate with a person with the intent to harass, purposely intercepts communications, records communications without the party's knowledge (excludes taping public figures at meetings and other lawful recordings)
 - "Electronic communication" means any transfer between persons of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photo-optical system.
 - MONT. CODE ANN. § 46-4-401 Definitions (2007). Recording Numbers Of Devices Used To Communicate
 - MONT. CODE ANN. § 46-4-402 (2007) Limitations on use of pen register or trap and trace device
 - MONT. CODE ANN. § 46-4-403 (2007) Order for pen register or trap and trace device-- installation--disclosures
 - MONT. CODE ANN. § 46-4-404 (2007) Immunity from suit. Except for gross negligence or willful or wanton misconduct, there is no cause of action against a service provider, landlord, or custodian or their officers, employees, or agents or

other nongovernmental person for injury or damage caused in furnishing facilities or assistance under the order or against a service provider or its officers, employees, or agents for providing the law enforcement agency with information received from the operation of the pen register or trap and trace device. The immunity provided by this section does not extend to any governmental agency, law enforcement agent, or prosecutor.

- **Computer Statutes**

- MONT. CODE ANN. § 45-6-311 (2007) Unlawful use of a computer.(1) A person commits the offense of unlawful use of a computer if the person knowingly or purposely: (a) obtains the use of any computer, computer system, or computer network without consent of the owner; (b) alters or destroys or causes another to alter or destroy a computer program or computer software without consent of the owner; or (c) obtains the use of or alters or destroys a computer, computer system, computer network, or any part thereof as part of a deception for the purpose of obtaining money, property, or computer services from the owner of the computer, computer system, computer network, or part thereof or from any other person.

- **Common Law**

- **False Light**
 - Board of Dentistry v. Kandarian, 886 P.2d 954 (Mont. 1994)
- Does not specifically accept the other three strands of the common law invasion of privacy

NEBRASKA PRIVACY LAW

- **State Constitutional Privacy Rights**
 - none
- **Search and Seizure**
 - NEB. CONST. art. 1, § 7 protects against unreasonable search and seizure.
 - State v. Trahan, 428 N.W.2d 619 (Neb. 1988) - No reasonable expectation of privacy in garbage which is accessible to the public and placed for collection.
- **Auto Exception**
 - State v. Konfrst, 556 N.W.2d 250 (Neb. 1996).
- **Open Fields**
 - State v. Trahan, 428 N.W.2d 619 (Neb. 1988).
- **Plain View**
 - State v. DeGroat, 508 N.W.2d 861 (Neb. 1993).
- **Statutory Privacy Rights**
 - NEB. REV. STAT. § 28-311.03 (2009) Any person who willfully harasses another person or a family or household member of such person with the intent to injure, terrify, threaten, or intimidate commits the offense of stalking. Certain exceptions for labor picketing.
 - NEB. REV. STAT. § 28-1310 (2009) Intimidation by telephone call; penalty; prima facie evidence. Unlawful to harass by phone and disturb the peace and right of privacy of any person where the calls are received.
 - NEB. REV. STAT. § 20-201 (2009). Right of privacy; legislative intent. Explicitly provides a right of privacy.
 - NEB. REV. STAT. § 20-202 (2009). Invasion of privacy; exploitation of a person for advertising or commercial purposes; situations; not applicable. Any person or corporation that exploits a natural person, name, likeness, or personality for advertising or commercial purposes shall be liable for the invasion of privacy. Exceptions apply for news reports, consent, public person (as long as not identified).
 - NEB. REV. STAT. § 20-203 (2009). Invasion of privacy; trespass or intrude upon a person's solitude. Any person, firm, or corporation that trespasses or intrudes upon any natural person in his or her place of solitude or seclusion, if the intrusion would be highly offensive to a reasonable person, shall be liable for invasion of privacy.
 - NEB. REV. STAT. § 20-204 (2009). Invasion of privacy; place person before public in false light. The false light in which the other was placed would be highly offensive to a reasonable person; and (2) the actor had knowledge of or acted in reckless disregard as to the falsity of the publicized matter and the false light in which the other would be placed.
 - NEB. REV. STAT. § 20-205 (2009). Publication or intrusion; not actionable. An otherwise actionable publication is lawful if the person consents to the depiction.
 - NEB. REV. STAT. § 20-206 (2009). Right of privacy; defenses and privileges
 - NEB. REV. STAT. § 20-207 (2009). Invasion of privacy; action; nonassignable
 - NEB. REV. STAT. § 20-208 (2009). Invasion of privacy; death of subject; effect
 - NEB. REV. STAT. § 20-209 (2009). Libel, slander, invasion of privacy; one cause of action

- NEB. REV. STAT. § 20-210 (2009). Judgment; bar against other actions
- NEB. REV. STAT. § 20-211 (2009). Invasion of privacy; statute of limitations
- NEB. REV. STAT. § 25-840.01 (2009). In an action for damages for the publication of a libel or for invasion of privacy as provided by section 20-204 by any medium, the plaintiff shall recover no more than special damages unless correction was requested as herein provided and was not published.
- **Public Records**
 - NEB. REV. STAT. § 84-712.01 (2009) Except when any other statute expressly provides that particular information or records shall not be made public, public records shall include all records and documents, regardless of physical form, of or belonging to this state, any county, city, village, political subdivision, or tax-supported district in this state, or any agency, branch, department, board, bureau, commission, council, subunit, or committee of any of the foregoing. Data which is a public record in its original form shall remain a public record when maintained in computer files.
 - NEB. REV. STAT. § 84-712.05 (2009). Records which may be withheld from the public; enumerated. Examples include personal information, medical records, Social Security numbers; credit card, charge card, or debit card numbers and expiration dates; and financial account numbers supplied to state and local governments by citizens, or trade secrets.
 - NEB. REV. STAT. § 20-146 (2009) No person engaged in procuring, gathering, writing, editing, or disseminating news or other information to the public shall be required to disclose in any federal or state proceeding, either published or unpublished.
 - NEB. REV. STAT. § 29-3506 (2009) Criminal history record information shall mean information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of issuance of arrest warrants, arrests, detentions, indictments, charges by information, and other formal criminal charges, and any disposition arising from such arrests, charges, sentencing, correctional supervision, and release. Criminal history record information shall not include intelligence or investigative information.
 - NEB. REV. STAT. § 29-3520 (2009). Criminal history record information; public record; criminal justice agencies; regulations; adopt. Complete criminal history record information maintained by a criminal justice agency shall be a public record open to inspection and copying by any person during normal business hours and at such other times as may be established by the agency maintaining the record. Criminal justice agencies may adopt such regulations with regard to inspection and copying of records as are reasonably necessary for the physical protection of the records and the prevention of unnecessary interference with the discharge of the duties of the agency.
- **Motor Vehicle Records**
 - NEB. REV. STAT. § 60-2903 (2009) The purpose of the Uniform Motor Vehicle Records Disclosure Act is to enact choices permitted under the federal legislation in the interest of ensuring that motor vehicle record information which is a matter of public record shall remain a matter of public record in this state to the maximum extent permitted under the federal law. (2) The Legislature intends that

to the extent permitted by the federal law, Nebraska law pertaining to motor vehicle records should continue to recognize such records as public records to the extent it has done so prior to the effective date of the federal legislation, and the terms of the Uniform Motor Vehicle Records Disclosure Act should be construed liberally to effect that purpose.

- NEB. REV. STAT. § 60-699 (2009) Accident Reports. All reports made by peace officers, made to or filed with peace officers in their respective offices or departments, or filed with or made by or to any other law enforcement agency of the state shall be open to public inspection, but accident reports filed by the operator or owner of a motor vehicle pursuant to this section shall not be open to public inspection.
- **Vehicle Identification Numbers**
 - NEB. REV. STAT. § 81-2005 (2009). State patrol; powers and duties enumerated. When in uniform, to require the driver of a vehicle to stop and exhibit his or her operator's license and registration card issued for the vehicle and submit to an inspection of such vehicle and the license plates and registration card thereon and to require the drivers of motor vehicles to present such vehicles within five days for correction of any defects revealed by such motor vehicle inspection as may lead the inspecting officer to reasonably believe that such motor vehicle is being operated in violation of the statutes of Nebraska or the rules and regulations of the Director of Motor Vehicles.
 - State v. Childs, 495 N.W.2d 475 (Neb 1993) - For investigative stops to be constitutional, they cannot be based only on a police officer's desire to verify compliance with motor vehicle registration statutes.
- **Consumer Credit**
 - NEB. REV. STAT. 20-149 (2009) - consumer reporting agencies must furnish upon request by the subject of any report, copies of the report or the information compiled by the agency concerning the consumer.
 - NEB. REV. STAT. § 8-2604 (2009) Consumers may place a security freeze on their credit report. If a security freeze is in place with respect to a consumer's file, the consumer reporting agency shall not release a credit report or any other information derived from the file to a third party without the prior express authorization of the consumer. This section does not prevent a consumer reporting agency from advising a third party that a security freeze is in effect with respect to a consumer's file.
 - NEB. REV. STAT. § 87-801 through -807 (2009) Financial Data Protection and Consumer Notification of Data Security Breach Act of 2006
 - Breach of the security of the system means the unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by an individual or a commercial entity. Good faith acquisition of personal information by an employee or agent of an individual or a commercial entity for the purposes of the individual or the commercial entity is not a breach of the security of the system if the personal information is not used or subject to further unauthorized disclosure. Acquisition of personal information pursuant to a search warrant, subpoena, or other court order or

pursuant to a subpoena or order of a state agency is not a breach of the security of the system.

- An individual or a commercial entity that conducts business in Nebraska and that owns or licenses computerized data that includes personal information about a resident of Nebraska shall, when it becomes aware of a breach of the security of the system, conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be used for an unauthorized purpose. If the investigation determines that the use of information about a Nebraska resident for an unauthorized purpose has occurred or is reasonably likely to occur, the individual or commercial entity shall give notice to the affected Nebraska resident. Notice shall be made as soon as possible and without unreasonable delay, consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system.

- **Financial Records**

- NEB. REV. STAT. § 8-112 (2009) Neither the director nor anyone connected with the department shall in any instance disclose the name of any depositor or debtor of any financial institution or other entity regulated by the department or the amount of his or her deposit or debt to anyone, except insofar as may be necessary in the performance of his or her official duty.

- **Employee Privacy**

- NEB. REV. STAT. § 48-612 (2009) - Each employer, whether or not subject to the Employment Security Law, shall keep true and accurate work records containing such information as the Commissioner of Labor may prescribe. Such records shall be open to inspection and be subject to being copied by the commissioner or his or her authorized representatives at any reasonable time and as often as may be necessary. The commissioner and the appeal tribunal may require from any such employer any sworn or unsworn reports, with respect to persons employed by it, which he, she, or it deems necessary for the effective administration of such law. Except as otherwise provided in section 48-612.01, information thus obtained or obtained from any individual pursuant to the administration of such law shall be held confidential.
- NEB. REV. STAT. § 48-1901 through -1910 (2009) - Drug Testing. Any results of any test performed on the body fluid or breath specimen of an employee, as directed by the employer, to determine the presence of drugs or alcohol shall not be used to deny any continued employment or in any disciplinary or administrative action unless certain quality control is in place. Unacceptable to not submit to the test. Can be grounds for a denial of employment. No information on whether the result is confidential or may be entered into evidence.

- **Electronic Surveillance**

- NEB. REV. STAT. § 86-274 (2009) Contents, defined
- NEB. REV. STAT. § 86-275 (2009) Electronic, mechanical, or other device, defined
- NEB. REV. STAT. § 86-276 (2009) Electronic communication, defined. Electronic communication means any transfer of signs, signals, writing, images, sounds,

data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system but does not include: (1) The radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit; (2) Any wire or oral communication; (3) Any communication made through a tone-only mobile paging device; or (4) Any communication from a mobile tracking device as defined in section 86-2,103.

- NEB. REV. STAT. § 86-277 (2009) Electronic communication service, defined
- NEB. REV. STAT. § 86-278 (2009) Electronic communication system, defined
- NEB. REV. STAT. § 86-279 (2009) Electronic storage, defined
- NEB. REV. STAT. § 86-280 (2009) Intercept, defined. Intercept means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.
- NEB. REV. STAT. § 86-290 (2009) Unlawful acts; penalty. Intentionally intercept, use, disclose or to endeavor, or procure any other person to the same any wire, electronic, or oral communication. Exceptions with the consent of one party, for law enforcement, for common carriers, for public frequencies, or interception to prevent harmful frequencies.
- NEB. REV. STAT. § 86-291 (2009) Interception; court order. Attorney general or county attorney may apply for an interception order where interception may provide or has provided evidence of the commission of the offense of murder, kidnapping, robbery, bribery, extortion, dealing in narcotic or other dangerous drugs, sexual assault of a child or a vulnerable adult, visual depiction or possessing a visual depiction of sexually explicit conduct of a child, or child enticement by means of a computer, or any conspiracy to commit any such offense.
- NEB. REV. STAT. § 86-292 (2009). Interception; privileged use. Law enforcement may disclose and use lawful interceptions to other agencies. Otherwise privileged content does not lose its privileged character.
- NEB. REV. STAT. § 86-293 (2009). Interception; procedure; appeal. Within a reasonable time, but not longer than ninety days after the termination of the period of an order or extensions thereof, the issuing judge shall cause the applicant to serve on the persons named in the order or the application and such other parties to intercepted communications which the judge may determine to be in the interest of justice an inventory which shall include: (i) The entry of the order of application; (ii) the date of such entry and the period of authorized or approved interception or the denial of the application; and (iii) whether, during such period, wire, electronic, or oral communications were or were not intercepted.
- NEB. REV. STAT. § 86-294 (2009). Interception; reports. Each year the attorney general has to report to the Admin Office of the United States Courts the number of interceptions applied for and granted.
- NEB. REV. STAT. § 86-295 (2009). Violations; penalty
- NEB. REV. STAT. § 86-296 (2009). Electronic devices; prohibited acts; penalty. Sends in intrastate commerce any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the unlawful surreptitious interception of wire,

electronic, or oral communications. Manufactures, assembles, possesses, or sells any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the unlawful surreptitious interception of wire, electronic, or oral communications. There are exceptions for law enforcement and federal and telecommunications employees in the normal course of business.

- NEB. REV. STAT. § 86-2,104 (2009) - Electronic communication service; unauthorized access; penalty. Any person who (a) intentionally accesses without authorization a facility through which an electronic communication service is provided or (b) intentionally exceeds an authorization to access the facility while it is in electronic storage in such service is subject to penalty. Doesn't apply to the employees to are responsible for the storage or to the person who is a user of the stored item.
- NEB. REV. STAT. § 86-2,105 (2009). Electronic communication service; disclosure. Common carriers may not disclose communications in storage to anyone but the intended recipient, except upon consent or to law enforcement if they appear to be in furtherance of a crime.
- NEB. REV. STAT. § 86-2,106 (2009). Electronic communication service; remote computing service; disclosure; government access. A governmental entity may require the disclosure by a provider of electronic communication service of the contents of an electronic communication that is in electronic storage in an electronic communications system for one hundred eighty days or less, only pursuant to a warrant. For longer than 180 days, a governmental entity may receive disclosure without notice to the customer if a warrant has been obtained, or with prior notice if an administrative subpoena or court order is used.
- NEB. REV. STAT. § 86-2,103 (2009). Mobile tracking device; use (1) A district court may issue a warrant or other order for the installation of a mobile tracking device, and such order may authorize the use of that device within the jurisdiction of the court and outside that jurisdiction if the device is installed in that jurisdiction. (2) For purposes of this section, mobile tracking device means an electronic or mechanical device which permits the tracking of the movement of a person or object.
- **Computer Statutes**
 - NEB. REV. STAT. § 28-1343.01 (2009). Unauthorized computer access. A person commits the offense of unauthorized computer access if the person intentionally and without authority penetrates a computer security system.
 - NEB. REV. STAT. § 28-1345 (2009). Any person who accesses or causes to be accessed any computer, computer system, computer software, or computer network without authorization or who, having accessed any computer, computer system, computer software, or computer network with authorization, knowingly and intentionally exceeds the limits of such authorization shall be guilty of a Class IV felony if he or she intentionally: (1) Alters, damages, deletes, or destroys any computer, computer system, computer software, computer network, computer program, data, or other property; (2) disrupts the operation of any computer, computer system, computer software, or computer network; or (3) distributes a destructive computer program with intent to damage or destroy any computer,

computer system, computer network, or computer software, except that any person who causes loss with a value of one thousand dollars or more by such conduct shall be guilty of a Class III felony.

- NEB. REV. STAT. § 28-1347 (2009) Any person who intentionally accesses any computer, computer system, computer software, computer network, computer program, or data without authorization and with knowledge that such access was not authorized or who, having accessed any computer, computer system, computer software, computer network, computer program, or data with authorization, knowingly and intentionally exceeds the limits of such authorization shall be guilty of a Class V misdemeanor. For any second or subsequent offense under this section, such person shall be guilty of a Class II misdemeanor.
- **Common Law**
 - Rights of privacy law are codified as NEB. REV. STAT. §§ 20-201 through 20-211. There still exists reference to the common law in cases:
 - See Wadman v. State, 510 N.W.2d 426 (Neb. Ct. App. 1993); Miller v. Amer. Sports Co., 467 N.W.2d 653 (Neb. 1991); Schoneweiss v. Dando, 435 N.W.2d 666 (Neb. 1989).

NEVADA PRIVACY LAW

- **State Constitutional Privacy Rights**
 - none
- **Search and Seizure**
 - NEV. CONST. art. I, § 18 Protects against unreasonable search and seizure.
 - **Auto Exception**
 - Fletcher v. State, 990 P.2d 192 (Nev. 1999)
 - **Open Fields**
 - State v. Barr, 651 P.2d 649 (Nev. 1982)
 - **Plain View**
 - Johnson v. State, 637 P.2d 1209 (Nev. 1981)
- **Statutory Privacy Rights**
 - NEV. REV. STAT. ANN. § 200.575 (2009) Stalking. A person who, without lawful authority, willfully or maliciously engages in a course of conduct that would cause a reasonable person to feel terrorized, frightened, intimidated or harassed, and that actually causes the victim to feel terrorized, frightened, intimidated or harassed, commits the crime of stalking. Increased penalties if done with a weapon or if a repeat offender.
- **Public Records**
 - NEV. REV. STAT. ANN. § 239.010 (2009) - Except as otherwise provided in subsection 3, all public books and public records of a governmental entity, the contents of which are not otherwise declared by law to be confidential, must be open at all times during office hours to inspection by any person.
 - Nev. Rev. Stat. Ann. § 239.0105 (2009) - confidentiality of certain local records including anything with personally identifying information, or social security numbers.
 - NEV. REV. STAT. ANN. § 239.013 (2009) library records are confidential
 - NEV. REV. STAT. ANN. § 239.012 (2009) - Public officers who act in good faith in disclosing or refusing to disclose information are immune from liability.
 - NEV. REV. STAT. ANN. § 665.130 (2009) - The reports filed with or prepared by the division of financial institutions and other information obtained from a depository institution are not public records and may not be disclosed, except information concerning financial institutions which by specific statute is made generally available to the public.
- **Motor Vehicle Records**
 - NEV. REV. STAT. ANN. § 483.916 (2009) - will release the driving record of any person to any driver's license administrator, employer/prospective employer or any insurer.
 - NEV. REV. STAT. ANN. § 482.235 (2009) - permanent records of vehicle registrations and certificates of title including VINs will be kept by the department of motor vehicles.
 - NEV. REV. STAT. ANN. § 484.229 (2009) - accident reports are confidential and are for the confidential use of the Department or other state agencies having use of the records for accident prevention. Other disclosures related to the parties involved in the accident are permissible.
- **Vehicle Identification Numbers**

- NEV. REV. STAT. ANN. § 484.241 (2009) - repair shops must keep records (including the VIN) of any motor vehicle which shows evidence of having been involved in an accident and which is repaired in the shop.
- NEV. REV. STAT. ANN. § 484.241 (2009) - it is unlawful to knowingly operate a vehicle which has an altered VIN.
- **Consumer Credit**
 - NEV. REV. STAT. ANN. § 599B.200 (2009) - A salesman or seller shall not disclose the name or address of any person who purchases goods or services pursuant to a solicitation governed by this chapter. Nothing in this section prohibits the disclosure of this information to: 1. Any person employed by or associated with the seller; 2. The commissioner or any employee of the division; or 3. Any law enforcement officer or agency that requires the information for investigative purposes.
 - NEV. REV. STAT. ANN. § 598C.120 (2009) - person shall not procure a consumer report to resell or disclose the report or the information contained in the report unless the person discloses to the reporting agency which originally furnished the report: 1. The identity of the intended ultimate user of the report or information; and 2. The only purposes for which the information will be used.
 - NEV. REV. STAT. ANN. § 598C.140 (2009) - A reporting agency may furnish a consumer report concerning a consumer for an extension of credit which he did not initiate only if: (a) The contemplated transaction represents a firm offer of credit to those consumers who meet specific criteria determined by the person; or (b) He has not requested that his name and address be excluded from any list to be provided for such a purpose.
 - NEV. REV. STAT. ANN. § 598C.300 (2009) consumer may place a security freeze in his file by making a request in writing by certified mail to the reporting agency. At the time of the request, the consumer must provide to the reporting agency sufficient identification to establish the identity of the consumer.
 - NEV. REV. STAT. ANN. § 603A.010 through 603A.300 (2009) Any data collector that owns or licenses computerized data which includes personal information shall disclose any breach of the security of the system data following discovery or notification of the breach to any resident of this State whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection 3, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system data.
 - "Breach of the security of the system data" means unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of personal information maintained by the data collector. The term does not include the good faith acquisition of personal information by an employee or agent of the data collector for a legitimate purpose of the data collector, so long as the personal information is not used for a purpose unrelated to the data collector or subject to further unauthorized disclosure.

- **Financial Records**

- NEV. REV. STAT. ANN. § 239A.080 (2009) - An officer, employee or agent of a governmental agency shall not request or receive the financial records of any customer from a financial institution unless: (a) The request relates to a lawful investigation of the customer; (b) The financial records are described in the request with particularity and are consistent with the scope and requirements of the investigation; and (c) The officer, employee or agent furnishes the financial institution with a customer authorization, subpoena or search warrant authorizing examination or disclosure of such records as provided in this chapter.
 - A director, officer, employee or agent of a financial institution shall not provide or authorize another person to provide to an officer, employee or agent of a governmental agency any financial records of a customer if the director, officer, employee or agent of the financial institution knows or has reason to believe that the financial records are being requested in connection with an investigation of the customer, unless the request is accompanied by a customer authorization, subpoena or search warrant authorizing examination or disclosure of such records as provided in this chapter.
- NEV. REV. STAT. ANN. § 239A.140 (2009) - Financial institutions must maintain for five years a record of all disclosures of the financial records of a customer.

- **Employee Privacy**

- **Electronic Surveillance**

- NEV. REV. STAT. ANN. § 179.410 through .515 (2009). Interception of oral or wire communication. Doesn't specifically include electronic communication in this section, but there is an electronic reference below.
- NEV. REV. STAT. ANN. § 179.460 (2009). Cases in which interception of wire or oral communications may be authorized. District Attorneys may apply to a supreme court or district judge for authorization to intercept a wire or oral communication if the interception may provide evidence of the commission of murder, kidnapping, robbery, extortion, bribery, destruction of public property by explosives, a sexual offense against a child or the commission of any offense which is made a felony by the provisions of chapter 453 or 454 of NRS.
- NEV. REV. STAT. ANN. § 179.465 (2009) Disclosure or use of intercepted communications. Permissible by law enforcement personnel performing official duties, or by any person who has lawfully received such information while giving testimony under oath in any criminal proceeding.
- NEV. REV. STAT. ANN. § 179.470 (2009) Application for order authorizing interception of communications; prerequisites to issuance of order. Require particularized information concerning the communication sought to be intercepted, the place where the communication will take place, the identity of the suspect and the nature of the criminal investigation.
- NEV. REV. STAT. ANN. § 179.475 (2009) Orders authorizing interceptions must limit the time period in which particular authorized eavesdropping is permitted.
- NEV. REV. STAT. ANN. § 179.485 (2009) Recordings of the contents of intercepted communications must be sealed and placed in the custody of the authorizing judge.

- NEV. REV. STAT. ANN. § 179.495 (2009) Notice. **1.** Within a reasonable time but not later than 90 days after the termination of the period of an order or any extension thereof, the judge who issued the order shall cause to be served on the chief of the investigation division of the department of public safety, persons named in the order and any other parties to intercepted communications, an inventory which must include notice of: **(a)** The fact of the entry and a copy of the order. **(b)** The fact that during the period wire or oral communications were or were not intercepted.
- NEV. REV. STAT. ANN. § 200.620 (2009). Interception and attempted interception of wire communication prohibited; exceptions. It is unlawful for any person to intercept or attempt to intercept any wire communication unless: (a) The interception or attempted interception is made with the prior consent of one of the parties to the communication; and (b) An emergency situation exists and it is impractical to obtain a court order as required. This section doesn't apply to common carriers who are acting in the course of employment.
- NEV. REV. STAT. ANN. § 200.650 (2009). Unauthorized, surreptitious intrusion of privacy by listening device prohibited. Except as otherwise provided, a person shall not intrude upon the privacy of other persons by surreptitiously listening to, monitoring or recording, or attempting to listen to, monitor or record, by means of any mechanical, electronic or other listening device, any private conversation engaged in by the other persons, or disclose the existence, content, substance, purport, effect or meaning of any conversation so listened to, monitored or recorded, unless authorized to do so by one of the persons engaging in the conversation.
- NEV. REV. STAT. ANN. § 200.690 (2009). Penalties for violating the prohibition against eavesdropping.
- NEV. REV. STAT. ANN. § 331.220 (2009) Surreptitious electronic surveillance prohibited; exceptions. Unlawful for a person to engage in any kind of surreptitious electronic surveillance on the grounds of any facility owned or leased by the State of Nevada without the knowledge of the person being observed. Exceptions include: authorized by court order, part of criminal investigation, as part of a system of security.
- NEV. REV. STAT. ANN. § 393.400 (2009) Surreptitious electronic surveillance; exceptions. Unlawful for a person to engage in any kind of surreptitious electronic surveillance on any property of a public school without the knowledge of the person being observed. Exceptions include: authorized by court order, part of criminal investigation, as part of a system of security, or if authorized by the teacher.
- NEV. REV. STAT. ANN. § 396.970 (2009) Surreptitious electronic surveillance on campus; exceptions. Unlawful for a person to engage in any kind of surreptitious electronic surveillance on a campus of the system without the knowledge of the person being observed. Exceptions include: authorized by court order, part of criminal investigation, as part of a system of security, or if authorized by the teacher.
- NEV. REV. STAT. ANN. § 707.340 (2009) Public utility furnishing telephone service required to assist peace officers in tracing certain callers; immunity for

good faith reliance; limitations concerning wiretapping. Ok to trace 911 calls and calls that seem to indicate the person has threatened the addressee.

- Osburn v. State, 44 P.3d 523 (Nev. 2002) - Attachment of an electronic tracking device to the bumper of defendant's vehicle, which was parked on the street outside his residence, did not constitute an unreasonable search or seizure under the Nevada Constitution.
- **Computer Statutes**
 - NEV. REV. STAT. ANN. § 205.473 through 205.513 (2009) - Unlawful Acts Regarding Computers and Information Services. Unlawful to knowingly and without authorization to obtain or permit access to a computer program or system or network. Unlawful to alter or delete any data, information, image, program, signal or sound contained in any computer, system or network which, if done on a written or printed document or instrument, would constitute forgery. Unlawful to use encryption improperly.
- **Common Law**
 - Helter v. Eight Judicial Dist. of Nevada, 874 P.2d 762 (Nev. 1994) - recognizes the four torts arising from an invasion of privacy.

NEW HAMPSHIRE PRIVACY LAW

- **State Constitutional Privacy Rights**
 - **Express**
 - none
 - **Implied**
 - N.H. CONST. pt. I, art. XV - the right against self incrimination is one of the rights of the accused.
- **Search and Seizure**
 - N.H. CONST. pt. I, art. XIX - protects against unreasonable searches and seizures of one's person, houses, and all one's possessions.
 - State v. Koppel, 499 A.2d 977 (N.H. 1985) - state constitution provides more protection than the Fourth Amendment. The stop and detention of a car is a seizure. Shows that there are no less intrusive means and the public interest significantly outweighs viewing a car stop any other way.
 - State v. Landry, 358 A.2d 661 (N.H. 1976) - analysis of reasonability of a seizure weighs the right to personal privacy against the state's compelling interest in safety on public highways.
 - **Auto Exception**
 - State v. Sterndale, 656 A.2d 409 (N.H. 1995) - declining to adopt the automobile exception to the warrant requirement.
 - **Open Fields**
 - State v. Pinder, 514 A.2d 1241 (N.H. 1986).
 - **Plain View**
 - State v. Murray, 598 A.2d 206 (N.H. 1991).
- **Statutory Privacy Rights**
 - N.H. REV. STAT. ANN. § 644:9 (2009) - Violation of Privacy. A person is guilty of a class A misdemeanor if such person unlawfully and without the consent of the persons entitled to privacy therein, installs or uses a device to observe or record persons with the expectation of privacy, where intimate body parts may be exposed.
 - N.H. REV. STAT. ANN. § 633:3-a (2009) Stalking. A person commits the offense of stalking if such person: (a) Purposely, knowingly, or recklessly engages in a course of conduct targeted at a specific person which would cause a reasonable person to fear for his or her personal safety or the safety of a member of that person's immediate family, and the person is actually placed in such fear; (b) Purposely or knowingly engages in a course of conduct targeted at a specific individual, which the actor knows will place that individual in fear for his or her personal safety or the safety of a member of that individual's immediate family or violates a protective order.
 - N.H. REV. STAT. ANN. §77-B:26 (2009). Confidentiality of Department of Revenue Administration Records. Notwithstanding any other provision of law and except as hereinafter provided, the records and files of the department of revenue administration respecting the administration of this chapter are confidential and privileged.
- **Individually Identifiable Government Records**

- N.H. REV. STAT. ANN. §106-B:14 (2009). Criminal Records inspected by authorized persons only.
 - Law enforcement personnel may request and receive any information documenting an individual's contact with the criminal justice system, including data regarding identification, arrest or citation, arraignment, judicial disposition, custody and supervision.
 - Any individual may request and receive a copy of his or her own criminal conviction and arrest records and related information.
 - Any individual or any public or private agency may request and receive a copy of the criminal conviction record of another who has provided authorization in writing, duly signed and notarized, explicitly allowing the requestor to receive such information.
 - An employee of or person under contract to the state of New Hampshire to whom such disclosure is necessary in connection with the processing, storage, and transmission of such information, or the programming, repair, maintenance, testing, or procurement of equipment used to process, store, or transmit such information.
- N.H. REV. STAT. ANN. § 478:4-b (2009)
 - The preparer of a document shall not include an individual's social security number, credit card number, or deposit account numbers in a document that is prepared and presented for recording in the office of the register of deeds. This paragraph shall not apply to state or federal tax liens, certified copies of death certificates, and other documents required by law to contain such information that are filed or recorded in the office of the register of deeds.
 - A deed or instrument that includes an individual's social security number, credit card number, or deposit account numbers, was filed with the register of deeds and is available on the Internet, the individual may request that the register of deeds redact such information from the Internet record. The register of deeds shall establish a procedure by which individuals may request that such information be redacted from its files which are available on the Internet. Upon request, the information shall be redacted.
- **Public Records**
 - N.H. REV. STAT. ANN. §201-D:11 (2009) Library User Records are confidential.
 - N.H. REV. STAT. ANN. §41:58 (2009) - all books, records, papers and documents in possession of officer or committee of a town are public.
 - N.H. REV. STAT. ANN. § 33-A:3-a (2009) - time period each record must be held for by the municipality. Suggests that these are the records available for inspection
 - N.H. REV. STAT. ANN. § 91-A:1-a (2009) - Court, governor's council any board of a commission, agency, or authority of state is a public proceeding.
 - N.H. REV. STAT. ANN. § 91-A:5 (2009) - exemptions from public record are pupil records, library records, confidential financial information and other files whose disclosure would constitute an invasion of privacy.
- **Motor Vehicle Records**

- N.H. REV. STAT. ANN. § 33-A: 3-a (2009) Time period the following records must be maintained by the local departments. Motor vehicle-application for title: until audited plus one year; Motor vehicle-titles and voided titles: sent to state division of motor vehicles; Motor vehicle permits-void and unused: until audited plus one year; Motor vehicle permits and registrations-used: current year plus 3 years.
- N.H. REV. STAT. ANN. § 263:60 (2009) A full record shall be kept by every court or justice in this state of every case in which a person is charged with a violation of any of the provisions of any law relative to motor vehicles, and an abstract of the record in cases of conviction shall be sent within 7 days by the court or justice to the department. Said abstracts shall be made upon forms prepared under authority of the director and shall include all necessary information as to the parties to the case, the nature and date of the offense, the date of the hearing, the plea and the judgment, and shall be certified by the clerk of the court or by the justice. The department shall keep such records in its office, and they shall be open to the inspection of any person.
- N.H. REV. STAT. ANN. § 260.14 (2009) - Proper motor vehicle records shall be kept by the department at its office. Notwithstanding RSA 91-A or any other provision of law to the contrary, except as otherwise provided in this section, such records shall not be public records or open to the inspection of any person.
 - Motor vehicle records may be made available pursuant to a court order or in response to a request from a state, a political subdivision of a state, the federal government, or a law enforcement agency for use in official business. The request shall be on a case-by-case basis. Any records received pursuant to this paragraph shall not be further transferred or otherwise made available to any other person or listed entity not authorized under this paragraph.
 - *Except for a person's photograph, computerized image, and social security number, motor vehicle records may be made available to the department of transportation for the enforcement of the electronic toll collection, pursuant to RSA 236:31. Any records received under this paragraph shall not be further transferred or otherwise made available to any non-governmental agency that is not a contracting agent of the department of transportation for the enforcement of electronic toll collection.*
- N.H. REV. STAT. ANN. § 236:31 (2009) - Any electronic toll collection monitoring equipment acquired, operated by, or used by the department, or its designee, shall be designed to make a record of the front, or rear, or both, portions of the vehicle, including any registration plates affixed to the vehicle. Such equipment shall not be designed to produce a photograph, microphotograph, videotape, or other recorded image of the face of the operator or any passenger in the motor vehicle, unless the production of such image is unavoidable because the operator or passenger is not in a passenger compartment, as on a motorcycle.
 - The department, and any designee of the department, shall maintain the confidentiality of all information acquired in connection with the administration and enforcement of toll evasion, including but not limited

to credit and account data, photographs or other images, and all personally identifying information obtained relative to owners of vehicles. Such information shall not be a public record subject to disclosure under RSA 91-A and shall be used solely for enforcement of this section.

- "Electronic toll collection system" means a system for electronically transmitting information from a device on a motor vehicle to receiving equipment located in a toll collection facility, in order to charge a valid electronic toll account holder the appropriate toll or charge for use of the highway or bridge.
 - "Electronic toll collection monitoring system" means a system whereby a vehicle sensor is placed in a location to work in conjunction with an electronic toll collection system to produce at least one photograph, microphotograph, videotape, recorded image, or written record of a portion of the vehicle when the vehicle is used or operated in violation of the electronic toll collection system rules. "Electronic toll collection monitoring system" shall also include any other technology that identifies a vehicle by a photographic, electronic, or other method.
 - N.H. REV. STAT. ANN. § 263:40-a (2009) The social security number shall not be a public record open to the inspection of any person. The department shall not sell or otherwise provide individual social security numbers or lists of social security numbers for any purpose which is not stated in this paragraph. The department shall only make the social security number available to other states for driver record purposes, to any national driver information repository established pursuant to federal law, or, on their request on a case by case basis (a) to a law enforcement agency that requires the social security number for investigative purposes, or (b) to the department of health and human services for use only in the administration of child support enforcement.
- **Vehicle Identification Numbers**
 - State v. McGann, 467 A.2d 571 (N.H. 1983) Under the New Hampshire Constitution, an official inspection of a vehicle identification number which is not in plain view and which is located within the vehicle constitutes a search. Consequently, for such a search to be legal, it must have taken place pursuant to a warrant or one of the established exceptions to the warrant requirement.
- **Consumer Credit**
 - N.H. REV. STAT. ANN. § 359-B:3 (2009) Consumer reports reflect credit worthiness, investigative report reflects character, both have restricted distribution.
 - N.H. REV. STAT. ANN. § 359-B:4 (2009) Consumer reports may be furnished in response to court order, by consumer's request or by a third party in connection with a transaction for the extension of credit or insurance.
 - N.H. REV. STAT. ANN. § 359-B:4a (2009) A consumer may elect to have information about such consumer excluded from any transaction not initiated by the consumer under RSA 359-B:4, II, including any list provided by a consumer reporting agency through pre-screening or direct solicitation transactions that are not initiated by the consumer, by notifying the consumer reporting agency by telephone or in writing.

- N.H. REV. STAT. ANN. § 359-B:5 (2009) Obsolete Information. In a credit report, can't disclose information that is antedate, ex. no bankruptcies from over 14 years ago.
- N.H. REV. STAT. ANN. § 359-B:6 (2009) Disclosure of Investigative Consumer Reports.
- N.H. REV. STAT. ANN. § 359-B:8 (2009) Disclosures to Governmental Agencies.
- N.H. REV. STAT. ANN. § 359-B:9 (2009) Disclosures to Consumers.
- N.H. REV. STAT. ANN. § 359-B:10 (2009) Conditions of Disclosure to Consumers.
- N.H. REV. STAT. ANN. § 359-B:13 (2009) Public Record Information for Employment Purposes is acceptable even without telling the record holder.
- N.H. REV. STAT. ANN. § 359-B:15 (2009) - Whenever credit or insurance for personal, family, or household purposes, or employment involving a consumer, is denied or the charge for such credit or insurance is increased either wholly or partly because of information contained in a consumer report from a consumer reporting agency, the user of the consumer report shall so advise the consumer against whom such adverse action has been taken and supply the name and address of the consumer reporting agency making the report.
- N.H. REV. STAT. ANN. § 359-B:20 (2009) Unauthorized Disclosures by Officers and Employees. Any officer or employee of a consumer reporting agency that knowingly and willfully provides information concerning an individual from the agency's files to a person not authorized to receive that information shall be fined not more than \$5,000 or imprisoned not more than one year, or both.
- N.H. REV. STAT. ANN. § 359-C:19 (2009) person doing business in this state who owns or licenses computerized data that includes personal information shall, when it becomes aware of a security breach, promptly determine the likelihood that the information has been or will be misused. If the determination is that misuse of the information has occurred or is reasonably likely to occur, or if a determination cannot be made, the person shall notify the affected individuals as soon as possible as required under this subdivision.
- N.H. REV. STAT. ANN. § 359-B:22; 23 (2009) - permissible for employees to issue a security freeze on their credit report.
- **Financial Records**
 - N.H. REV. STAT. ANN. § 383:10-e (2009) Banks and Banking. The commissioner may disclose to the public the number and type of complaints or inquiries filed by consumers against a particular person or entity; provided, however, that no such disclosure shall abridge the confidentiality of consumer complaints or inquiries.
 - N.H. REV. STAT. ANN. § 392:9-a (2009) All confidential information received in connection with any petition or application of or concerning a family fiduciary services company shall be confidential communications, shall not be subject to subpoena, and shall not be made public unless, in the judgment of the commissioner, the ends of justice and the public advantage will be served by the publication of the information. The commissioner may, at his or her discretion on request or otherwise, determine that confidential information received in connection with any petition or application of or concerning a public trust company other than a family fiduciary services company should not be publicly available, in which case such information shall be confidential communications,

shall not be subject to subpoena, and shall not be disclosed unless, in the judgment of the commissioner, the ends of justice and the public advantage will be served by the disclosure of the information.

- **Employee Privacy**

- N.H. REV. STAT. ANN. § 91-A:6 (2009) Employment security. Keeps records exempt per the public record requirement and medical information, etc.
- N.H. REV. STAT. ANN. 282-A:117 (2009) Unemployment Compensation. Each employing unit shall keep true and accurate work records for such periods of time and containing such information as the commissioner may by rules prescribe. Such records shall be open to inspection and subject to be copied or reproduced by the commissioner, or his authorized representatives in this state at any reasonable time and as often as may be necessary at a place selected by the commissioner.

- **Electronic Surveillance**

- N.H. REV. STAT. ANN. § 570-A:1 (2009) Definitions. Doesn't specifically include electronic communications.
- N.H. REV. STAT. ANN. § 570-A:2 (2009) Interception and Disclosure of Telecommunication or Oral Communications Prohibited. Willful interception or disclosure of interception is a felony. Exception for law enforcement officers if acting in the course of duty, common carriers, the FCC and operators of school buses in some circumstances.
- N.H. REV. STAT. ANN. § 570-A:3 Manufacture, Distribution, Possession, and Advertising of Telecommunication or Oral Communication Intercepting Devices Prohibited
- N.H. REV. STAT. ANN. § 570-A:4 Confiscation of Telecommunication or Oral Communication Intercepting Devices
- N.H. REV. STAT. ANN. § 570-A:5 Immunity of Witnesses
- N.H. REV. STAT. ANN. § 570-A:6 Prohibition of Use as Evidence of Intercepted Telecommunications or Oral Communications
- N.H. REV. STAT. ANN. § 570-A:7 Authorization for Interception of Telecommunications or Oral Communications. The attorney general or county attorney may apply to a judge for interception if the interception may provide evidence of the commission of organized crime, as defined in, XI, or evidence of the commission of the offenses of homicide, kidnapping, gambling, theft as defined in, corrupt practices as defined in, child pornography under, computer pornography and child exploitation under, criminal conduct in violation of the securities law, as defined, criminal conduct in violation of the security takeover disclosure laws, as defined in, and, robbery as defined in, arson as defined in hindering apprehension or prosecution as defined in tampering with witnesses and informants as defined in aggravated felonious sexual assault as defined in felonious sexual assault as defined in escape as defined in, bail jumping as defined in insurance fraud as defined in, dealing in narcotic drugs, marijuana, or other dangerous drugs, hazardous waste violations under or any conspiracy to commit any of the foregoing offenses.
- N.H. REV. STAT. ANN. § 570-A:8 Authorization for Disclosure and Use of Intercepted Telecommunications or Oral Communications. Other law

enforcement agencies can be informed of the communication if in the course of their duties.

- N.H. REV. STAT. ANN. § 570-A:9 (2009) Procedure for Interception of Telecommunication or Oral Communications
- N.H. REV. STAT. ANN. § 570-A:10 (2009) Reports Concerning Intercepted Telecommunications or Oral Communications. Within 30 days after the expiration of an order, or each extension thereof, or the denial of an order approving an interception, the approving/denying judge will inform the admin office of the United States Courts.
- **Computer Statutes**
 - N.H. REV. STAT. ANN. § 638:16 through §638:16 (2009) unauthorized access, disruption of system, and data tampering are crimes.
- **Common Law**
 - Hamberger v. Eastman, 206 A.2d 239 (N.H. 1964) - recognizes the four strands of the invasion of privacy common law. Specifically ruled on intrusion in this case.

NEW JERSEY PRIVACY LAW

- **State Constitutional Privacy Rights**
 - **Implied**
 - State v. Reid, 914 A.2d 310 (N.J. Super. Ct. App. Div. 2007) The right to privacy of New Jersey citizens under the New Jersey Constitution has been expanded to areas not afforded such protection under the Fourth Amendment. While 10 states have explicit rights to privacy in their state constitutions, New Jersey is among the few states to have found an implied right to privacy in its state charter. Of these, only New Jersey appears to have recognized a right to what has been called "informational privacy." Informational privacy has been variously defined as shorthand for the ability to control the acquisition or release of information about oneself, or an individual's claim to control the terms under which personal information is acquired, disclosed, and used. In general, informational privacy encompasses any information that is identifiable to an individual. This includes both assigned information, such as a name, address, or Social Security number, and generated information, such as financial or credit card records, medical records, and phone logs. Personal information will be defined as any information, no matter how trivial, that can be traced or linked to an identifiable individual.
- **Search and Seizure**
 - N.J. CONST. art I, para. 7 - protects against unreasonable search and seizure.
 - In re Quinlan, 355 A.2d 647 (N.J. 1976) - there is a reasonable expectation of privacy in garbage.
 - **Auto Exception**
 - State v. Birkenmeier, 888 A.2d 1283 (N.J. 2005)
 - **Open Fields**
 - Middlesex City Health Dept. v. Roehsler, 561 A.2d 1212 (N.J. 1989).
 - **Plain View**
 - State v. Bruzzese, 463 A.2d 320 (N.J. 1983)
- **Statutory Privacy Rights**
 - N.J. STAT. ANN. § 2A:58D-1 (2009) - Invasion of privacy with photographs, films, videotapes, liability, civil action; damages, costs. An actor who, without license or privilege to do so, photographs, films, videotapes, records, or otherwise reproduces in any manner, the image of another person whose intimate parts are exposed or who is engaged in an act of sexual penetration or sexual contact, without that person's consent and under circumstances in which a reasonable person would not expect to be observed, shall be liable to that person, who may bring a civil action.
 - N.J. STAT. ANN. § 2C:14-9 (2009). Invasion of privacy, degree of crime; defenses, privileges. actor commits a crime of the fourth degree if, knowing that he is not licensed or privileged to do so, and under circumstances in which a reasonable person would know that another may expose intimate parts under circumstances a person would not expect to be observed.
 - N.J. STAT. ANN. § 2C:12-10 (2009) - A person is guilty of stalking, a crime of the fourth degree, if he purposefully or knowingly engages in a course of conduct

directed at a specific person that would cause a reasonable person to fear bodily injury to himself or a member of his immediate family or to fear the death of himself or a member of his immediate family.

- N.J. STAT. ANN. § 56:8-164 (2009). Prohibited actions relative to display of Social Security numbers. No person, including any public or private entity, shall: (1) Publicly post or publicly display an individual's Social Security number, or any four or more consecutive numbers taken from the individual's Social Security number; (2) Print an individual's Social Security number on any materials that are mailed to the individual, unless State or federal law requires the Social Security number to be on the document to be mailed; (3) Print an individual's Social Security number on any card required for the individual to access products or services provided by the entity; (4) Intentionally communicate or otherwise make available to the general public an individual's Social Security number; (5) Require an individual to transmit his Social Security number over the Internet, unless the connection is secure or the Social Security number is encrypted; or (6) Require an individual to use his Social Security number to access an Internet web site, unless a password or unique personal identification number or other authentication device is also required to access the Internet web site.
- **Public Records**
 - N.J. STAT. ANN. § 2A:4A-60 (2009) - records pertaining to juveniles must be strictly safeguarded from public inspection.
 - N.J. STAT. ANN. § 47:1A-1 through -13 (2009) government records shall be readily accessible for inspection, copying, or examination by the citizens of this State, with certain exceptions, for the protection of the public interest, and any limitations on the right of access.
 - exceptions include pension records, incomplete legal proceedings, biotech trade secrets, test questions for state exams,
 - that portion of any document which discloses the Social Security number, credit card number, unlisted telephone number or driver license number of any person; except for use by any government agency, including any court or law enforcement agency, in carrying out its functions, or any private person or entity acting on behalf thereof, or any private person or entity seeking to enforce payment of court-ordered child support; except with respect to the disclosure of driver information by the New Jersey Motor Vehicle Commission as permitted.
- **Motor Vehicle Records**
 - N.J. STAT. ANN. § 47:1A-1.1 (2009) - Driver's license numbers are not public records, but government agents in the course of employment may view them.
 - N.J. STAT. ANN. § 39:2-3.4 (2009) - Notwithstanding the provisions of P.L.1963, c.73 (C.47:1A-1 et seq.) or any other law to the contrary, except as provided in this act, the Motor Vehicle Commission and any officer, employee or contractor thereof shall not knowingly disclose or otherwise make available to any person personal information about any individual obtained by the commission in connection with a motor vehicle record.
 - A person requesting a motor vehicle record including personal information shall produce proper identification and shall complete and submit a written

request form provided by the chief administrator for the commission's approval.

- The written request form shall bear notice that the making of false statements therein is punishable and shall include, but not be limited to, the requestor's name and address; the requestor's driver's license number or corporate identification number; the requestor's reason for requesting the record; the driver's license number or the name, address and birth date of the person whose driver record is requested; the license plate number or VIN number of the vehicle for which a record is requested; any additional information determined by the chief administrator to be appropriate and the requestor's certification as to the truth of the foregoing statements.
- Prior to the approval of the written request form, the commission may also require the requestor to submit documentary evidence supporting the reason for the request.
- Personal information shall be disclosed for use in connection with matters of motor vehicle or driver safety and theft; motor vehicle emissions; motor vehicle product alterations, recalls or advisories; performance monitoring of motor vehicles and dealers by motor vehicle manufacturers; and removal of non-owner records from the original owner records of motor vehicle manufacturers to carry out the purposes of the Automobile Information Disclosure Act or Cost Savings Act.
- May be disclosed to: government agencies, For use in the normal course of business by a legitimate business or its agents, employees or contractors, but only to verify the accuracy of personal information, for use in educational initiatives or to produce statistical reports (if the personal information is redacted), use in connection with the operation of private toll transportation facilities.

- **Vehicle Identification Numbers**

- State v. Ball, 530 A.2d 833 (N.J. Super. Ct. App. Div. 1987) - no expectation of privacy in exterior VIN.

- **Consumer Credit**

- N.J. STAT. ANN. § 56:11-17 (2009) No person which accepts a credit card for a consumer transaction shall require the credit card holder, as a condition of using a credit card in completing the consumer transaction, to provide for recordation on the credit card transaction form or any other form, any personal identification information that is not required by the issuer to complete the credit card transaction, including, but not limited to, the credit card holder's address or telephone number, or both; provided, however, that the credit card holder's telephone number may be required on a credit card transaction form if the credit card transaction is one for which the credit card issuer does not require authorization.
- N.J. STAT. ANN. § 56:11-21 (2009) when a credit card is required as a form of identification for acceptance of a check, the credit card number may not be recorded.
- N.J. STAT. ANN. § 56:8-161. Definitions relative to security of personal information

- N.J. STAT. ANN. § 56:8-162. Methods of destruction of certain customer records
- N.J. STAT. ANN. § 56:8-163. Disclosure of breach of security to customers. Any business that conducts business in New Jersey, or any public entity that compiles or maintains computerized records that include personal information, shall disclose any breach of security of those computerized records following discovery or notification of the breach to any customer who is a resident of New Jersey whose personal information was, or is reasonably believed to have been, accessed by an unauthorized person. The disclosure to a customer shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection c. of this section, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. Disclosure of a breach of security to a customer shall not be required under this section if the business or public entity establishes that misuse of the information is not reasonably possible.
- N.J. STAT. ANN. § 56:8-165 (2009). Regulations concerning security of personal information. The commissioner will promulgate records as needed.
- N.J. STAT. ANN. § 56:11-46 (2009) - consumers may elect to put a security freeze on their credit reports.
- **Financial Records**
 - N.J. STAT. ANN. § 17:16K-3 (2009) Disclosure of information by financial institution to third party. A financial institution may disclose information relative to an electronic fund transfer or account to a third party when: 1. The disclosure is necessary for the completion of an electronic fund transfer; 2. The possessor of the account gives written permission to the financial institution to disclose the information; 3. The disclosure is for the purpose of verifying the existence and condition of an account for a third party, including, but not limited to, a credit bureau or a merchant; 4. The disclosure is necessary to resolve an error or an inquiry as to an alleged error; 5. The disclosure is made to a supervisory agency in the exercise of its supervisory and regulatory examination functions with respect to a financial institution; or 6. The disclosure is made to a government agency in the exercise of its statutory functions with respect to a person applying for or receiving public assistance.
 - N.J. STAT. ANN. § 17:12B-117 (2009) Confidential relationship of an [loan or building] association to its members. The relationship of an association to each of its members constitutes a confidential relationship and no association or any of its directors, officers or employees shall disclose or be required to disclose a list of the members of the association, in whole or in part to any person; provided, however, every member of an association shall have the right to inspect the records of such association which pertain solely to his own accounts.
- **Employee Privacy**
 - N.J. STAT. ANN. § 12:17-10.9 Failing or refusing to take an employer drug test (a) Where a drug-free workplace and/or drug testing is a prerequisite of employment, an employee who tests positive for illegal drugs on a bona fide drug test of the employer or refuses to provide a test sample for the employer violates a condition of employment. If separated from employment for this reason, the employee shall be disqualified for benefits for misconduct connected with such work. (b) In order

for the disqualification for benefits in (a) above to apply, the employer shall have a written drug test policy which has been conveyed to the employees.

- **Electronic Surveillance**

- N.J. STAT. ANN. § 2A:156A-1 (2009) Short title. New Jersey Wiretapping and Electronic Surveillance Control Act.
- N.J. STAT. ANN. § 2A:156A-2 (2009) Definitions. "Electronic communication" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectric or photo-optical system that affects interstate, intrastate or foreign commerce, but does not include: (1) Any wire or oral communication; (2) Any communication made through a tone-only paging device; or (3) Any communication from a tracking device;
- N.J. STAT. ANN. § 2A:156A-3 (2009) Interception, disclosure or use of wire or oral communications; violation; penalty. Purposely intercepts, endeavors to intercept, or procures or disclose or use any other person to intercept or endeavor to intercept any wire, electronic or oral communication.
- N.J. STAT. ANN. § 2A:156A-4 (2009) Exceptions include law enforcement, common carriers, and persons intercepting public frequencies, with the consent of one party.
- N.J. STAT. ANN. 2A:156A-5 (2009) Possession, sale, distribution, manufacture, or advertisement of intercepting devices; violation; penalty
- N.J. STAT. ANN. 2A:156A-6 (2009) Exceptions and lawful activities concerning devices.
- N.J. STAT. ANN. 2A:156A-7 (2009) Nuisance; seizure and forfeiture of intercepting devices
- N.J. STAT. ANN. 2A:156A-8 (2009) Authorization for application for order to intercept communications. Judge may enter an ex parte order, as requested or as modified, authorizing the interception of a wire, electronic or oral communication, if the court determines on the basis of the facts submitted by the applicant that there is or was probable cause for belief that: The person whose communication is to be intercepted is engaging or was engaged over a period of time as a part of a continuing criminal activity or is committing, has or had committed or is about to commit an offense that included in § 2A:156A-8 (ex. kidnapping, gambling, robbery, bribery). Also must find that normal investigative procedures were unsuccessful.
- N.J. STAT. ANN. 2A:156A-9 (2009) Application for order; contents
- N.J. STAT. ANN. 2A:156A-10 (2009) Grounds for entry of order
- N.J. STAT. ANN. § 2A:156A-11 (2009) Orders affecting public and certain private communication facilities; privileged communications
- N.J. STAT. ANN. § 2A:156A-12 (2009) Order; contents; limitations; extensions; renewals; progress reports; assistance of providers; ...
- N.J. STAT. ANN. § 2A:156A-13 (2009) Verbal approval for emergency interception
- N.J. STAT. ANN. § 2A:156A-14 (2009). Recording, transfer, custody of tapes
- N.J. STAT. ANN. § 2A:156A-15 (2009). Sealing of applications, orders and supporting papers; destruction; disclosure of contents; violations

- N.J. STAT. ANN. § 2A:156A-16 (2009). Service, contents of inventory
- N.J. STAT. ANN. § 2A:156A-17 (2009). Disclosure of intercepted communications
- N.J. STAT. ANN. § 2A:156A-18 (2009). Disclosure of intercepted communications relating to other offenses
- N.J. STAT. ANN. § 2A:156A-19 (2009). Unlawful use, disclosure, third degree crime
- N.J. STAT. ANN. § 2A:156A-20 (2009). Disclosure of contents of intercepted communications at trial, proceeding
- N.J. STAT. ANN. § 2A:156A-21 (2009). Action to suppress contents of intercepted communications
- N.J. STAT. ANN. § 2A:156A-22 (2009). Report by issuing or denying judge to Administrative Director of courts; contents
- N.J. STAT. ANN. § 2A:156A-23 (2009). Annual reports of Superior Court, Supreme Court and attorney general; records of attorney general ...
- N.J. STAT. ANN. § 2A:156A-24 (2009). Civil action for damages, attorney's fee by persons whose communications are intercepted unlawfully
- N.J. STAT. ANN. § 2A:156A-25 (2009). Good faith reliance on court order as defense
- N.J. STAT. ANN. § 2A:156A-26 (2009). Partial invalidity
- N.J. STAT. ANN. § 2A:156A-27 (2009). Unlawful access to stored communications
- N.J. STAT. ANN. § 2A:156A-28 (2009). Disclosure of contents
- N.J. STAT. ANN. § 2A:156A-29 (2009). Requirements for access
- N.J. STAT. ANN. § 2A:156A-30 (2009). Backup preservation
- N.J. STAT. ANN. § 2A:156A-31 (2009). Cost reimbursement
- N.J. STAT. ANN. § 2A:156A-32 (2009). Civil action
- N.J. STAT. ANN. § 2A:156A-33 (2009). Defense to civil, criminal action
- N.J. STAT. ANN. § 2A:156A-34 (2009). Exclusivity of remedies
- **Computer Statutes**
 - N.J. STAT. ANN. § 2C:20-25 (2009). Computer criminal activity; degree of crime; sentencing. Person is guilty of computer criminal activity if the person purposely or knowingly and without authorization, or in excess of authorization: a. Accesses any data, data base, computer storage medium, computer program, computer software, computer equipment, computer, computer system or computer network; b. Alters, damages or destroys any data, data base, computer, computer storage medium, computer program, computer software, computer system or computer network, or denies, disrupts or impairs computer services, including access to any part of the Internet, that are available to any other user of the computer services; c. Accesses or attempts to access any data, data base, computer, computer storage medium, computer program, computer software, computer equipment, computer system or computer network for the purpose of executing a scheme to defraud, or to obtain services, property, personal identifying information, or money, from the owner of a computer or any third party. d. Obtains, takes, copies or uses any data, data base, computer program, computer software, personal identifying information, or other information stored in a computer, computer network, computer system, computer equipment or computer storage medium; or e.

Accesses and recklessly alters, damages or destroys any data, data base, computer, computer storage medium, computer program, computer software, computer equipment, computer system or computer network.

- N.J. STAT. ANN. § 2C:20-31 (2009). Wrongful access, disclosure of information; degree of crime; sentencing
- N.J. STAT. ANN. § 2C:20-33 (2009). Obtaining, copying, accessing program, software valued at \$1,000 or less
- **Common Law**
 - Romaine v. Kallinger, 537 A.2d 284 (N.J. 1988) Accepts false light and disclosure.
 - Rumbauskas v. Cantor, 649 A.2d 853 (N.J. 1994) - suggests that New Jersey accepts all four torts for the invasion of privacy. This case in particular dealt with appropriation.

NEW MEXICO PRIVACY LAW

- **State Constitutional Privacy Rights**
 - none
- **Search and Seizure**
 - N.M. CONST. art. II, § 10 - protects against unreasonable search and seizure.
 - **Auto Exception**
 - State v. Cardenas-Alvarez, 25 P.3d 225 (N.M. 2001)
 - **Open Fields**
 - State v. Bigler, 673 P.2d 140 (N.M. Ct. App. 1983)
 - **Plain View**
 - State v. Garcia, 413 P.2d 210 (N.M. 1966)
- **Statutory Privacy Rights**
 - N.M. STAT. ANN. § 30-3A-3 (2008) - Stalking consists of a person knowingly pursuing a pattern of conduct that would cause a reasonable person to feel frightened, intimidated or threatened. The alleged stalker must intend to place another person in reasonable apprehension of death, bodily harm, sexual assault, confinement or restraint or the alleged stalker must intend to cause a reasonable person to fear for his safety or the safety of a household member. In furtherance of the stalking, the alleged stalker must commit one or more of the following acts on more than one occasion: (1) following another person, in a place other than the residence of the alleged stalker, (2) placing another person under surveillance by being present outside that person's residence, school, workplace or motor vehicle or any other place frequented by that person, other than the residence of the alleged stalker; or (3) harassing another person.
 - N.M. STAT. ANN. § 24-21-3 (2008) Genetic Information Privacy Act - no person shall obtain genetic information or samples for genetic analysis from a person without first obtaining informed and written consent from the person or the person's authorized representative
 - N.M. STAT. ANN. § 30-12-1 (2008) Abuse of Privacy. Knowingly and without authority reading or interrupting communications of another is a crime.
- **Individually Identifiable Government Records**
 - N.M. STAT. ANN. § 29-10-7 (2008) Arrest Record Information Act. Some information is public including: records of traffic offenses and accident reports; statistical or analytical records or reports in which individuals are not identified and from which their identities are not ascertainable, and court records.
 - N.M. STAT. ANN. § 29-10-4 (2008) Lists arrest record information that is considered confidential including sources, methods or information on any person accused by not charged with a crime
 - N.M. STAT. ANN. § 57-12B-4 (2008) - use of Social Security numbers is restricted. No public display and no requirement to type this number into an internet site unless the site is encrypted and secure.
- **Public Records**
 - N.M. STAT. ANN. § 14-2-5 (2008) - declared to be the public policy of this state, that all persons are entitled to the greatest possible information regarding the affairs of government and the official acts of public officers and employees. It is the further intent of the legislature, and it is declared to be the public policy of this

state, that to provide persons with such information is an essential function of a representative government and an integral part of the routine duties of public officers and employees.

- N.M. STAT. ANN. § 14-2-1 (2008) - Lists exceptions to inspecting public records including (1) records pertaining to physical or mental examinations and medical treatment of persons confined to an institution; (2) letters of reference concerning employment, licensing or permits; (3) letters or memorandums that are matters of opinion in personnel files or students' cumulative files; and other documents determined to be confidential by law.
- N.M. STAT. ANN. § 32A-2-32 (2008) All social records pertaining to the child, including all related diagnostic evaluations, psychiatric reports, medical reports, social studies reports, records from local detention facilities, client-identifying records from facilities for the care and rehabilitation of delinquent children, pre-parole reports and supervision histories obtained by the juvenile probation office, parole officers and parole board or in possession of the department, are confidential and shall not be disclosed directly or indirectly to the public, but may be disclosed to certain other sources.
- **Motor Vehicle Records**
 - N.M. STAT. ANN. § 66-2-7 (2008). Records of the department - All records of the department relating to the administration and enforcement of the Motor Vehicle Code [66-1-1 NMSA 1978] and any other law relating to motor vehicles, the administration and enforcement of which is charged to the department, other than those declared by law to be confidential for the use of the department, shall be open to public inspection during office hours.
 - N.M. STAT. ANN. § 66-7-213 (2008) Accident reports confidential; exceptions. A. All accident reports made by persons involved in accidents or by persons in charge of garages shall be without prejudice to the individual so reporting and shall be for the confidential use of the state highway and transportation department or other state agencies having use for the records for accident prevention purposes or for the administration of the laws of this state relating to the deposits of security and proof of financial responsibility by persons driving or the owners of motor vehicles, except that the state highway and transportation department may disclose: (1) the identity of a person involved in an accident when his identity is not otherwise known or when the person denies his presence at the accident; or (2) the fact that the owner or operator of a motor vehicle involved in the accident is or is not insured and if he is insured the name and address of his insurance carrier.
- **Vehicle Identification Numbers**
 - State v. Bolton, 801 P.2d 98 (N.M. Ct. App. 1990). No expectation of privacy in an exterior VIN
- **Consumer Credit**
 - N.M. STAT. ANN. § 56-3-2(2008) A credit bureau, upon request, shall disclose the content of all information about that particular consumer which is included in his credit report or rating, if the consumer making the request presents adequate identification.

- N.M. STAT. ANN. § 56-3-3 (2008) - Credit bureau may only supply identifying information such as names and addresses to non credit granting, government agencies unless otherwise provided.
- N.M. STAT. ANN. § 56-3-4 (2008) In dealing with businesses, professions and individuals, a credit bureau shall require service contracts to be executed in which the regular subscriber or the occasional user certifies that inquiries shall be made only for the purposes of the granting of credit or other bona fide business transaction, such as evaluation of present or prospective credit risks or evaluation of the qualifications of present or prospective employees. The credit bureau shall refuse service to any prospective subscriber or user who will not so certify, and shall discontinue service to any who fails to honor the above contract provisions.
- **Financial Records**
 - N.M. STAT. ANN. § 58-1-38 (2008) Neither the commissioner [director of the financial institutions division of the regulation and licensing department], nor his deputies or employees, nor the state corporation commission [public regulation commission], nor any member thereof, nor any deputy, clerk or employee in its office shall divulge any information acquired by them in the discharge of their duties, except in so far as the same may be rendered necessary by law. The commissioner [director] may exchange information as to the conditions of banks with the United States comptroller of the currency, federal deposit insurance corporation, federal reserve banks, and banking departments of other states.
 - N.M. STAT. ANN. § 56-3A-3 (2008). Consumers may elect to put a security freeze on their consumer reports.
- **Employee Privacy**
 - N.M. STAT. ANN. § 50-11-1 through -6 (2008) - Employee Privacy Act. Deals with discrimination of smokers.
- **Electronic Surveillance**
 - N.M. STAT. ANN. § 30-12-1 (2008) Interference with communications; exception. Any sort of tampering or intercepting is a misdemeanor except if done by a common carrier or switchboard operator or one party consents to the interception.
 - N.M. STAT. ANN. § 30-12-2 (2008) Grounds for order of interception. attorney general or district attorney can apply for the interception if evidence from the interception will provide info for the crime of murder, kidnapping, extortion, robbery, trafficking or distribution of controlled substances or bribery of a witness; the crime of burglary, aggravated burglary, criminal sexual penetration, arson, mayhem, receiving stolen property or commercial gambling, if punishable by imprisonment for more than one year; or an organized criminal conspiracy to commit any of the aforementioned crimes.
 - N.M. STAT. ANN. § 30-12-3 (2008) Form of application
 - N.M. STAT. ANN. § 30-12-4 (2008) Entry of order; determination
 - N.M. STAT. ANN. § 30-12-5 (2008) Contents of order
 - N.M. STAT. ANN. § 30-12-6 (2008) Order; extension; requirements
 - N.M. STAT. ANN. § 30-12-7 (2008) Method of recording communication; custody
 - N.M. STAT. ANN. § 30-12-8 (2008) Use of contents as evidence; disclosure; motion to suppress
 - N.M. STAT. ANN. § 30-12-9 (2008) Disclosure; when and by whom allowed

- N.M. STAT. ANN. § 30-12-10 (2008) Interception of privileged or unauthorized communications. Interception doesn't allow a communication to lose its privileged character.
- N.M. STAT. ANN. § 30-12-11 (2008) Right of privacy; damages
- **Computer Statutes**
 - N.M. STAT. ANN. §30-45-1 through -7 (2008). Computer abuse. A person who knowingly, willfully and without authorization, or having obtained authorization, uses the opportunity the authorization provides for purposes to which the authorization does not extend: directly or indirectly alters, changes, damages, disrupts or destroys any computer, computer network, computer property, computer service or computer system.
- **Common Law**
 - Smith v. City of Artesia, 772 P.2d 373 (N.M. Ct. App. 1989) Accepts the four strands of the Restatement of Torts invasion of privacy.

NEW YORK PRIVACY LAW

- **State Constitutional Privacy Rights**
 - none
- **Search and Seizure**
 - N.Y. CONST. art I, § 12 Protects against unreasonable searches and seizures, and unreasonable interception of telephone and telegraph communications.
 - **Auto Exception**
 - People v. Galak, 616 N.E.2d 842 (N.Y. 1993)
 - **Open Fields**
 - People v. Reynolds, 523 N.E.2d 291 (N.Y. 1988).
 - **Plain View**
 - People v. Howard, 395 N.E.2d 291 (N.Y. App. Div. 1977).
- **Statutory Privacy Rights**
 - N.Y. CIV. RIGHTS § 50 (2009) - Right of privacy. A person, firm or corporation that uses for advertising purposes, or for the purposes of trade, the name, portrait or picture of any living person without having first obtained the written consent of such person, or if a minor of his or her parent or guardian, is guilty of a misdemeanor.
 - N.Y. GEN. BUS. § 670 through 675 (2009) - protect the personal privacy of individuals and their families who rent video cassette tapes and movies and similar audio visual materials, without unreasonably restricting the ability of video tape service providers to collect and use information as is necessary to conducting their businesses. Cannot disclose personally identifiable information about a consumer and his/her rentals unless to the consumer or by written consent.
 - N.Y. PENAL LAW §§ 120.45 through 120.55 (2009) Stalking in the fourth, third, second, and first degree is unlawful. The degree depends on injury to the victim, whether it is a repeat offense and whether the person was carrying a weapon while stalking.
 - N.Y. GEN. BUS. § 390-b (2009) - NY Anti-phishing Act of 2006. It is unlawful for any person, by means of a web page, electronic [fig 1] message, or [fig 2] other use of the internet [fig 3] to solicit, request [fig 4] or [fig 5] collect identifying information by deceptively representing [fig 6] himself or herself, either directly or by implication, to be a business or a governmental entity and doing so without the authority or approval of such business or such governmental entity
- **Public Records**
 - N.Y. PUB. OFF. LAW §§ 84 (2009) - Freedom of Information Act. Declares that government is a public business and the public should have access to the records.
 - N.Y. PUB. OFF. LAW §§ 91 through 94 (2009) Personal Privacy Protection Law. Each agency that maintains a system of records shall: (a) except when a data subject provides an agency with unsolicited personal information, maintain in its records only such personal information which is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or executive order, or to implement a program specifically authorized by law; (b) consistent with the standards of paragraph (a) of this subdivision, maintain all records used by the agency to make any determination about any data subject with accuracy, relevance, timeliness and completeness provided, however, that

personal information or records received by an agency from another governmental unit for inclusion in public safety agency records shall be presumed to be accurate; (c) collect personal information directly from the data subject whenever practicable, except when collected for the purpose of making quasi-judicial determinations; (d) provide each data subject whom it requests to supply information to be maintained in a record, at the time of the initial request, with notification as provided in this paragraph. Where such notification has been provided, subsequent requests for information from the data subject to be maintained in the same record need not be accompanied by notification unless the initial notification is not applicable to the subsequent request.

- No agency may disclose any record or personal information unless such disclosure is: (a) pursuant to a written request by or the voluntary written consent of the data subject, provided that such request or consent, by its terms, limits and specifically describes or is directed to certain enumerated official parties, including the bureau of the census, ordered by subpoena or court order, etc.
- **Motor Vehicle Records**
 - N.Y. VEH & TRAF. LAW § 202 (2009) - Sale of registration information. The Commissioner may sell registration lists as long as the purpose is not contrary to public policy. Any such sale of registration information shall be limited to only that part of the vehicle registration records describing the name and address of the owner of the vehicle and the make, model, year, weight, body style, number of passengers and cylinders, fuel, license number, type of registration and transaction, validation and expiration date and vehicle identification number of the vehicle. Also the individual registrants will be notified.
- **Vehicle Identification Numbers**
 - People v. Class, 494 N.E.2d 444 (N.Y. 1986) - Despite the Supreme Court of the United States reversal [New York v. Class, 475 U.S. 106 (1986)], on remand the NY Court of Appeals still found the officer's search of the VIN number located inside the car an illegal search. Where, as here, we have already held that the State Constitution has been violated; we should not reach a different result following reversal on Federal constitutional grounds unless respondent demonstrates that there are extraordinary or compelling circumstances. That showing has not been made.
- **Consumer Credit**
 - N.Y. GEN. BUS. LAW § 380 through § 380-u (2009) - Fair Credit Reporting Act.
 - § 380-b. Permissible dissemination of reports
 - § 380-d. Disclosure to consumers
 - § 380-e. Methods and conditions of disclosure to consumers
 - § 380-g. Public record information. At the time such public record information is reported to the user of such consumer report, notify the consumer of the fact that public record information is being reported by the consumer reporting agency, together with the name and address of the person to whom such information is being reported; or (b) maintain reasonable procedures designed to ensure that whenever public record information is reported it is complete and up to date to the extent practicable. It shall be deemed a reasonable procedure for a consumer

reporting agency to accurately report the status of public record information as of the date recorded in its files provided such information is updated on a regular basis.

- § 380-h. Restrictions on investigative consumer reports
- § 380-i. Requirements on users of consumer reports
- § 380-j. Prohibited information No consumer reporting agency shall report or maintain in the file on a consumer, information: (1) relative to an arrest or a criminal charge unless there has been a criminal conviction for such offense, or unless such charges are still pending, (2) relative to a consumer's race, religion, color, ancestry or ethnic origin, or (3) which it has reason to know is inaccurate.
- § 380-p. Unauthorized disclosures by officers or employees; penalty. Any officer or employee of a consumer reporting agency who knowingly and willfully provides information concerning an individual from the agency's files to a person not authorized to receive that information shall, upon conviction, be fined not more than five thousand dollars or imprisoned not more than one year, or both.
- § 380-q. Disclosure of medical information Whenever any provision of this article requires disclosure of medical information, or the disclosure of a reason for adverse action which involves medical information, such information or reason shall be disclosed only to a physician designated by the consumer for such purpose.
- § 380-r. Disclosures to governmental agencies. Notwithstanding the provision of section three hundred eighty-b of this article, a consumer reporting agency may furnish identifying information respecting any consumer, limited to his name, address, former addresses, places of employment, or former places of employment to a governmental agency.
- N.Y. GEN. BUS. LAW § 380-s (2009). Theft of identity. No person, firm, partnership, corporation, or association or employee thereof shall knowingly and with the intent to defraud, obtain, possess, transfer, use, or attempt to obtain, possess, transfer, or use credit, goods, services or anything else of value in the name of another person without his or her consent.
- N.Y. GEN. BUS. LAW § 380-t (2009). Security freeze. Consumers may request a security freeze on their consumer credit report.
- N.Y. GEN. BUS. LAW § 899-aa (2009), Notification of Security breach.
 - Any person or business which conducts business in New York state, and which owns or licenses computerized data which includes private information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the system to any resident of New York state whose private information was, or is reasonably believed to have been, acquired by a person without valid authorization. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision four of this section, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system.

- "Personal information" shall mean any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person;
 - (b) "Private information" shall mean personal information consisting of any information in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted, or encrypted with an encryption key that has also been acquired: (1) Social Security number; (2) driver's license number or non-driver identification card number; or (3) account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account;
 - "Private information" does not include publicly available information which is lawfully made available to the general public from federal, state, or local government records.
 - N.Y. GEN. BUS. LAW § 399-h (2009) Disposal of records containing personal identifying information. [fig 1] No person, business, firm, partnership, association, or corporation [fig 2], not including the state or its political subdivisions, shall dispose of a record containing personal identifying information unless the person, business, firm, partnership, association, or corporation, [fig 3] or other person under contract with the business, firm, partnership, association, or corporation [fig 4] does any of the following: a. shreds the record before the disposal of the record; or b. destroys the personal identifying information contained in the record; or c. modifies the record to make the personal identifying information unreadable; or d. takes actions consistent with commonly accepted industry practices that it reasonably believes will ensure that no unauthorized person will have access to the personal identifying information contained in the record.
- **Financial Records**
 - N.Y. BANKING LAW § 36 (2009) Right of Inspection of the Superintendent of Banks. The superintendent shall also have power at any time to examine every agency [fig 1], branch or office located in this state of any foreign banking corporation, including, but not limited to, all of the books, accounts or records of every agency, branch or office located in this state of such foreign banking corporation as well as all of the books, accounts or records maintained in this state of any agency, branch or office not located in this state of such foreign banking corporation for the purpose of ascertaining whether it has violated any law and for any other purpose.
 - The superintendent shall have the power to make such special investigations as he shall deem necessary to determine whether any individual, partnership, unincorporated association or corporation has violated any of the provisions of this chapter; and to the extent necessary for this purpose the superintendent shall have the power to examine all relevant books, records, accounts and documents.
 - **Employee Privacy**

- N.Y. LAB. LAW § 804 (2009) - Final reports of board of inquiries regarding labor disputes are public, however any information other than that having a direct bearing on the dispute obtained about any labor union or individual business of a person, firm or corporation must be excluded. Certain exceptions apply.
- **Electronic Surveillance**
 - N.Y.C.P.L.R. 4506 (2009) Eavesdropping evidence; admissibility; motion to suppress in certain cases. Not allowed to admit evidence obtained in contravention to the law.
 - N.Y. CRIM. PROC. LAW § 700.05 (2009) Eavesdropping and video surveillance warrants; definitions of terms
 - N.Y. CRIM. PROC. LAW § 700.10 (2009) Eavesdropping and video surveillance warrants; in general. Not issued for a period longer than is necessary to achieve the objective of the authorization, or in any event longer than thirty days.
 - N.Y. CRIM. PROC. LAW § 700.15 (2009) Eavesdropping and video surveillance warrants; when issuable. Requires probable cause that the person will commit a designated offense and that other investigation techniques have failed.
 - N.Y. CRIM. PROC. LAW § 700.20 (2009) Eavesdropping and video surveillance warrants; application
 - N.Y. CRIM. PROC. LAW § 700.21 (2009) Temporary authorization for eavesdropping or video surveillance in emergency situations
 - N.Y. CRIM. PROC. LAW § 700.25 (2009) Eavesdropping warrants; determination of application
 - N.Y. CRIM. PROC. LAW § 700.30 (2009) Eavesdropping and video surveillance warrants; form and content
 - N.Y. CRIM. PROC. LAW § 700.35 (2009) Eavesdropping and video surveillance warrants; manner and time of execution
 - N.Y. CRIM. PROC. LAW § 700.40 (2009) Eavesdropping and video surveillance warrants; order of extension
 - N.Y. CRIM. PROC. LAW § 700.50 (2009) Eavesdropping and video surveillance warrants; progress reports and notice. Within a reasonable time, but in no case later than ninety days after termination of an eavesdropping or video surveillance warrant, or expiration of an extension order, except as otherwise provided in subdivision four, written notice of the fact and date of the issuance of the eavesdropping or video surveillance warrant was issued.
 - N.Y. PENAL LAW § 250.00 (2009) Eavesdropping; definitions of terms. "Electronic communication" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photo-optical system, but does not include: (a) any telephonic or telegraphic communication; or (b) any communication made through a tone only paging device; or (c) any communication made through a tracking device consisting of an electronic or mechanical device which permits the tracking of the movement of a person or object; or (d) any communication that is disseminated by the sender through a method of transmission that is configured so that such communication is readily accessible to the general public.

- N.Y. PENAL LAW § 250.05 (2009) Eavesdropping. A person is guilty of eavesdropping when he unlawfully engages in wiretapping, mechanical overhearing of a conversation, or intercepting or accessing of an electronic communication.
- N.Y. PENAL LAW § 250.10 (2009) Possession of eavesdropping devices
- N.Y. PENAL LAW § 250.15 (2009) Failure to report wiretapping
- N.Y. PENAL LAW § 250.20 (2009) Divulging an eavesdropping warrant is prohibited.
- N.Y. PENAL LAW § 250.25 (2009) Tampering with private communications. Opening a letter or other communication, holding oneself out as an agent of the intended recipient without consent.
- N.Y. PENAL LAW § 250.30 (2009) Unlawfully obtaining communications information
- N.Y. PENAL LAW § 250.35 (2009) Failing to report criminal communications
- N.Y. PENAL LAW § 250.40 (2009) Unlawful surveillance; definitions
- N.Y. PENAL LAW § 250.45 (2009) Unlawful surveillance in the second degree. Installs a recording device for the purpose of viewing another in an intimate way without their consent.
- N.Y. PENAL LAW § 250.50 (2009) Unlawful surveillance in the first degree
- N.Y. PENAL LAW § 250.65 (2009) These provisions don't apply to law enforcement or video surveillance set up for the purpose of security that is conspicuously posted.
- **Computer Statutes**
 - N.Y. PENAL LAW § 156.05 through 156.50 (2009) Unauthorized use of a computer. A person is guilty of unauthorized use of a computer when he or she knowingly uses [fig 1], causes to be used, or accesses a computer [fig 2], computer service, or computer network without authorization [fig 3].
 - Computer Trespass. Accesses the computer and tries to commit a felony.
 - Computer Tampering, fourth, third, second, first degree. Intentionally alters or destroys a computer.
 - Unlawful duplication of computer material, fourth, third, second, first degree. Copies, reproduces or duplicates in any manner any computer data or computer program and thereby intentionally and wrongfully deprives or appropriates from an owner thereof an economic value. Or uses a computer in the commission of a felony.
 - Criminal possession of a computer. Having no right to do so, he knowingly possesses, in any form, any copy, reproduction or duplicate of any computer data or computer program which was copied, reproduced or duplicated in violation of section 156.30 of this article, with intent to benefit himself or a person other than an owner thereof.
- **Common Law**
 - Messenger v. Gruner + Jahr Printing & Publ'g, 727 N.E.2d 549 (N.Y. 2000) New York does not recognize a common law right of privacy. N.Y. Civ. Rights Law §§ 50, 51 provide a limited statutory right of privacy.

NORTH CAROLINA PRIVACY LAW

- **State Constitutional Privacy Rights**
 - none
- **Search and Seizure**
 - N.C. Const. art. I, § 20 Prohibits general warrants to search without evidence of the act committed. Prohibits seizing any person not named.
 - **Auto Exception**
 - State v. Isleib, 356 S.E.2d 573 (N.C. 1987)
 - **Open Fields**
 - State v. Burch, 320 S.E.2d 28 (N.C. Ct. App. 1984).
 - **Plain View**
 - State v. Blackwelder, 238 S.E.2d 190 (N.C. Ct. App. 1977).
- **Statutory Privacy Rights**
 - N.C. GEN. STAT. ANN. § 14-277.3A (2009) Stalking. Therefore, the General Assembly enacts this law to encourage effective intervention by the criminal justice system before stalking escalates into behavior that has serious or lethal consequences. A defendant is guilty of stalking if the defendant willfully on more than one occasion harasses another person without legal purpose or willfully engages in a course of conduct directed at a specific person without legal purpose and the defendant knows or should know that the harassment or the course of conduct would cause a reasonable person to do any of the following: (1) Fear for the person's safety or the safety of the person's immediate family or close personal associates. (2) Suffer substantial emotional distress by placing that person in fear of death, bodily injury, or continued harassment.
- **Individually Identifiable Government Records**
 - N.C. GEN. STAT. ANN. § 58-39-1 through -76 (2009) - Insurance Information and Privacy Protection Act.
 - § 58-39-26. Federal privacy disclosure notice requirements.
 - § 58-39-27. Privacy notice and disclosure requirement exceptions.
 - § 58-39-45. Access to recorded personal information. Any individual, after proper identification, submits a written request to an insurance institution, agent, or insurance-support organization for access to recorded personal information about the individual that is reasonably described by the individual and reasonably locatable and retrievable by the insurance institution, agent, or insurance-support organization, the insurance institution, agent, or insurance-support organization if in writing.
 - § 58-39-55. Reasons for adverse underwriting decisions
 - § 58-39-75. Disclosure limitations and conditions An insurance institution, agent, or insurance-support organization shall not disclose any personal or privileged information about an individual collected or received in connection with an insurance transaction unless the disclosure is with the written consent of the individual and other such requirements
 - § 58-39-76. Limits on sharing account number information for marketing purposes. An insurance institution, insurance agent, or insurance-support organization shall not disclose, other than to a consumer reporting agency, an account number or similar form of access number or access code for a

- credit card account, deposit account, or transaction account of a consumer to any nonaffiliated third party for use in telemarketing, direct mail marketing, or other marketing through electronic mail to the consumer.
- N.C. GEN. STAT. ANN. § 58-39-130 through -165 (2009) Customer Information Safeguards Protection Act. Establish standards for developing and implementing administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information. Also to provide privacy and security protection consistent with federal regulations governing the privacy and security of medical records when this Part is consistent with those federal regulations. In those instances in which this Part and the federal regulations are inconsistent and this Part provides privacy and security protection beyond that offered by the federal regulations, the purpose of this Part is to provide that additional privacy and security protection.
 - § 58-39-145. Information security program. Each licensee shall implement a comprehensive written information security program that includes administrative, technical, and physical safeguards for the protection of customer information. The administrative, technical, and physical safeguards included in the information security program shall be appropriate to the size and complexity of the licensee and the nature and scope of its activities.
 - § 58-39-150. Objectives of information security program. Licensee's information security program shall be designed to: (1) Ensure the security and confidentiality of customer information; (2) Protect against any anticipated threats or hazards to the security or integrity of the information; and (3) Protect against unauthorized access to or use of the information that could result in substantial harm or inconvenience to any customer.
 - N.C. GEN. STAT. ANN. § 75-64 (2009). Destruction of personal information records. Any business that conducts business in North Carolina and any business that maintains or otherwise possesses personal information of a resident of North Carolina must take reasonable measures to protect against unauthorized access to or use of the information in connection with or after its disposal.
 - N.C. GEN. STAT. ANN. § 75-62 (2009). Must redact SSN from publicly displayed documents and if an SSN is requested online, the information must be encrypted and the site secure.
 - N.C. GEN. STAT. ANN. § 75-65 (2009). Protection from security breaches. Any business that owns or licenses personal information of residents of North Carolina or any business that conducts business in North Carolina that owns or licenses personal information in any form (whether computerized, paper, or otherwise) shall provide notice to the affected person that there has been a security breach following discovery or notification of the breach. The disclosure notification shall be made without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection (c) of this section, and consistent with any measures necessary to determine sufficient contact information, determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system. For the purposes of this section, personal

information shall not include electronic identification numbers, electronic mail names or addresses, Internet account numbers, Internet identification names, parent's legal surname prior to marriage, or a password unless this information would permit access to a person's financial account or resources.

- **Public Records**

- N.C. GEN. STAT. ANN. § 115C-319 (2009) - personnel files of employees of local boards of education are not subject to inspection
- N.C. GEN. STAT. ANN. § 115C-320 (2009) - local boards of education must keep records on their employees that will be open to public inspection and include name, age and salary.
- N.C. GEN. STAT. ANN. § 153A-98 (2009) - personnel files of county employees are not subject to inspection but information such as name, age, current position and salary is a public record.
- N.C. GEN. STAT. ANN. § 132-1 (2009) - The public records and public information compiled by the agencies of North Carolina government or its subdivisions are the property of the people. Therefore, it is the policy of this State that the people may obtain copies of their public records and public information free or at minimal cost unless otherwise specifically provided by law. As used herein, "minimal cost" shall mean the actual cost of reproducing the public record or public information.
- N.C. GEN. STAT. ANN. § 132-1.1 through -1.12 (2009) lists confidential records not available for inspection. These include sensitive security information, autopsy photos, personally identifying information including SSNs, trade secrets, passwords, etc.
- N.C. GEN. STAT. § 132-10 (2009) Geographical information systems databases and data files developed and operated by counties and cities are public records within the meaning of this Chapter. The county or city shall provide public access to such systems by public access terminals or other output devices. Upon request, the county or city shall furnish copies, in documentary or electronic form, to anyone requesting them at reasonable cost.

- **Motor Vehicle Records**

- N.C. GEN. STAT. § 20-43.1 (2009) - Division may disclose personal information to federally designated organ procurement organizations and eye banks operating in this State for the purpose of identifying individuals who have indicated an intent to be an organ donor. Personal information authorized under this subsection is limited to the individual's first, middle, and last name, date of birth, address, sex, county of residence, and driver's license number. Employees of the Division who provide access to or disclosure of information in good-faith compliance with this subsection are not liable in damages for access to or disclosure of the information.
 - The Division shall disclose personal information contained in motor vehicle records in accordance with the federal Driver's Privacy Protection Act of 1994
- Motor Vehicle Accident Reports are public records, but should be released only after the Division of Motor Vehicles has redacted personal identifying information in accordance with the federal Drivers Privacy Protection Act. See

opinion of Attorney General to Mr. George Tatum, Commissioner, North Carolina Division of Motor Vehicles, 2005 N.C. AG LEXIS 1 (2/9/05).

- **Vehicle Identification Numbers**

- N.C. GEN. STAT. § 20-108 (2009) (a) Any person who knowingly buys, receives, disposes of, sells, offers for sale, conceals, or has in his possession any motor vehicle, or engine or transmission or component part which has been stolen or removed from a motor vehicle and from which the manufacturer's serial or engine number or other distinguishing number or identification mark or number placed thereon under assignment from the Division has been removed, defaced, covered, altered, or destroyed for the purpose of concealing or misrepresenting the identity of said motor vehicle or engine or transmission or component part is guilty of a Class 2 misdemeanor.
- (b) The Commissioner and such officers and inspectors of the Division of Motor Vehicles as he has designated may take and possess any motor vehicle or component part if its engine number, vehicle identification number, or manufacturer's serial number has been altered, changed, or obliterated or if such officer has probable cause to believe that the driver or person in charge of the motor vehicle or component part has violated subsection (a) above.

- **Consumer Credit**

- N.C. GEN. STAT. ANN. § 58-39-40 (2009). Investigative consumer reports. No insurance institution, agent, or insurance-support organization may prepare or request an investigative consumer report about an individual in connection with an insurance transaction involving an application for insurance, a policy renewal, a policy reinstatement, or a change in insurance benefits unless the insurance institution or agent informs the individual: (1) That he may request to be interviewed in connection with the preparation of the investigative consumer report; and (2) That upon a request pursuant to G.S. 58-39-45 he is entitled to receive a copy of the investigative consumer report.
- N.C. Gen. Stat. § 75-63 (2009). Permits consumers to request a security freeze on their consumer report.

- **Financial Records**

- N.C. GEN. STAT. ANN. § 53B-1 through -10 (2009) Financial Privacy Act.
 - § 53B-3 (2009) - It is the policy of the state that financial records are confidential and financial institutions may not provide such records to government authorities except as provided in this chapter.
 - § 53B-4 (2009) Provisions under which government authorities may have access to a customer's financial records including pursuant to customer authorization, search warrant, subpoena or court order.
 - § 53B-8 (2009). Disclosure of financial records - No financial institution or its officer, employee, or agent may disclose a customer's financial record to a government authority except as provided in this Chapter. This section does not prohibit a financial institution from giving notice of or disclosing the name, address, and existence of an account to a government authority that makes a written statement for requesting that record.

- **Employee Privacy**

- N.C. GEN. STAT. ANN. § 95-232 (2009) - permits employee drug testing, but does not specifically require results be kept confidential or not be entered into evidence.
- **Electronic Surveillance**
 - N.C. GEN. STAT. ANN. § 14-155 (2009) - Unauthorized connections with telephone or telegraph. It shall be unlawful for any person to tap or make any connection with any wire or apparatus of any telephone or telegraph company operating in this State, except such connection as may be authorized by the person or corporation operating such wire or apparatus. Any person violating this section shall be guilty of a Class 3 misdemeanor. Each day's continuance of such unlawful connection shall be a separate offense. No connection approved by the Federal Communications Commission or the North Carolina Utilities Commission shall be a violation of this section.
 - N.C. GEN. STAT. ANN. § 15A-286 (2009) Definitions. "Electronic communication" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate or foreign commerce but does not include: a. Any wire or oral communication; b. Any communication made through a tone-only paging device; or c. Any communication from a tracking device (as defined in section 3117 of Title 18 of the United States Code).
 - N.C. GEN. STAT. ANN. § 15A-287 (2009) Interception and disclosure of wire, oral, or electronic communications prohibited. Exceptions for common carriers, public frequencies, law enforcement, or with the consent of one party.
 - N.C. GEN. STAT. ANN. § 15A-288 Manufacture, distribution, possession, and advertising of wire, oral, or electronic communication intercepting devices prohibited.
 - N.C. GEN. STAT. ANN. § 15A-289 Confiscation of wire, oral, or electronic communication interception devices.
 - N.C. GEN. STAT. ANN. § 15A-290 Offenses for which orders for electronic surveillance may be granted. Drug trafficking, continuing criminal enterprise, murder, kidnapping, hostage taking, robbery, extortion, bribery, rape, or any sexual offense, or when the interception may expedite the apprehension of persons indicted for the commission of these offenses.
 - N.C. GEN. STAT. ANN. § 15A-291 Application for electronic surveillance order; judicial review panel
 - N.C. GEN. STAT. ANN. § 15A-292 Request for application for electronic surveillance order
 - N.C. GEN. STAT. ANN. § 15A-293 Issuance of order for electronic surveillance; procedures for implementation.
 - N.C. GEN. STAT. ANN. § 15A-294 Authorization for disclosure and use of intercepted wire, oral, or electronic communications. Not for longer than 30 days, there must be probable cause that the person is committing the offense.
 - N.C. GEN. STAT. ANN. § 15A-295 Reports concerning intercepted wire, oral, or electronic communications. In January of each year, the Attorney General of this State must report to the Administrative Office of the United States Court the

information required to be filed by section 2519 of Title 18 of the United States Code, as heretofore or hereafter amended, and file a copy of the report with the Administrative Office of the Courts of North Carolina.

- **Computer Statutes**

- N.C. GEN. STAT. ANN. § 14-451 through -458 (2009) Computer Related Crime
 - § 14-454. Accessing computers. Unlawful to access or cause access to a computer, system or network for the purpose of devising a scheme to defraud or to obtain property of services. Exceptions Apply.
 - § 14-454.1. Accessing government computers
 - § 14-455. Damaging computers, computer programs, computer systems, computer networks, and resources
 - § 14-456. Denial of computer services to an authorized user
 - § 14-456.1. Denial of government computer services to an authorized user
 - § 14-457. Extortion
 - § 14-458. Computer trespass; penalty

- **Common Law**

- Hall v. Post, 372 S.E.2d 711 (N.C. 1988) Accepts appropriation and intrusion strands of the invasion of privacy. Rejects false light and public disclosure.

NORTH DAKOTA PRIVACY LAW

- **State Constitutional Privacy Rights**
 - none
- **Search and Seizure**
 - N.D. CONST. art I, § 8 - protects against unreasonable search and seizure.
 - **Auto Exception**
 - State v. Washington, 737 N.W.2d 382 (N.D. 2007)
 - **Open Fields**
 - State v. Washington, 343 N.W.2d 361 (N.D. 1984)
 - **Plain View**
 - State v. Gronlund, 356 N.W.2d 144 (N.D. 1984)
- **Statutory Privacy Rights**
 - N.D. CENT. CODE § 12.1-17-07.1 (2009) - "Stalk" means to engage in an intentional course of conduct directed at a specific person which frightens, intimidates, or harasses that person, and that serves no legitimate purpose. The course of conduct may be directed toward that person or a member of that person's immediate family and must cause a reasonable person to experience fear, intimidation, or harassment. No person may intentionally stalk another person.
 - N.D. CENT. CODE § 14-02-01 (2009) - General personal rights. Every person, subject to the qualifications and restrictions provided by law, has the right of protection from bodily restraint or harm, from personal insult, from defamation, and from injury to the person's personal relations.
 - N.D. CENT. CODE § 8-10-09 (2009) - Disclosing telegraph and telephone messages. Every person who willfully obtains any knowledge of a telegraphic or telephonic message, by connivance with a clerk, operator, messenger, or other employee of a telegraph or telephone company, and every clerk, operator, messenger, or other employee who willfully divulges to any but the person for whom it was intended, the contents of any telephonic or telegraphic message entrusted to that person for transmission or delivery, or the nature thereof, or who willfully refuses or fails to duly transmit or deliver any such message, is guilty of a class A misdemeanor.
 - N.D. CENT. CODE § 11-18-23 (2009). Social Security Number Protection. Filing or recording documents with recorder -- Social Security numbers. 1. A document that includes a Social Security number may not be filed or recorded with the recorder unless a law requires the Social Security number to be in the document in order to be filed or recorded. A document that is required to contain a social security number may be recorded in the real estate records with the Social Security number redacted. 2. Notwithstanding any other provision of law, when a copy of a document that includes a Social Security number is requested, the recorder is not required to redact the Social Security number unless the document was filed or recorded with the recorder after December 1, 2003.
- **Public Records**
 - N.D. CENT. CODE § 44-04-18 (2009) - Except as otherwise specifically provided by law, all records of a public entity are public records, open and accessible for inspection during reasonable office hours.

- N.D. CENT. CODE § 44-04-18.1 through -31 (2009) - lists the exceptions to the public record disclosure rules. For example, public employee personal, medical and assistance records are confidential, medical records email addresses, personal and financial information in a customer complaint, etc.
- N.D. CENT. CODE § 37-18-11(2009) - records and papers regarding veterans must be kept in a manner to best service the public interest while respecting the veterans' right of privacy.
- N.D. CENT. CODE § 65-05-32 (2009) - workers compensation hearing information is confidential.
- **Motor Vehicle Records**
 - N.D. CENT. CODE § 39-02-05 (2009) Except as provided by chapter 39-33, all registration and license records in the office of the department must be public records and must be open to inspection by the public during business hours.
 - "Motor vehicle record" means any record that pertains to a motor vehicle operator's license or permit, motor vehicle registration, motor vehicle title, or identification document issued by the department, or other state or local agency authorized to issue any of such forms of credentials. A record includes all books, papers, photographs, photostats, cards, films, tapes, recordings, electronic data, printouts, or other documentary materials regardless of physical form or characteristics.
 - N.D. CENT. CODE § 39-33-02 (2009). Disclosure and use of personal information from department records prohibited. Notwithstanding any other provision of law, the department may not knowingly disclose personal information about any person obtained by the department in connection with a motor vehicle record.
 - N.D. CENT. CODE § 39-33-08 (2009). Resale or redisclosure. 1. An authorized recipient of personal information may resell or redisclose the information for any use permitted under section 39-33-05. 2. The department shall require any authorized recipient who resells or rediscloses personal information to maintain for a period of not less than five years records as to the person receiving the information and the permitted use for which it was obtained and to make these records available for inspection by the department upon request.
 - N.D. CENT. CODE § 24-02-11. Records of Transportation Department open to public -- Certain records not open to public. The director is custodian of, and shall preserve, the files and records of the department. The files and records of the department must be open to public inspection under reasonable regulations. However, records relating to the financial condition of any party are not open to public inspection if there is a pending bid for a government contract from the department.
- **Vehicle Identification Numbers**
 - N.D. CENT. CODE, § 12.1-23-08.1; -08.2 (2009) - illegal to remove a VIN or sell a vehicle without a VIN.
- **Consumer Credit**
 - N.D. CENT. CODE, § 51-30-02 (2009) - Security Breach Notification. Any person that conducts business in this state, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data

to any resident of the state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in section 51-30-04, or any measures necessary to determine the scope of the breach and to restore the integrity of the data system.

- N.D. CENT. CODE, § 51-33-02 (2009) - Consumers have a right to obtain a security freeze on their consumer reports
- **Financial Records**
 - N.D. CENT. CODE, § 44-04-18.4 (2009) Trade secret, proprietary, commercial, and financial information is confidential if it is of a privileged nature and it has not been previously publicly disclosed. "Financial information" means information pertaining to monetary resources of a person that has not been previously publicly disclosed and that if the information were to be disclosed would impair the public entity's future ability to obtain necessary information or would cause substantial competitive injury to the person from which the information was obtained.
 - N.D. CENT. CODE 44-04-18.17 (2009). Personal and financial information in a consumer complaint. Personal and financial information submitted to a state agency as part of a consumer complaint, or gathered pursuant to an investigation of a consumer complaint, is an exempt record as defined in subsection 5 of section 44-04-17.1.
 - For purposes of this section, "personal and financial information" means the home address, home telephone number, Social Security number, consumer report, and credit, debit, or electronic fund transfer card number of the complainant and any person on whose behalf the complaint is made, and any account number of a business or individual at a bank, brokerage, or other financial institution.
 - "Personal and financial information" does not include the nature of the complaint, name of the complainant or any person on whose behalf the complaint was submitted, or the address or telephone number of the business that is the subject of the complaint.
 - N.D. CENT. CODE § 6-01-07 (2009) - records of state banking boards are open. Certain limitations regarding personal information apply.
 - N.D. CENT. CODE § 6-01-07.1 (2009) records obtained by the department of banking during examination of a financial institution are confidential.
 - N.D. CENT. CODE 6-08.1-03 (2009). Duty of confidentiality. A financial institution may not disclose customer information to any person, governmental agency, or law enforcement agency unless the disclosure is made in accordance with any of the following: 1. Pursuant to consent granted by the customer in accordance with this chapter. 2. To a person other than a governmental agency or law enforcement agency pursuant to valid legal process. 3. To a governmental agency or law enforcement agency pursuant to valid legal process in accordance with this chapter. 4. For the purpose of reporting a suspected violation of the law in accordance with this chapter. 5. For the purpose of notifying the agriculture commissioner that a financial institution has notified a customer of the availability of the North Dakota agricultural mediation service. 6. As part of the disclosure

made of deposits of public corporations with financial institutions in the security pledge.

- **Employee Privacy**

- N.D. CENT. CODE, § 34-01-15 (2009) - permits employers to require drug testing if the employer covers the costs. No information on whether the results would be confidential.

- **Electronic Surveillance**

- N.D. CENT. CODE § 12.1-15-02 (2009) Interception of wire or oral communications -- Eavesdropping. Guilty of a felony if intentionally intercepts, endeavors to intercept, or discloses any wire or oral communication by use of any electronic, mechanical, or other device. Also can't loiter about with the intent to hear conversations. Exceptions for acting under the law, consented, or were a party to the communication.
- N.D. CENT. CODE § 29-29.2-01 (2009) Definitions. "Electronic communication" means transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photo-optical system, but does not include: a. The radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit; b. A wire or oral communication; c. A communication made through a tone-only paging device; or d. A communication from a tracking device, defined as an electronic or mechanical device that permits the tracing of the movement of a person or object.
- N.D. CENT. CODE § 29-29.2-02 (2009) Ex parte order for wiretapping and eavesdropping. An ex parte order for wiretapping or eavesdropping, or both, may be issued by any judge of competent jurisdiction. The order may be issued upon application of the attorney general, or an assistant attorney general, or a state's attorney, or an assistant state's attorney, showing by affidavit that there is probable cause to believe that evidence will be obtained of the commission or attempted commission of a felony violation of chapter 19-03.1 [Uniform Controlled Substances Act]
- N.D. CENT. CODE § 29-29.2-03 (2009) Order may direct others to furnish assistance
- N.D. CENT. CODE § 29-29.2-04 (2009) Reports to attorney general. A state's attorney shall report annually to the attorney general information as to the number of applications made for orders permitting the interception of wire, electronic, or oral communications; the offense specified in the order or application.
- N.D. CENT. CODE § 29-29.2-05 (2009) Inapplicability. If given prior consent or working with law enforcement under the color of law.
- N.D. CENT. CODE § 29-29.3-01 (2009) Definitions. Pen Registers and Trap/Trace Devices. "Electronic communication" means transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photo-optical system. The term does not include the radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit, a wire or oral communication, a communication made through a tone-only paging device, or a communication from a tracking device.

- N.D. CENT. CODE § 29-29.3-02 (2009) Prohibition on pen register and trap and trace device use--Exception
- N.D. CENT. CODE § 29-29.3-03 (2009) Application for an order for a pen register or a trap and trace device
- N.D. CENT. CODE § 29-29.3-04 (2009) Issuance of an order for a pen register or a trap and trace device--Notice
- N.D. CENT. CODE § 29-29.3-05 (2009) Assistance in installation and use of a pen register or a trap and trace device
- **Computer Statutes**
- N.D. CENT. CODE § 12.1-06.1-08 (2009). Computer fraud -- Computer crime -- Classification
 - A person commits computer fraud by gaining or attempting to gain access to, altering, damaging, modifying, copying, disclosing, taking possession of, or destroying any computer, computer system, computer network, or any part of the computer, system, or network, without authorization, and with the intent to devise or execute any scheme or artifice to defraud, deceive, prevent the authorized use of, or control property or services by means of false or fraudulent pretenses, representations, or promises.
 - A person commits computer crime by intentionally and either in excess of authorization given or without authorization gaining or attempting to gain access to, altering, damaging, modifying, copying, disclosing, taking possession of, introducing a computer contaminant into, destroying, or preventing the authorized use of any computer, computer system, or computer network, or any computer software, program, or data contained in the computer, computer system, or computer network.
- **Common Law**
 - Hougum v. Valley Mem. Homes, 574 N.W.2d 812 (N.D. 1998) - This Court has not decided whether a tort action exists in North Dakota for invasion of privacy. See American Mut. Life Ins. Co. v. Jordan, 315 N.W.2d 290, 295-96 (N.D. 1982); City of Grand Forks v. Grand Forks Herald, Inc., 307 N.W.2d 572, 578 n.3 (N.D. 1981); Volk v. Auto-Dine Corp., 177 N.W.2d 525, 529 (N.D. 1970); See also Nelson v. J.C. Penney Co., Inc., 70 F.3d 962, 967 [***8] (8th Cir. 1995) rehearing and suggestion for rehearing en banc denied, 75 F.3d 343, 347 (8th Cir. 1996). Claims for invasion of privacy are recognized in some form in virtually all jurisdictions.
 - Unclear whether N.D. would recognize a claim under the invasion privacy under any of the strands of common law as listed in the Restatement.
 - The court evaluated Hougum's claims arguendo, and determined that he didn't even meet the requirements of the common law, so the court wouldn't have to decide the issue.

OHIO PRIVACY LAW

- **State Constitutional Privacy Rights**
 - none
- **Search and Seizure**
 - OHIO CONST. art. I, § 14 - protects against unreasonable search and seizure.
 - State v. Brown, 484 N.E.2d 215 (Ohio Ct. App. 1984) - no reasonable expectation of privacy exists as to trash placed for collection.
 - **Auto Exception**
 - State v. Moore, 734 N.E.2d 804 (Ohio 2000)
 - **Open Fields**
 - State v. Paxton, 615 N.E.2d 1086 (Ohio Ct. App. 1992).
 - **Plain View**
 - State v. Williams, 377 N.E.2d 1013 (Ohio 1978).
- **Statutory Privacy Rights**
 - OHIO REV. CODE ANN. § 1347.01 through .99 (2009) - Personal Information Systems Act. Outlines the use and disclosure of personal information by government agencies. Gives rights of disclosure to the named person, and a cause of action for wrongly disclosed information. State agencies are to have rules to prevent the disclosure of personal information and must notify persons if their information is disclosed. There are some exceptions for criminal investigations.
 - OHIO REV. CODE ANN. § 2903.211 (2009) - Menacing by stalking is prohibited. No person by engaging in a pattern of conduct shall knowingly cause another person to believe that the offender will cause physical harm to the other person or cause mental distress to the other person. No person, through the use of any electronic method of remotely transferring information, including, but not limited to, any computer, computer network, computer program, or computer system, shall post a message with purpose to urge or incite another to commit a violation of division (A)(1) of this section.
 - OHIO REV. CODE ANN. § 2913.49 (2009). Identity fraud. As used in this section, "personal identifying information" includes, but is not limited to, the following: the name, address, telephone number, driver's license, driver's license number, commercial driver's license, commercial driver's license number, state identification card, state identification card number, Social Security card, Social Security number, birth certificate, place of employment, employee identification number, mother's maiden name, demand deposit account number, savings account number, money market account number, mutual fund account number, other financial account number, personal identification number, password, or credit card number of a living or dead individual.
 - No person, without the express or implied consent of the other person, shall use, obtain, or possess any personal identifying information of another person with intent to do either of the following: (1) Hold the person out to be the other person; (2) Represent the other person's personal identifying information as the person's own personal identifying information.

- No person shall create, obtain, possess, or use the personal identifying information of any person with the intent to aid or abet another person in violating this section.
 - No person, with intent to defraud, shall permit another person to use the person's own personal identifying information.
- **Individually Identifiable Government Records**
 - OHIO REV. CODE ANN. § 1347.02 (2009) - Every state agency that collects personal information must maintain a system for management. The purpose is to develop procedures for purposes of monitoring the accuracy, relevance, timeliness, and completeness of the personal information in this system, and, in accordance with the procedures, maintain the personal information in the system with the accuracy, relevance, timeliness, and completeness that is necessary to assure fairness in any determination made with respect to a person on the basis of the information.
 - OHIO REV. CODE ANN. § 1347.02 (2009) A state or local agency shall only use the personal information in a personal information system in a manner that is consistent with the purposes of the system.
 - OHIO REV. CODE ANN. § 1347.07 (2009) - no state or agency may put personal information on an interconnected system unless it will contribute to the efficiency of the system. Cannot collect personal information unless it contributes to the lawful purpose of the agency.
 - OHIO REV. CODE ANN. § 1347.12 (2009). Disclosure or notification by state or local agency of breach of security of personal information system is required.
- **Public Records**
 - OHIO REV. CODE ANN. § 149.43 (2009). Except as provided, public records are open for inspection or copying. This section lists some exceptions including: medical records, confidential law enforcement investigatory records, information from the DNA database, financial statements and data any person submits for any purpose to the Ohio housing finance agency or the controlling board in connection with applying for, receiving, or accounting for financial assistance from the agency, and information that identifies any individual who benefits directly or indirectly from financial assistance from the agency, etc.
- **Motor Vehicle Records**
 - Beacon Journal Publishing v. Andrews, 358 N.E.2d 565 (Ohio 1993) All documents in possession of the registrar of motor vehicles, including all abstracts of records required to be received by and maintained by the registrar are public records and should be kept open at all reasonable times for public inspection.
 - OHIO REV. CODE ANN. § 4505.14 (2009) The registrar of motor vehicles, or the clerk of the court of common pleas, upon the application of any person and payment of the proper fees, may prepare and furnish lists containing title information in such form and subject to such territorial division or other classification as they may direct. The registrar or the clerk may search the records of the bureau of motor vehicles and the clerk and make reports thereof, and make copies of their title information and attestations thereof.

- OHIO REV. CODE ANN. § 4505.08 (2009) Employers and prospective employers may access the commercial driving record of employees and prospective employees.
- OHIO REV. CODE ANN. § 4501.271 (2009). Request by peace officer, correctional employee, or youth services employee for confidentiality of residence address or use of business address. A peace officer, correctional employee, or youth services employee may file a written request with the bureau of motor vehicles to do either or both of the following: (a) Prohibit disclosure of the officer's or employee's residence address as contained in motor vehicle records of the bureau; (b) Provide a business address to be displayed on the officer's or employee's driver's license or certificate of registration, or both.
- **Vehicle Identification Numbers**
 - OHIO REV. CODE ANN. § 4549.62 (2009) Unlawful to alter or conceal VIN numbers.
 - State v. Sanchez, 606 N.E.2d 1058 (Ohio App. 1992) - A deputy clerk of a municipal court cannot be prosecuted for theft in office for disclosing motor vehicle identification information obtained from an office computer to a member of the general public, since such information is a public record.
 - State v. Halczyzak, 496 N.E.2d 925 (Ohio App. 1986) - The act of viewing a VIN does not violate the Fourth Amendment so long as the VIN is in a place ordinarily in plain view from the exterior of the automobile. Under the same circumstances, a computer check of a VIN is not violative.
- **Consumer Credit**
 - OHIO REV. CODE ANN. § 3904.07 (2009) No insurance institution, agent, or insurance support organization may prepare or request an investigative consumer report about an individual in connection with an insurance transaction involving an application for insurance, a policy renewal, a policy reinstatement, or a change in insurance benefits unless the insurance institution or agent informs the individual that he may request to be interviewed in connection with the preparation of the investigative consumer report.
 - OHIO REV. CODE ANN. § 1349.17 (2009). Restrictions on recording credit card, telephone or Social Security numbers (A) No person shall record or cause to be recorded either of the following: (1) A credit card account number of the other party to a transaction, when a check, bill of exchange, or other draft is presented for payment; (2) The telephone number or social security account number of the other party to a transaction, when payment is made by credit card charge agreement, check, bill of exchange, or other draft.
 - OHIO REV. CODE ANN. § 1349.19 (2009) Any person that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system, following its discovery or notification of the breach of the security of the system, to any resident of this state whose personal information was, or reasonably is believed to have been, accessed and acquired by an unauthorized person if the access and acquisition by the unauthorized person causes or reasonably is believed will cause a material risk of identity theft or other fraud to the resident. The disclosure described in this division may be made pursuant to any provision of a contract entered into by the person with another

person prior to the date the breach of the security of the system occurred if that contract does not conflict with any provision of this section and does not waive any provision of this section. For purposes of this section, a resident of this state is an individual whose principal mailing address as reflected in the records of the person is in this state.

- OHIO REV. CODE ANN. §1349.52 (2009) - Consumer may place a security freeze on their consumer report.
- **Financial Records**
 - OHIO REV. CODE ANN. §9.02 (2009) Any party, including a governmental authority, that requires or requests a financial institution to assemble or provide a customer's financial records in connection with any investigation, action, or proceeding shall pay the financial institution for all actual and necessary costs directly incurred in searching for, reproducing, or transporting these records, if the financial institution is not a party to the investigation.
 - This section is not intended to expand, limit, or otherwise affect any authority granted under federal law or the law of this state to any party, including a governmental authority, to procure, request, or require a customer's financial records.
- **Employee Privacy**
- **Electronic Surveillance**
 - OHIO REV. CODE ANN. § 2933.51 Definitions. (2009) "Electronic communication" means a transfer of a sign, signal, writing, image, sound, datum, or intelligence of any nature that is transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photo-optical system. "Electronic communication" does not mean any of the following: (1) A wire or oral communication; (2) A communication made through a tone-only paging device; (3) A communication from an electronic or mechanical tracking device that permits the tracking of the movement of a person or object.
 - OHIO REV. CODE ANN. § 2933.52 (2009) Prohibition against interception of communications; exceptions. Intercept, attempt to intercept, procure, use or disclose or with another person to intercept or attempt to intercept a wire, oral, or electronic communication. Exceptions include common carriers, law enforcement or consent.
 - OHIO REV. CODE ANN. § 2933.521 (2009) Divulging content of communication by provider of electronic communication service
 - OHIO REV. CODE ANN. § 2933.522 (2009) Authority of judges of courts of common pleas
 - OHIO REV. CODE ANN. § 2933.53 (2009) Application for interception warrant; contents; exemptions
 - OHIO REV. CODE ANN. § 2933.54 (2009) Issuance of interception warrant; hearings. Requires probable cause for a named offense in § 2933.51 (listed by statute).
 - OHIO REV. CODE ANN. § 2933.55 (2009) Extension of interception warrant; approval of interceptions beyond scope of warrant
 - OHIO REV. CODE ANN. § 2933.56 (2009) Contents of interception warrant; sealing of records

- OHIO REV. CODE ANN. § 2933.57 (2009) Oral order for interception without warrant
- OHIO REV. CODE ANN. § 2933.58 (2009) Instruction of investigative officers; privileged communications; validity of warrant
- OHIO REV. CODE ANN. § 2933.57 (2009). Oral order for interception without warrant
- OHIO REV. CODE ANN. § 2933.58 (2009). Instructions to investigative officers; procedure for interception; territorial validity
- OHIO REV. CODE ANN. § 2933.581 (2009). Persons providing information, facilities or technical assistance to officer; prohibited disclosures; ...
- OHIO REV. CODE ANN. § 2933.59 (2009). Execution of warrant or oral order; recording or resume; termination; tampering; destruction of ...
- OHIO REV. CODE ANN. § 2933.591 (2009). Giving warning of possible surveillance
- OHIO REV. CODE ANN. § 2933.60 (2009). Reports by judges and prosecuting attorneys
- OHIO REV. CODE ANN. § 2933.61 (2009). Service of inventory on interested persons; inspection of materials. Within a reasonable time not later than ninety days after the filing of an application for an interception warrant that is denied or after the termination of the period of an interception warrant or any extensions of an interception warrant, the judge of a court of common pleas who issued the warrant or extension or denied the application shall cause to be served on the persons named in the application or the interception warrant, and on any other parties to intercepted wire, oral, or electronic communications that the judge determines in the judge's discretion should be notified in the interest of justice, an inventory
- OHIO REV. CODE ANN. § 2933.62 (2009). Conditions for receiving results in evidence or disclosure
- OHIO REV. CODE ANN. § 2933.63 (2009). Motion to suppress evidence; appeals by state
- OHIO REV. CODE ANN. § 2933.64 (2009). Training in wiretapping and electronic surveillance
- OHIO REV. CODE ANN. § 2933.65 (2009). Civil and criminal actions for violations
- OHIO REV. CODE ANN. § 2933.66 (2009). Judge to conform proceedings to constitutions
- OHIO REV. CODE ANN. § 2933.76 (2009) Order authorizing installation and use of pen register or trap and trace device
- OHIO REV. CODE ANN. § 2933.77 (2009) Assistance by provider of electronic communication service, landlord, or custodian. The provider, landlord, custodian, or other person, in accordance with the order, shall furnish the law enforcement officer or investigative officer with all information, facilities, and technical assistance necessary to accomplish the installation and operation of the pen register or trap and trace device unobtrusively
- OHIO REV. CODE ANN. § 4931.26 (2009). Divulging telegraph message. It is illegal for an employee of a messenger company to divulge the contents of a communication to an unauthorized recipient.

- OHIO REV. CODE ANN. § 4931.27 (2009). Delaying telegraph message
- OHIO REV. CODE ANN. § 4931.28 (2009). Interfering with telegraph or telephone messages. It illegal to break in or tap private telegraph or telephone communications.
- OHIO REV. CODE ANN. § 4931.29 (2009). Divulging telephone communication. No person connected with a telephone company, incorporated or unincorporated, operating a telephone line or engaged in the business of transmitting to, from, through, or in this state, telephone messages, in any capacity, shall willfully divulge a private telephone message or the nature of such message, or a private conversation between persons communicating over the wires of such company, or willfully delay the transmission of a telephonic message or communication, with intent to injure, deceive, or defraud the sender or receiver thereof or any other person, or any such telephone company, or to benefit himself or any other person.
- **Computer Statutes**
 - OHIO REV. CODE ANN. § 2913.04 (2009). Computer Crime. No person, in any manner and by any means, including, but not limited to, computer hacking, shall knowingly gain access to, attempt to gain access to, or cause access to be gained to any computer, computer system, computer network, cable service, cable system, telecommunications device, telecommunications service, or information service without the consent of, or beyond the scope of the express or implied consent of, the owner of the computer, computer system, computer network, cable service, cable system, telecommunications device, telecommunications service, or information service or other person authorized to give consent.
 - OHIO REV. CODE ANN. § 2913.421 (2009). Illegally transmitting multiple commercial electronic mail messages; unauthorized access of computer
- **Common Law**
 - **Appropriation, Intrusion, Disclosure**
 - Housh v. Peth, 133 N.E.2d 340 (Ohio 1956).
 - **False Light**
 - Welling v. Weinfeld, 866 N.E.2d 1051 (Ohio 2007).

OKLAHOMA PRIVACY LAW

- **State Constitutional Privacy Rights**
 - none
- **Search and Seizure**
 - OKLA. CONST. art. II, § 30 - protects against unreasonable search and seizure
 - **Auto Exception**
 - Gomez v. State, 168 P.3d 1139 (Okla. Crim. App. 2007).
 - **Open Fields**
 - Fite v. State, 873 P.2d 293 (Okla. Crim. App. 1993).
 - **Plain View**
 - Lyons v. State, 787 P.2d 460 (Okla. Crim. App. 1990).
- **Statutory Privacy Rights**
 - OKLA. STAT. tit. 21, § 839.1 (2008). Right of privacy--Use of name or picture for advertising without consent--Misdemeanor. Any person, firm or corporation that uses for the purpose of advertising for the sale of any goods, wares or merchandise, or for the solicitation of patronage by any business enterprise, the name, portrait or picture of any person, without having obtained, prior or subsequent to such use, the consent of such person, or, if such person is a minor, the consent of a parent or guardian, and, if such person is deceased, without the consent of the surviving spouse, personal representatives, or that of a majority of the deceased's adult heirs, is guilty of a misdemeanor.
 - OKLA. STAT. tit. 21, § 839.1A (2008). Use of name or picture of Armed Forces member for advertising without consent--Misdemeanor
 - OKLA. STAT. tit. 21, § 839.2 (2008). Right of action--Damages
 - OKLA. STAT. tit. 21, § 839.3 (2008). Right of photographer to exhibit specimens of work--Other uses excepted
 - OKLA. STAT. tit. 21, § 1171 (2008). Prohibition against peeping toms
 - OKLA. STAT. tit. 21, § 1172 (2008). Obscene, threatening or harassing telecommunication or other electronic communications--Penalty
 - OKLA. STAT. tit. 21, § 1173 (2008). Any person who willfully, maliciously, and repeatedly follows or harasses another person in a manner that: 1. Would cause a reasonable person or a member of the immediate family of that person as defined in subsection F of this section to feel frightened, intimidated, threatened, harassed, or molested; and 2. Actually causes the person being followed or harassed to feel terrorized, frightened, intimidated, threatened, harassed, or molested.
 - OKLA. STAT. tit. 15, § 776.8 (2008) - AntiPhishing Act of 2006. A person may not, with the intent to engage in conduct involving the fraudulent use or possession of the identifying information of a person: 1. Create a web page or Internet domain name that is represented as a legitimate online business without the authorization of the registered owner of the business; and 2. Use that web page or a link to the web page, that domain name, or another site on the Internet to induce, request, or solicit another person to provide identifying information for a purpose that the other person believes is legitimate.
- **Public Records**
 - OKLA. STAT. tit. 51, § 24A.1 (2008) - Oklahoma Open Records Act. The purpose of this act is to ensure and facilitate the public's right of access to and review of

government records so they may efficiently and intelligently exercise their inherent political power. The privacy interests of individuals are adequately protected in the specific exceptions to the Oklahoma Open Records Act or in the statutes which authorize, create or require the records. Except where specific state or federal statutes create a confidential privilege, persons who submit information to public bodies have no right to keep this information from public access nor reasonable expectation that this information will be kept from public access; provided, the person, agency or political subdivision shall at all times bear the burden of establishing such records are protected by such a confidential privilege.

- OKLA. STAT. tit. 51, § 24A.2 through -A.28 (2008) Exceptions to the open record rule including law enforcement records, personnel records, research records, library records.
- OKLA. STAT. tit. 74, § 840-2.11 (2008). State employee personal information-- Confidentiality. The home addresses, home telephone numbers, Social Security numbers, and information related to personal electronic communication devices of current and former state employees shall not be open to public inspection or disclosure without written permission from the current or former state employees or without an order from a court of competent jurisdiction.
- **Motor Vehicle Records**
 - OKLA. STAT. tit. 47, § 2-129 (2008). Those in custody of confidential and privileged information within this title of motor vehicles shall not disseminate this information.
 - OKLA. STAT. tit. 47, § 1109 (2008). All information contained in certificates of title, applications therefore, vehicle registration records and computer data files is hereby declared to be confidential information and shall not be copied by anyone or disclosed to anyone other than employees of the Oklahoma Tax Commission or the Corporation Commission in the regular course of their employment, except as provided in subsection B of this section. As used in this section, "personal information" means information that identifies an individual including name, address (excluding the five-digit zip code) and telephone number, but does not include information on vehicular accidents, driving violations and driver's status.
 - Personal information referred to in subsection A of this section shall be disclosed for use in connection with matters of motor vehicle or driver safety and theft, motor vehicle emissions, motor vehicle product alterations, recalls or advisories, and removal of non-owner records from the original owner records of motor vehicle manufacturers.
 - OKLA. STAT. tit. 47, § 10-115 (2008). Confidentiality of reports relating to collisions. All collision reports made by persons involved in collisions shall be without prejudice to the individual so reporting and shall be for the confidential use of the Department or other state agencies having use for the records for collision prevention purposes, or for the administration of the laws of this state relating to the deposit of security and proof of financial responsibility by persons driving or the owners of motor vehicles, except that the Department may disclose the identity of a person involved in a collision when the identity is not otherwise known or when the person denies any presence at a collision.

- All collision reports and supplemental information filed in connection with the administration of the laws of this state relating to the deposit of security or proof of financial responsibility shall be confidential and not open to general public inspection, nor shall copying of lists of the reports be permitted, except, however, that the reports and supplemental information may be examined by, or the Department may provide a copy to, any person named therein, a representative of the person as designated in writing by the person, or as provided in Section 40-102 of this title.
 - No reports or information mentioned in this section shall be used as evidence.
- **Vehicle Identification Numbers**
 - Dick v. State, 596 P.2d 1265 (Okla. Crim. App. 1979) - viewing a VIN through the windshield with a flashlight is not a search.
 - OKLA. STAT. tit. 47, § 1503 (2008) - Any person who knowingly alters, counterfeits, defaces, destroys, disguises, falsifies, forges, obliterates, or knowingly removes a vehicle identification number, with the intent to misrepresent the identity or prevent the identification of a motor vehicle or motor vehicle part, upon conviction is guilty of a felony. Anyone who knowingly sells such vehicle is also guilty of a felony.
- **Consumer Credit**
 - OKLA. STAT. tit. 24, § 147 (2008) - Consumer reporting agency must disclose all information it has on a consumer to that consumer, except for medical records.
 - OKLA. STAT. tit. 24, §§ 149 through 159 (2008) Oklahoma Consumer Report Security Freeze Act.
 - permits security freezes = a notice placed in a consumer report of a consumer, at the request of the consumer and subject to certain exceptions, that prohibits the consumer reporting agency from releasing the consumer report or credit score of the consumer relating to the opening of new accounts or the extension of credit.
 - Security Breaches of personal information. Not codified law yet, BUT:
 - H.R. 2245, 51st Sess. (Okla. 2008), *available at* 2008 OK. ALS 86.
- **Financial Records**
 - OKLA. STAT. tit. 6, § 208 (2008). The following records in the Oklahoma State Banking Department are designated as public records: 1. All applications for state bank charters and supporting information with the exception of personal financial records of individual applicants; 2. All records introduced at public hearings on bank charter applications; 3. Information disclosing the failure of a state bank, an out-of-state bank and branches of out-of-state banks located in this state and the reasons therefore; 4. Reports of completed investigations which uncover a shortage of funds in a bank, an out-of-state bank and branches of out-of-state banks located in this state, 5. Names of all stockholders and officers of banks, out-of-state banks, out-of-state bank holding companies, and branches of out-of-state banks located in this state filed in the office of the Secretary of State; and 6. Regular financial call reports issued at the time of the state bank calls.
 - All other records in the Department shall be confidential and not subject to public inspection. However, the Banking Board, Commissioner, or Deputy

Commissioner may divulge such confidential information with the written approval of the Commissioner after receipt of a written request.

- OKLA. STAT. tit. 6, § 2201 through § 2208 (2008) "Financial Privacy Act". Its purpose is to maintain the privacy and confidentiality of the records of customers of financial institutions.
 - § 2203. Financial institutions prohibited from disclosing financial records unless (a) it has written consent from the customer for the specific record requested; or (b) it has been served with a subpoena issued pursuant to Section 4 for the specific record requested.
 - § 2204. Subpoena of financial records by certain entities makes financial records available.
 - § 2205. Disclosures or releases authorized
 - Nothing in the Financial Privacy Act shall prohibit the disclosure or release of any financial record or information to any supervisory agency in the exercise of its supervisory or regulatory functions with respect to a financial institution.
 - Nothing in the Financial Privacy Act prohibits a financial institution from disclosing or releasing any financial record or information to another financial institution for the usual and regular business purposes of the latter or from providing copies of any financial record to any court or government authority as an incident to perfecting a security interest, proving a claim in bankruptcy or otherwise collecting on a debt either owed the financial institution itself or owed the financial institution in its role as a fiduciary.
 - Nothing in the Financial Privacy Act prohibits a financial institution from notifying a government authority that such institution or an officer, employee or agent of such institution has information that may be relevant to a possible violation of any statute or regulation.
- **Employee Privacy**
 - Tanique, Inc. v. State, 99 P.3d 1209 (Okla. Civ. App. 2004) - explicitly held that an employee, lacking a possessory interest in his or her place of employment, has no expectation of privacy in the employer's premises under the Fourth Amendment.
 - OKLA. STAT. tit. 13, § 560 (2008). Confidentiality of testing results and records-- Disclosure of general health information prohibited. Drug and alcohol test results and related information must be kept separate from personnel records and otherwise confidential.
 - OKLA. STAT. tit. 13, § 559 (2008) Sample collection of drug and alcohol testing of employees must be done with regard to their privacy.
- **Electronic Surveillance**
 - OKLA. STAT. tit. 13, § 176.1 (2008) Short title. Security of Communication Act.
 - OKLA. STAT. tit. 13, § 176.2 (2008). Definitions. "Electronic communication" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic,

- photoelectronic or photooptical system, but does not include: a. any wire or oral communication, b. any communication made through a tone-only paging device, or c. any communication from a tracking device;
- OKLA. STAT. tit. 13, § 176.3 (2008). Prohibited acts--Felonies--Penalties--Venue. Willfully intercepts, endeavors to intercept or procures any other person to intercept or endeavor to intercept any wire, oral or electronic communication; 2. Willfully uses, endeavors to use or procures any other person to use or endeavor to use any electronic, mechanical or other device to intercept any oral communication; 3. Willfully discloses or endeavors to disclose to any other person the contents of any wire, oral or electronic communication, knowing or having reason to know that the information was obtained in violation of the provisions of the Security of Communications Act;
 - OKLA. STAT. tit. 13, § 176.4 (2008). Acts not prohibited. Law enforcement, common carriers, FCC, with consent of one party.
 - OKLA. STAT. tit. 13, § 176.5 (2008). Seizure and forfeiture of certain devices
 - OKLA. STAT. tit. 13, § 176.6 (2008). Use of certain intercepted communications as evidence prohibited
 - OKLA. STAT. tit. 13, § 176.7 (2008). Court order authorizing interception of communications. Attorney general or district attorney may submit and application if such interception may provide evidence of acts of biochemical terrorism, terrorism, terrorism hoax, and biochemical assault as defined in Section 1268.1 of Title 21 of the Oklahoma Statutes, the commission of the offense of murder, the cultivation or manufacture or distribution of narcotic drugs or other controlled dangerous substances as defined in the Uniform Controlled Dangerous Substances Act, or trafficking in illegal drugs, as defined in the Trafficking in Illegal Drugs Act, and any conspiracy to commit the crimes specifically enumerated in this section.
 - OKLA. STAT. tit. 13, § 176.8 (2008). Disclosure of information
 - OKLA. STAT. tit. 13, § 176.9 (2008). Application for court order--Contents--Additional evidence--Ex parte order--Specifications of order--Time ...
 - OKLA. STAT. tit. 13, § 176.10 (2008). Recording intercepted communication--Seal--Inventory--Inspection--Violation
 - OKLA. STAT. tit. 13, § 176.11 (2008). Reports
 - OKLA. STAT. tit. 13, § 176.12 (2008). Conditions for use of intercepted communication as evidence or disclosure at trial
 - OKLA. STAT. tit. 13, § 176.13 (2008). Suppression of intercepted communication or evidence derived therefrom
 - OKLA. STAT. tit. 13, § 176.14 (2008). State's right to appeal certain orders
 - OKLA. STAT. tit. 13, § 177.1 (2008). Definitions. "Electronic communication" means any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electro-magnetic, photo-electronic or photo-optical system, but does not include: a. any wire or oral communication, b. any communication made through a tone-only paging device, or c. any communication from a tracking device;
 - OKLA. STAT. tit. 13, § 177.2 (2008). Installation or use of pen register or trap and trace device without court order--Exceptions--Penalty

- OKLA. STAT. tit. 13, § 177.3 (2008). Application for order or extension of order
- OKLA. STAT. tit. 13, § 177.4 (2008). Court order--Contents--Duration
- OKLA. STAT. tit. 13, § 177.5 (2008). Assistance of service provider, landlord, custodian or other person--Compensation--Liability--Defense
- OKLA. STAT. tit. 21, § 1202 (2008). Eavesdropping. Every person guilty of secretly loitering about any building, with intent to overhear discourse therein, and to repeat or publish the same to vex, annoy, or injure others, is guilty of a misdemeanor.
- **Computer Statutes**
 - OKLA. STAT. tit. 21, §§ 1953; 1957; 1958 (2008). Computer Crimes Act. It shall be unlawful to:
 - 1. Willfully, and without authorization, gain or attempt to gain access to and damage, modify, alter, delete, destroy, copy, make use of, disclose or take possession of a computer, computer system, computer network or any other property;
 - 2. Use a computer, computer system, computer network or any other property as hereinbefore defined for the purpose of devising or executing a scheme or artifice with the intent to defraud, deceive, extort or for the purpose of controlling or obtaining money, property, services or other thing of value by means of a false or fraudulent pretense or representation;
 - 3. Willfully exceed the limits of authorization and damage, modify, alter, destroy, copy, delete, disclose or take possession of a computer, computer system, computer network or any other property;
 - 4. Willfully and without authorization, gain or attempt to gain access to a computer, computer system, computer network or any other property;
 - 5. Willfully and without authorization use or cause to be used computer services;
 - 6. Willfully and without authorization disrupt or cause the disruption of computer services or deny or cause the denial of access or other computer services to an authorized user of a computer, computer system or computer network;
 - 7. Willfully and without authorization provide or assist in providing a means of accessing a computer, computer system or computer network in violation of this section;
 - 8. Willfully use a computer, computer system, or computer network to annoy, abuse, threaten, or harass another person; and
 - 9. Willfully use a computer, computer system, or computer network to put another person in fear of physical harm or death.
- **Common Law**
 - McCormack v. Okla. Publ'g Co., 613 P.2d 737 (Okla. 1980) - accepts the four strands of the invasion of privacy as dictated by the Restatement.

OREGON PRIVACY LAW

- **State Constitutional Privacy Rights**
- **Search and Seizure**
 - OR. CONST. art. I, § 9 - protects against unreasonable search and seizure
 - **Auto Exception**
 - State v. Meharry, 149 P.3d 1155 (Or. 2006).
 - **Open Fields**
 - State v. Brown, 461 P.2d 836 (Or. Ct. App. 1969).
 - **Plain View**
 - State v. Holt, 630 P.2d 854 (Or. 1981).
- **Statutory Privacy Rights**
 - OR. REV. STAT. ANN. § 163.730 through .755 (2007). The person knowingly alarms or coerces another person or a member of that person's immediate family or household by engaging in repeated and unwanted contact with the other person; it is objectively reasonable for a person in the victim's situation to have been alarmed or coerced by the contact; and the repeated and unwanted contact causes the victim reasonable apprehension regarding the personal safety of the victim or a member of the victim's immediate family or household.
 - OR. REV. STAT. ANN. § 247.955 (2007) Use of Lists of Electors for Commercial Purposes Prohibited. There are some exceptions.
- **Public Records**
 - OR. REV. STAT. ANN. § 19.420 (2007) - right to inspect any public record of a public body unless otherwise provided.
 - OR. REV. STAT. ANN. § 19.445 through § 19.502 (2007) - provides the list of records exempt from disclosure including: criminal investigatory information, advisory communication within public bodies, home addresses, email, medical records, etc.
- **Motor Vehicle Records**
 - OR. REV. STAT. ANN. § 802.220 (2007) Except as otherwise provided, the records the Department of Transportation maintains on vehicles are public records.
 - The department may charge the fee established under ORS 802.230 for furnishing to the public information from the records the department maintains under ORS 802.200 concerning driver licenses or driver permits.
 - The records the department keeps under ORS 802.200 on judgments or convictions under ORS 810.375 shall be open to the inspection of any person during reasonable business hours. Nothing in this subsection authorizes the release of personal information as defined in ORS 802.175.
 - The department shall upon request furnish any person certified abstracts of the employment driving record and the nonemployment driving record of any person whose driving records are maintained under ORS 802.200.
 - Abstracts don't contain any accident or conviction for violation of motor vehicles laws that occurred more than three years immediately preceding a request for abstract, but can be provided for individuals and their agents involved in the accident.

- The records the department maintains under ORS 802.200 concerning odometer readings for vehicles are public records.
 - OR. REV. STAT. ANN. § 802.177 (2007). Prohibition on release of personal information from motor vehicle records. Except as otherwise provided in ORS 802.179, neither the Department of Transportation nor any officer, employee or contractor of the department may knowingly disclose or otherwise make available to any person personal information about an individual that is obtained by the department in connection with a motor vehicle record.
 - OR. REV. STAT. ANN. § 802.179 (2007). Exceptions for disclosing personal information from motor vehicle records include to government agencies carrying out their legitimate functions.
- **Vehicle Identification Numbers**
 - OR. REV. STAT. ANN. § 803.103 (2007). Vehicle identification number check. With every vehicle title transfer, the Department of Transportation shall check the vehicle identification number or numbers on the vehicle title or other primary ownership records against those listed as stolen by the Law Enforcement Data System.
 - OR. REV. STAT. ANN. § 803.212 (2007) Inspectors may refer a vehicle to law enforcement officials for a VIN inspection if the VIN has been tampered with. If a referral is made the law enforcement agency must inspect the vehicle and may seize and hold the vehicle until completing the investigation.
 - State v. Turechek, 701 P.2d 1131 (Or. Ct. App. 1985) - There is no recognized privacy exception with regard to a VIN, but its location in the car may give rise to a reasonable expectation of privacy.
- **Consumer Credit**
 - OR. REV. STAT. ANN. § 746.635 (2007) No insurer, insurance producer or insurance-support organization may prepare or request an investigative consumer report about an individual in connection with an insurance transaction involving an application for insurance, a policy renewal, a policy reinstatement or a change in insurance benefits unless the insurer or insurance producer informs the individual.
 - OR. REV. STAT. ANN. § 746.665 (2007) A licensee or insurance-support organization may not disclose any personal or privileged information about an individual collected or received in connection with an insurance transaction unless the disclosure meets one or more of the following conditions: written authorization, reasonably necessary to perform a business function and there is an agreement not to disclose further.
 - OR. REV. STAT. ANN. § 646A.214 (2007). Verification of identity in credit or debit card transactions. A merchant that accepts a credit card or debit card for a transaction may require that the credit card or debit card holder provide personal information, other than the personal information that appears on the face of the credit card or debit card, for the purposes of verification of the card holder's identity. The merchant may not write the information on the credit card or debit card transaction form.
- **Financial Records**

- OR. REV. STAT. ANN. § 192.555 (2007). No financial institution shall provide any financial records of any customer to a state or local agency. No state or local agency shall request or receive from a financial institution any financial records of customers. Exceptions include if the financial institution suspects a violation of law by its customer.
- OR. REV. STAT. ANN. § 192.560 (2007) A financial institution may disclose financial records of a customer to a state or local agency, and such an agency may request and receive such records, when the customer has authorized such disclosure as provided in this section [in writing, identify records to be disclosed, state that the customer understands why the records are being requested].
- **Employee Privacy**
 - OR. REV. STAT. ANN. § 659.840 (2007) Requiring Breathalyzer or Lie Detector Test Prohibited; Exception for Breathalyzer Test
 - OR. REV. STAT. ANN. § 659A.500 (2007) Requiring breathalyzer, polygraph, psychological stress or brain-wave test or genetic test prohibited; exceptions
 - OR. REV. STAT. ANN. § 825.410 (2007) Motor carrier employers must institute a drug and alcohol testing program.
- **Electronic Surveillance**
 - OR. REV. STAT. ANN. § 133.721 (2007). Definitions for ORS 41.910 and 133.721 to 133.739. "Electronic communication" means any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a radio, electromagnetic, photoelectronic or photo-optical system, or transmitted in part by wire, but does not include: (a) Any oral communication or any communication that is completely by wire; or (b) Any communication made through a tone-only paging device.
 - OR. REV. STAT. ANN. § 133.723 (2007). Records confidential. Applications for orders permitting the interception of communications shall remain confidential
 - OR. REV. STAT. ANN. § 133.724 (2007). Order for interception of communications; application; grounds for issuance; contents of order; progress.
 - OR. REV. STAT. ANN. § 133.726 (2007). Interception of oral communication without order; order for interception of oral communication;
 - OR. REV. STAT. ANN. § 133.727 (2007). Proceeding under expired order prohibited.
 - OR. REV. STAT. ANN. § 133.729 (2007). Recording intercepted communications; method; delivery to court; custody. If possible, permitted interceptions should be recorded.
 - OR. REV. STAT. ANN. § 133.731 (2007). Inventory; contents; inspection of intercepted communications. Within a reasonable time but not later than 90 days after the termination of the period of an order issued under ORS 133.724, or extensions thereof, the issuing or denying judge shall cause to be served, on the persons named in the order or the application, and such other parties to intercepted communications as the judge may determine in the judge's discretion should be served in the interest of justice, an inventory.
 - OR. REV. STAT. ANN. § 133.733 (2007). Procedure for introduction as evidence.
 - OR. REV. STAT. ANN. § 133.735 (2007). Suppression of intercepted communications; procedure; grounds; appeal.

- OR. REV. STAT. ANN. § 133.736 (2007). Motion to suppress intercepted oral communication; right of state to appeal.
- OR. REV. STAT. ANN. § 133.737 (2007). Disclosure and use of intercepted communications. The contents of intercepted communications may be disclosed pursuant to the performance of official law enforcement duties or while under testimony in a state proceeding.
- OR. REV. STAT. ANN. § 133.739 (2007). Civil damages for willful interception, disclosure or use of communications; attorney fees; defense. Any person whose communication was intercepted or disclosed in violation of law has a civil cause of action and punitive damages are available.
- OR. REV. STAT. ANN. § 165.535 (2007). Definitions applicable to obtaining contents of communications. "Telecommunication" means the transmission of writing, signs, signals, pictures and sounds of all kinds by aid of wire, cable or other similar connection between the points of origin and reception of such transmission, including all instrumentalities, facilities, equipment and services (including, among other things, the receipt, forwarding and delivering of communications) incidental to such transmission.
- OR. REV. STAT. ANN. § 165.540 (2007). Obtaining contents of communications.
- OR. REV. STAT. ANN. § 165.542 (2007) Reports required concerning use of electronic listening device. Within 30 days report to the district attorney. Collect annually by the attorney general.
- OR. REV. STAT. ANN. § 165.543 (2007). Interception of communications. Willfully intercepts, attempts to intercept or improperly uses wire or oral communication who is not a party to the communication is guilty of a misdemeanor.
- OR. REV. STAT. ANN. § 165.545 (2007). Prohibitions not applicable to fire or police activities for rebroadcasting emergency calls.
- OR. REV. STAT. ANN. § 165.657 (2007) Definitions. "Electronic communication" means any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a radio, electromagnetic, photoelectronic or photo-optical system, or transmitted in part by wire, but does not include: (a) Any oral communication or any communication that is completely by wire; or (b) Any communication made through a tone-only paging device.
- OR. REV. STAT. ANN. § 165.659 (2007) Prohibition on installation or use unless otherwise granted under this chapter
- OR. REV. STAT. ANN. § 165.661 (2007) Service provider use
- OR. REV. STAT. ANN. § 165.663 (2007) Police use by police
- OR. REV. STAT. ANN. § 165.667 (2007) Court order. upon application, a court shall enter an ex parte order authorizing the installation and use of a pen register or a trap and trace device if the court finds that there is probable cause to believe that: an individual is committing, has committed or is about to commit: A particular felony of murder, kidnapping, arson, robbery, bribery, extortion or other crime dangerous to life and punishable as a felony and other enumerated crimes.
- OR. REV. STAT. ANN. § 165.669 (2007) Duties of person executing order; compensation

- OR. REV. STAT. ANN. § 165.671 (2007) Defenses, civil or criminal action
- OR. REV. STAT. ANN. § 165.673 (2007) Disclosure of telephone numbers. No law enforcement agency shall disclose lists of telephone numbers produced by a pen register or trap and trace device except in the performance of a law enforcement function or as otherwise provided by law or order of a court.
- OR. REV. STAT. ANN. § 133.619 (2007). Execution of warrant authorizing mobile tracking device.
- **Computer Statutes**
 - OR. REV. STAT. ANN. § 164.377 (2007). Any person commits computer crime who knowingly accesses, attempts to access or uses, or attempts to use, any computer, computer system, computer network or any part thereof for the purpose of: (a) Devising or executing any scheme or artifice to defraud; (b) Obtaining money, property or services by means of false or fraudulent pretenses, representations or promises; or (c) Committing theft, including, but not limited to, theft of proprietary information. (3) Any person who knowingly and without authorization alters, damages or destroys any computer, computer system, computer network, or any computer software, program, documentation or data contained in such computer, computer system or computer network, commits computer crime. (4) Any person who knowingly and without authorization uses, accesses or attempts to access any computer, computer system, computer network, or any computer software, program, documentation or data contained in such computer, computer system or computer network, commits computer crime.
- **Common Law**
 - McLain v. Boise Cascade Corp., 533 P.2d 343 (Or. 1975). Recognizes Prosser's four strands of invasion of privacy torts.

PENNSYLVANIA PRIVACY LAW

- **State Constitutional Privacy Rights**
 - none
- **Search and Seizure**
 - PA. CONST. ANN. art. I, § 8 - security from unreasonable search and seizure guaranteed.
 - Commonwealth v. Perdue, 566 A.2d 489 (Pa. 1989) - There is no reasonable expectation of privacy in items that are in a garbage can, these are considered abandoned.
 - Commonwealth v. Lemanski, 529 A.2d 1085 (Pa. Super. Ct. 1986) - no reasonable expectation of privacy in something that can be viewed from a public vantage point. Ex. glass greenhouse, 200 feet from the street, blocked by trees.
 - **Auto Exception**
 - Commonwealth v. Hernandez, 935 A.2d 1275 (Pa. 2007) - Pennsylvania has not adopted the full federal automobile exception under Pa. Const. art. I, § 8. Warrantless vehicle searches in the Commonwealth of Pennsylvania must be accompanied not only by probable cause, but also by exigent circumstances beyond mere mobility; one without the other is insufficient. This dual requirement of probable cause plus exigency is an established part of Pennsylvania's state constitutional jurisprudence.
 - **Open Fields**
 - Commonwealth v. Blosenski Disposal Svc., 566 A.2d 845 (Pa. 1989)
 - **Plain View**
 - Commonwealth v. Jefferies, 311 A.2d 914 (Pa. 1973)
- **Statutory Privacy Rights**
 - 18 PA. CONS. STAT. ANN. § 2709.1 (2008) - A person commits the crime of stalking when the person either: (1) engages in a course of conduct or repeatedly commits acts toward another person, including following the person without proper authority, under circumstances which demonstrate either an intent to place such other person in reasonable fear of bodily injury or to cause substantial emotional distress to such other person; or (2) engages in a course of conduct or repeatedly communicates to another person under circumstances which demonstrate or communicate either an intent to place such other person in reasonable fear of bodily injury or to cause substantial emotional distress to such other person.
 - 71 PA. CONS. STAT. ANN. §§ 2601 through 2608 (2008) - Social Security Number Privacy Act. Allows individuals to use an alternate number when applying for the renewal of state licenses. Can't put a Social Security number on a health care card, but the Dept. of Public Welfare has an exemption to this Act.
 - 74 PA. CONS. STAT. ANN. § 201 (2008) Privacy of Social Security number. No entity in the state may publicly display SSNs, ask for a SSN input on a website unless the site is secure and the input encrypted, or mail anything with the SSN on the outside of the envelope.
- **Public Records**
 - 65 PA. CONS. STAT. ANN. § 67.305 (2008) A record in the possession of a Commonwealth agency or local agency shall be presumed to be a public record.

The presumption shall not apply if: (1) the record is exempt under section 708; (2) the record is protected by a privilege; or (3) the record is exempt from disclosure under any other Federal or State law or regulation or judicial order or decree.

- 65 PA. CONS. STAT. ANN. § 66.3-1 (2008) - An agency may not deny a requester access to a public record due to the intended use of the public record by the requester.
- 65 PA. CONS. STAT. ANN. § 67.706 (2008) If the information which is not subject to access is an integral part of the public record, legislative record or financial record and cannot be separated, the agency shall redact from the record the information which is not subject to access, and the response shall grant access to the information which is subject to access. The agency may not deny access to the record if the information which is not subject to access is able to be redacted.
- 65 PA. CONS. STAT. ANN. § 67.708 (2008) Exceptions to access of public records include information that would compromise security or contains personal information or hinders an agency's ability to conduct an investigation, etc.
- 30 PA. CONS. STAT. ANN. §§ 324 (2008) Any records maintained by the commission or any issuing agent or other agent of the commission that contain or include the home address of any individuals or any other personal information about individuals such as height, weight, color of hair and/or color of eyes, including but not limited to fishing licenses and applications therefore, boat registrations and applications therefore and permits and applications therefore, are not public records.
- 35 PA. CONS. STAT. ANN. §§ 7309 (2008) Employee health records identifying individuals are confidential.
- Sullivan v. Pittsburgh, 561 A.2d 863 (Pa. Commw. Ct. 1989) - must weigh privacy vs. public's right to know. Investigative reports by police are not public records.
- **Motor Vehicle Records**
 - 75 PA. CONS. STAT. ANN. § 3747 (2008) - Accident reports shall be for the confidential use of the department or any other governmental agency or their representatives having use for the records for accident prevention purposes, except that the department shall disclose the identity of a person involved in an accident when the identity is not otherwise known or when the person denies his presence at the accident and shall disclose whether any person or vehicle was covered by a vehicle insurance policy and the name of the insurer.
 - 75 PA. CONS. STAT. ANN. § 6104 (2008) The department may supply copies of and information concerning registrations, titles and security interests of vehicles and such statistical data as it may deem to be in the public interest.
 - 75 PA. CONS. STAT. ANN. § 6114 (2008) - unlawful to buy or sell driving records without consent, court order or authorization.
 - Any police officer, or any officer, employee or agent of any commonwealth agency or local authority which makes or receives records or reports required to be filed under this title to sell, publish or disclose or offer to sell, publish or disclose records or reports which relate to the driving record of any person.
- **Vehicle Identification Numbers**

- 75 PA. CONS. STAT. ANN. § 6308 (2008) Authority of Police Officer - Whenever a police officer is engaged in a systematic program of checking vehicles or drivers or has reasonable suspicion that a violation of this title is occurring or has occurred, he may stop a vehicle, upon request or signal, for the purpose of checking the vehicle's registration, proof of financial responsibility, vehicle identification number or engine number or the driver's license, or to secure such other information as the officer may reasonably believe to be necessary to enforce the provisions of this title.
- 75 PA. CONS. STAT. ANN. § 6308 (2008) Inspection of Garages and Dealer Premises. -- Any police officer or authorized department employee may inspect any vehicle in any garage or repair shop or on the premises of any dealer, miscellaneous motor vehicle business, salvage motor vehicle auction or pool operator, salvor, scrap metal processor, or other public place of business for the purpose of locating stolen vehicles or parts or vehicles or vehicle parts with identification numbers removed or falsified. The owner of the garage or repair shop or the dealer or other person shall permit any police officer or authorized department employee to make investigations under this subsection.
- 18 PA. CONS. STAT. ANN. § 1.4 (2008) - Alteration Or Destruction Of Vehicle Identification Number.-- Any person who alters, counterfeits, defaces, destroys, disguises, falsifies, forges, obliterates or removes a vehicle identification number with the intent to conceal or misrepresent the identity or prevent the identification of a motor vehicle or motor vehicle part commits a felony of the third degree.
- Commonwealth v. Grabowski, 452 A.2d 827 (Pa. Super. Ct. 1982) - Police view of VIN is not a search even if the police had to raise car with a forklift. Exterior examination of a car isn't a search.
- **Consumer Credit**
 - 7 PA. CONS. STAT. ANN. § 6223 (2008) Confidentiality of Credit Records. Compliance review documents [prepared for or created by an audit, loan review or compliance committee appointed by the board of directors of a depository institution] are confidential and are not discoverable or admissible in evidence in any civil action arising out of matters evaluated by the compliance review committee.
 - 73 PA. CONS. STAT. ANN. § 2503 (2008) A consumer may elect to place a security freeze on his consumer report by providing proper identification to a consumer reporting agency.
 - 73 PA. CONS. STAT. ANN. § 2303 (2008) Breach Of Personal Information Notification Act. An entity that maintains, stores or manages computerized data that includes personal information shall provide notice of any breach of the security of the system following discovery of the breach of the security of the system to any resident of this Commonwealth whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person. The notice shall be made without unreasonable delay.
 - For the purpose of this section, a resident of this Commonwealth may be determined to be an individual whose principal mailing address, as

reflected in the computerized data which is maintained, stored or managed by the entity, is in this Commonwealth.

- An entity must provide notice of the breach if encrypted information is accessed and acquired in an unencrypted form, if the security breach is linked to a breach of the security of the encryption or if the security breach involves a person with access to the encryption key.
- **Financial Records**
 - 7 PA. CONS. STAT. ANN. § 6209 (2008) Licensees operating under the provisions of this act shall maintain adequate and complete records of all business transacted, containing such information and in such form as shall be prescribed by the Secretary of Banking by general rule or regulation. The records of licensees shall be maintained in the English language. The records of licensees shall be retained for a period of two years after the date of final payment on any contract.
 - Commonwealth v. DeJohn, 403 A.2d 1283 (Pa. 1979) - There is a reasonable expectation of privacy in bank records. Requires a warrant to inspect.
 - 15 PA. CONS. STAT. ANN. § 1508 (2008) - Corporate financial records may be inspected by shareholders.
- **Employee Privacy**
 - 43 PA. CONS. STAT. ANN. § 1322 (2008) An employer shall, at reasonable times, upon request of an employee, permit that employee or an agent designated by the employee to inspect his or her own personnel files used to determine his or her own qualifications for employment, promotion, additional compensation, termination or disciplinary action. The employer shall make these records available during the regular business hours of the office where these records are usually and ordinarily maintained, when sufficient time is available during the course of a regular business day, to inspect the personnel files in question. The employer may require the requesting employee or the agent designated by the employee to inspect such records on the free time of the employee or agent.
 - 35 PA. CONS. STAT. ANN. § 7309 (2008) Employee Health Records.
 - Upon request by the department, employers shall provide copies of employee health and exposure records maintained by the employer, including, but not limited to, those records maintained and supplied to the Federal Government by employers as mandated under applicable State and Federal statutes and regulations except as access by third parties is limited by said statutes and regulations.
 - Employees under this act shall have the right of access to exposure and medical records in the manner set forth by OSHA pursuant to 29 CFR 1910.20 (relating to access to employee exposure and medical records).
 - 65 PA. CONS. STAT. ANN. § 67.708 (2008) The following records relating to an agency employee are exempt from public disclosure: (i) A letter of reference or recommendation pertaining to the character or qualifications of an identifiable individual, unless it was prepared in relation to the appointment of an individual to fill a vacancy in an elected office or an appointed office requiring Senate confirmation. (ii) A performance rating or review. (iii) The result of a civil service or similar test administered by a Commonwealth agency, legislative agency or judicial agency. The result of a civil service or similar test administered by a local

agency shall not be disclosed if restricted by a collective bargaining agreement. Only test scores of individuals who obtained a passing score on a test administered by a local agency may be disclosed. (iv) The employment application of an individual who is not hired by the agency. (v) Workplace support services program information. (vi) Written criticisms of an employee. (vii) Grievance material, including documents related to discrimination or sexual harassment. (viii) Information regarding discipline, demotion or discharge contained in a personnel file. This subparagraph shall not apply to the final action of an agency that results in demotion or discharge. (ix) An academic transcript.

- **Electronic Surveillance**

- 18 PA. CONS. STAT. ANN. § 5701 (2008) Wiretapping and Electronic Surveillance Control Act
- 18 PA. CONS. STAT. ANN. § 5702 (2008) Definitions. "Electronic communication." Any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photo-optical system, except: (1) Deleted. (2) Any wire or oral communication, (3) Any communication made through a tone-only paging device, (4) Any communication from a tracking device (as defined in this section).
- 18 PA. CONS. STAT. ANN. § 5703 (2008) Interception, disclosure or use of wire, electronic or oral communications. Intentionally intercepts, endeavors to intercept, procures any other person or uses or discloses or endeavors to intercept any wire, electronic or oral communication.
- 18 PA. CONS. STAT. ANN. § 5704 (2008) Exceptions to prohibition of interception and disclosure of communications. Communications operators, law enforcement, consent of one party, emergency response systems as long as there is a warning that the conversation is being recorded, public frequencies.
- 18 PA. CONS. STAT. ANN. § 5705 (2008) Possession, sale, distribution, manufacture or advertisement of electronic, mechanical or other devices
- 18 PA. CONS. STAT. ANN. § 5706 (2008) Exceptions to prohibitions in possession, sale, distribution, manufacture or advertisement of electronic, mechanical or other devices
- 18 PA. CONS. STAT. ANN. § 5707 (2008) Seizure and forfeiture of electronic, mechanical or other devices
- 18 PA. CONS. STAT. ANN. § 5708 (2008) Order authorizing interception of wire, electronic or oral communications. Lists the crimes that can warrant surveillance including murder, manslaughter, terrorist threats. The application must show probable cause that the person tapped will or had completed this crime.
- 18 PA. CONS. STAT. ANN. § 5709 (2008) Application for order
- 18 PA. CONS. STAT. ANN. § 5710 (2008). Grounds for entry of order
- 18 PA. CONS. STAT. ANN. § 5711 (2008). Privileged communications
- 18 PA. CONS. STAT. ANN. § 5712 (2008). Issuance of order and effect
- 18 PA. CONS. STAT. ANN. § 5713 (2008). Emergency situations
- 18 PA. CONS. STAT. ANN. § 5713.1 (2008). Emergency hostage and barricade situations

- 18 PA. CONS. STAT. ANN. § 5714 (2008). Recording of intercepted communications. Records kept during the surveillance include date and time, etc.
- 18 PA. CONS. STAT. ANN. § 5715 (2008). Sealing of applications, orders and supporting papers
- 18 PA. CONS. STAT. ANN. § 5716 (2008). Service of inventory and inspection of intercepted communications
- 18 PA. CONS. STAT. ANN. § 5717 (2008). Investigative disclosure or use of contents of wire, electronic or oral communications or derivative ...
- 18 PA. CONS. STAT. ANN. § 5718 (2008). Interception of communications relating to other offenses. Can still be admitted if a judge finds that the rules of intercepting communications were followed otherwise.
- 18 PA. CONS. STAT. ANN. § 5719 (2008). Unlawful use or disclosure of existence of order concerning intercepted communication
- 18 PA. CONS. STAT. ANN. § 5720 (2008). Service of copy of order and application before disclosure of intercepted communication in trial, ...
- 18 PA. CONS. STAT. ANN. § 5721.1 (2008). Evidentiary disclosure of contents of intercepted communication or derivative evidence
- 18 PA. CONS. STAT. ANN. § 5722 (2008). Report by issuing or denying judge
- 18 PA. CONS. STAT. ANN. § 5723 (2008). Annual reports and records of Attorney General and district attorneys
- 18 PA. CONS. STAT. ANN. § 5724 (2008). Training
- 18 PA. CONS. STAT. ANN. § 5725 (2008). Civil action for unlawful interception, disclosure or use of wire, electronic or oral communication. There's a civil cause of action against a communication interceptor.
- 18 PA. CONS. STAT. ANN. § 5726 (2008). Action for removal from office or employment
- 18 PA. CONS. STAT. ANN. § 5728 (2008). Injunction against illegal interception
- 18 PA. CONS. STAT. ANN. § 5741 (2008). Unlawful access to stored communications. No one except for the custodian of the communications or an authorized user of communications may have access.
- 18 PA. CONS. STAT. ANN. § 5742 (2008). Disclosure of contents
- 18 PA. CONS. STAT. ANN. § 5743 (2008). Requirements for governmental access. May be disclosed if there is a warrant, subpoena, or subscriber consent.
- 18 PA. CONS. STAT. ANN. § 5747 (2008). Civil action
- 18 PA. CONS. STAT. ANN. § 5748 (2008). Exclusivity of remedies
- 18 PA. CONS. STAT. ANN. § 5749 (2008). Retention of certain records. Shall maintain all recordings of oral communications intercepted under section 5704(16) (relating to exceptions to prohibition of interception and disclosure of communications) for a minimum of 31 days after the date of the interception. All recordings made under section 5704(16) shall be recorded over or otherwise destroyed no later than 90 days after the date of the recording unless certain exceptions apply including the necessity of the recording for a proceeding.
- 18 PA. CONS. STAT. ANN. § 5761 (2008). Mobile tracking devices. Expired on Dec. 30, 2008, but the legislature seemed to have renewed the statute (2008 Pa. Laws 111). Mobile trackers can be authorized by the Court of Common Pleas, for

90 days. Private areas may not be monitored unless there are exigent circumstances or probable cause of criminal activity within the area.

- **Computer Statutes**

- 18 PA. CONS. STAT. ANN. § 7601 through § 7661 (2008)
 - § 7611. Unlawful use of computer and other computer crimes. Accesses or exceeds authorization to access, alters, damages or destroys any computer, computer system, computer network, computer software, computer program, computer database, World Wide Web site or telecommunication device or any part thereof with the intent to interrupt the normal functioning of a person or to devise or execute any scheme or artifice to defraud or deceive or control property or services by means of false or fraudulent pretenses, representations or promises;
 - § 7613. Computer theft
 - § 7614. Unlawful duplication
 - § 7615. Computer trespass A person commits the offense of computer trespass if he knowingly and without authority or in excess of given authority uses a computer or computer network with the intent to: (1) temporarily or permanently remove computer data, computer programs or computer software from a computer or computer network; (2) cause a computer to malfunction, regardless of the amount of time the malfunction persists; (3) alter or erase any computer data, computer programs or computer software;(4) effect the creation or alteration of a financial instrument or of an electronic transfer of funds; or (5) cause physical injury to the property of another.
 - § 7616. Distribution of computer virus
 - § 7641. Computer-assisted remote harvesting of animals. A person who engages in computer-assisted remote harvesting of an animal or provides or operates a facility for another person to engage in computer-assisted remote harvesting of an animal commits a misdemeanor of the third degree.
 - § 7661. Unlawful transmission of electronic mail

- **Common Law**

- Burger v. Blair Med. Assocs., 964 A.2d 374 (Pa. 2008). Recognizes the four invasion of privacy torts based on the Restatement.
 - “In the present case, although again we recognize there is overlap, neither of the torts of invasion of privacy nor breach of confidentiality is entirely subsumed within the other.”

RHODE ISLAND PRIVACY LAW

- **State Constitutional Privacy Rights**
 - none
- **Search and Seizure**
 - R.I. CONST. art. I, § 6 - protects against unreasonable search and seizure.
 - **Auto Exception**
 - State v. Werner, 615 A.2d 1010 (R.I. 1992).
 - **Open Fields**
 - State v. Beane, 609 A.2d 950 (R.I. 1992).
 - **Plain View**
 - State v. Robalewski, 418 A.2d 817 (R.I. 1980).
- **Statutory Privacy Rights**
 - R.I. GEN. LAWS § 9-1-28.1 (2009). Right to privacy -- Action for deprivation of right. (a) Right to privacy created. It is the policy of this state that every person in this state shall have a right to privacy which shall be defined to include any of the following rights individually, freedom from: unreasonable intrusion upon one's physical solitude or seclusion, appropriation of one's name or likeness, unreasonable publicity given to one's private life, publicity that reasonably places another in a false light before the public.
 - R.I. GEN. LAWS § 11-52-4.2 (2009). Cyberstalking and cyberharassment prohibited. (a) Whoever transmits any communication by computer or other electronic device to any person or causes any person to be contacted for the sole purpose of harassing that person or his or her family is guilty of a misdemeanor, and shall be punished by a fine of not more than five hundred dollars (\$ 500).
 - R.I. GEN. LAWS § 11-59-2 (2009). Stalking prohibited. (a) Any person who: (1) harasses another person; or (2) willfully, maliciously, and repeatedly follows another person with the intent to place that person in reasonable fear of bodily injury, is guilty of the crime of stalking.
 - R.I. GEN. LAWS § 6-48-8 (2009) - Social Security protection. Person or entity, including a state or local agency, may not do any of the following:
 - (1) Intentionally communicate or otherwise make available to the general public an individual's Social Security number; (2) Print an individual's social security number on any card required for the individual to access products or services provided by the person or entity; (3) Require an individual to transmit his or her Social Security number over the Internet, unless the connection is secure or the Social Security number is encrypted; (4) Require an individual to use his or her Social Security number to access an Internet Website, unless a password or unique personal identification number or other authentication device is also required to access the Internet Website; and (5) Print an individual's social security number on any materials that are mailed to the individual.
- **Public Records**
 - R.I. GEN. LAWS § 38-2-1 (2009). The public's right to access to public records and the individual's right to dignity and privacy are both recognized to be principles of the utmost importance in a free society. The purpose of this chapter is to facilitate public access to public records. It is also the intent of this chapter to protect from disclosure information about particular individuals maintained in the

files of public bodies when disclosure would constitute an unwarranted invasion of personal privacy.

- R.I. GEN. LAWS § 38-2-2 (2009). Provides exceptions to public records trade secrets, adoption proceedings, personal information, test questions from licensing examinations, etc.
- R.I. GEN. LAWS § 38-2-6 (2009) Commercial use of public records. No person or business entity shall use information obtained from public records pursuant to this chapter to solicit for commercial purposes or to obtain a commercial advantage over the party furnishing that information to the public body.
- R.I. GEN. LAWS § 8-10-21 (2009). Records of court. The records of the family court shall be public records, except that records of hearings in matters set forth in § 14-1-5, together with stenographic notes and transcripts of those hearings, shall not be available for public inspection unless the court shall otherwise order. Notwithstanding the foregoing provisions, the records of the family court in criminal matters involving adults shall be public records.
 - The record of delinquent or wayward adjudications of juveniles may be accessed by law enforcement personnel to be used for law enforcement purposes only and shall remain otherwise confidential.
- **Motor Vehicle Records**
 - R.I. GEN. LAWS § 31-2-10 (2009). The administrator shall upon request furnish a certified abstract of the record of any operator on file fully designating the motor vehicles, if any, registered in the name of the operator, the record of all convictions of the operator of any of the provisions of this title, and the record of all the operator's involvements in accidents required to be reported.
 - R.I. GEN. LAWS § 31-35-20 (2009). Registration and license information shall be furnished to the public on request.
- **Vehicle Identification Numbers**
 - R.I. GEN. LAWS § 31-9-5 (2009). It is a felony to alter or destroy a VIN with fraudulent intent.
- **Consumer Credit**
 - R.I. GEN. LAWS § 6-13.1-21 (2009) No person or business shall request a credit report in connection with a consumer's application for credit, employment, or insurance unless a consumer is first informed that a credit report may be requested in connection with the application. Whenever credit or insurance for personal, family, or household purposes, or employment, involving a consumer is denied or the charge for that credit or insurance is increased either wholly or partly because of information contained in a credit report from a credit bureau, the user of the credit report shall advise the consumer against whom the adverse action has been taken and supply the name and address of the credit bureau making the report.
 - R.I. GEN. LAWS § 6-48-1 through -7 (2009) Consumer Empowerment And Identity Theft Prevention Act Of 2006. This act establishes the right of consumers to protect themselves from identity theft or fraud by conferring upon them the right to voluntarily place a security freeze on their credit report.
 - R.I. GEN. LAWS § 11-49.2-3 (2009) - Any state agency or person that owns, maintains or licenses computerized data that includes personal information, shall disclose any breach of the security of the system which poses a significant risk of

identity theft following discovery or notification of the breach in the security of the data to any resident of Rhode Island whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person or a person without authority, to acquire said information. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

- **Financial Records**

- R.I. GEN. LAWS § 19-9-18 (2009) - All regulated institutions shall, unless they have reason to doubt the validity of the identification, accept as sufficient identification for the cashing of checks and other banking transactions, involving municipal, state, or federal funds in amounts less than seven hundred and fifty dollars (\$ 750), duly authorized Rhode Island identification cards issued pursuant to the provision of § 3-8-6(b) or the picture identification card issued by the department of elderly affairs or an operator's or chauffer's license

- **Employee Privacy**

- R.I. GEN. LAWS § 28-6.5-1 (2009) - Employee drug testing. The employer has reasonable grounds to believe based on specific aspects of the employee's job performance and specific contemporaneous observations, capable of being articulated, concerning the employee's appearance, behavior or speech that the employee's use of controlled substances is impairing his or her ability to perform his or her job;
 - The employer keeps the results of any test confidential, except for disclosing the results of a "positive" test only to other employees with a job-related need to know, and to defend against any legal action brought by the employee against the employer.

- **Electronic Surveillance**

- R.I. GEN. LAWS § 11-35-21 (2009). Unauthorized interception, disclosure or use of wire, electronic, or oral communication. Unlawful to willfully intercept, attempt to intercept, or procure any other person to intercept or attempt to intercept, any wire, electronic, or oral communication; or use or disclose such information. Exceptions for law enforcement, communications carrier, consent from one party to the communication.
- R.I. GEN. LAWS § 12-5.1-1 (2009). Definitions.
 - "Designated offense" means the offenses of: (i) Murder, robbery, kidnapping, extortion, assault with a dangerous weapon, and assault with intent to rob or murder; (ii) Arson in the first degree, arson in the second degree, or arson in the third degree; (iii) Bribery or larceny involving the receipt of stolen property of a value of more than five hundred dollars (\$ 500); (iv) Any violation of chapter 28 of title 21 where the offense is punishable by imprisonment for more than one year; (v) Any violation of chapters 19, 47, or 51 of title 11, where the offense is punishable by imprisonment for more than one year; (vi) The lending of money at a rate of interest in violation of law; (vii) Being a fugitive from justice for any of

the offenses provided in this subdivision; and (viii) Conspiracy to commit any of the offenses provided in this subdivision.

- "Electronic communication" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system, but does not include: (i) Any wire or oral communication; (ii) Any communication made through a tone-only paging device; or (iii) Any communication from a tracking device.
 - R.I. GEN. LAWS § 12-5.1-2 (2009). Application for orders. Attorney general or assistant attorney general makes the order.
 - R.I. GEN. LAWS § 12-5.1-3 (2009). Where application may be made
 - R.I. GEN. LAWS § 12-5.1-4 (2009). Issuance of orders
 - R.I. GEN. LAWS § 12-5.1-5 (2009). Form and content of orders
 - R.I. GEN. LAWS § 12-5.1-6 (2009). Approval of interception of wire, electronic, or oral communication. Requires probable cause.
 - R.I. GEN. LAWS § 12-5.1-7 (2009). Execution of orders
 - R.I. GEN. LAWS § 12-5.1-8 (2009). Maintenance and custody of records
 - R.I. GEN. LAWS § 12-5.1-9 (2009). Return of inventory.
 - (a) Within a reasonable time but not later than ninety (90) days after the termination of the period of the order or of extensions of the order, the presiding justice of the superior court shall cause to be served on the person named in the order or application, and any other parties to the intercepted communications that the presiding justice of the superior court may determine in his or her direction to be in the interest of justice, an inventory of the interception
 - R.I. GEN. LAWS § 12-5.1-10 (2009). Disclosure and use of intercepted wire or oral communications
 - R.I. GEN. LAWS § 12-5.1-11 (2009). Notice of intention
 - R.I. GEN. LAWS § 12-5.1-12 (2009). Suppression of evidence
 - R.I. GEN. LAWS § 12-5.1-13 (2009). Civil remedy
 - R.I. GEN. LAWS § 12-5.1-14 (2009). Annual report of interceptions to the general assembly
 - R.I. GEN. LAWS § 12-5.1-15 (2009). Conformity to the law of the United States
 - R.I. GEN. LAWS § 12-5.1-16 (2009). Severability. If any provision of this chapter or its application to any person or circumstances is held invalid, its invalidity shall not affect other provisions or applications of the chapter which can be given effect without the invalid provision or application, and to this end the provisions of this chapter are declared to be severable.
- **Computer Statutes**
 - R.I. GEN. LAWS § 11-52-2 (2009). Access to computer for fraudulent purposes. Whoever directly or indirectly accesses or causes to be accessed any computer, computer system, or computer network for the purpose of: (1) devising or executing any scheme or artifice to defraud; (2) obtaining money, property, or services by means of false or fraudulent pretenses, representations, or promises; or (3) damaging, destroying, altering, deleting, or removing any program or data contained in it in connection with any scheme or artifice to defraud, shall be guilty of a felony.

- R.I. GEN. LAWS § 11-52-3 (2009). Intentional access, alteration, damage, or destruction. Whoever, intentionally, without authorization, and for fraudulent or other illegal purposes, directly or indirectly, accesses, alters, damages, or destroys any computer, computer system, computer network, computer software, computer program, or data contained in a computer, computer system, computer program, or computer network shall be guilty of a felony
- R.I. GEN. LAWS § 11-52-4.1 (2009). Computer trespass. Unlawful for any person to use a computer or computer network without authority and with the intent to: 1) remove, halt, or otherwise disable any computer data, computer programs, or computer software from a computer or computer network; (2) cause a computer to malfunction regardless of how long the malfunction persists; (3) Alter or erase any computer data, computer programs, or computer software; (4) Effect the creation or alteration of a financial instrument or of an electronic transfer of funds; (5) Cause physical injury to the property of another; (6) Make or cause to be made an unauthorized copy of software or data; (7) Forge e-mail header information to send unsolicited bulk electronic mail; (8) to sell software that forges email headers.
- R.I. GEN. LAWS § 11-52-7 (2009). Use of false information. (a) Whoever intentionally or knowingly makes a transmission of false data for the purpose of submitting a claim for payment, or makes, presents, or uses or causes to be made, presented, or used any data for the purpose of submitting a claim for payment with knowledge of its falsity and with knowledge that it will be used for any claim for payment, shall be guilty of a felony. (b) Whoever intentionally or knowingly: (1) makes a transmission of false data; or (2) makes, presents or uses or causes to be made, presented or used any data for any other purpose with knowledge of its falsity, shall be guilty of a misdemeanor
- R.I. GEN. LAWS § 11-52-8. Tampering with computer source documents. (a) Whoever intentionally or knowingly conceals, destroys, or alters or intentionally or knowingly causes another to conceal, destroy, or alter any computer source document used for a computer, computer program, computer system, or computer network, when the computer source document is required to be kept by law, shall be guilty of a misdemeanor. And if the intent is to obstruct an official civil or criminal investigation, the person is guilty of a felony.
- **Common Law**
 - *See* R.I. GEN. LAWS § 9-1-28.1 (2009) - codifying the four strands of the common law tort of the invasion of privacy.

SOUTH CAROLINA PRIVACY LAW

- **State Constitutional Privacy Rights**
 - **Express**
 - S.C. CONST. art. I, § 10 (2007) - Searches and seizures; invasions of privacy. The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures and unreasonable invasions of privacy shall not be violated . . .
 - **Implied**
 - S.C. CONST. art. I, § 12 (2007) Double jeopardy; self incrimination. No person shall be subject for the same offense to be twice put in jeopardy of life or liberty, nor shall any person be compelled in any criminal case to be a witness against himself.
- **Search and Seizure**
 - S.C. CONST. art. I, § 10 (2007) protects against unreasonable search and seizure
 - **Auto Exception**
 - State v. Cox, 351 S.E.2d 570 (S.C. 1986)
 - **Open Fields**
 - Not recognized or discussed.
 - **Plain View**
 - State v. Culbreath, 387 S.E.2d 255 (S.C. 1990)
- **Statutory Privacy Rights**
 - S.C. CODE ANN. § 16-3-1700 (2007)"Stalking" means a pattern of words, whether verbal, written, or electronic, or a pattern of conduct that serves no legitimate purpose and is intended to cause and does cause a targeted person and would cause a reasonable person in the targeted person's position to fear: (1) death of the person or a member of his family; (2) assault upon the person or a member of his family; (3) bodily injury to the person or a member of his family; (4) criminal sexual contact on the person or a member of his family; (5) kidnapping of the person or a member of his family; or (6) damage to the property of the person or a member of his family.
 - S.C. CODE ANN. § 44-117-10 through -30 (2007). Prescription Information Privacy Act. Prescription drug information transfer and receipt; exceptions. No patient prescription drug information may be transferred or received by a person without the written consent of the patient or a person authorized by law to act on behalf of the patient. The exceptions include certain transmissions between licensed practitioners, and informational requests about prescriptions from consumers.
 - S.C. CODE ANN. § 44-117-310 through -380 (2007) - Electronic Prescription Processing Act. Due diligence requirements to prevent unauthorized viewing of patient prescription information.
 - S.C. CODE ANN. § 44-115-10 through -150 (2007). Physicians' Patient Records Act. Patients and Physicians rights concerning transfer and viewing of patient information and records, and custody of records. Also transferring records with the consent of the patient cannot be withheld from a patient for unpaid bills
- **Public Records**

- S.C. CODE ANN. § 30-4-15 (2007). Findings and purpose The General Assembly finds that it is vital in a democratic society that public business be performed in an open and public manner so that citizens shall be advised of the performance of public officials and of the decisions that are reached in public activity and in the formulation of public policy. Toward this end, provisions of this chapter must be construed so as to make it possible for citizens, or their representatives, to learn and report fully the activities of their public officials at a minimum cost or delay to the persons seeking access to public documents or meetings.
- S.C. CODE ANN. § 30-4-40 (2007) Lists exemptions from disclosure in public records including personal nature information, trade secrets, records of law enforcement disclosing informants, autopsy videos, etc.
- S.C. CODE ANN. § 30-4-50 (2007) No information contained in a police incident report or in an employee salary schedule revealed in response to a request pursuant to this chapter may be utilized for commercial solicitation.
 - Also, the home addresses and home telephone numbers of employees and officers of public bodies revealed in response to a request pursuant to this chapter may not be utilized for commercial solicitation. However, this provision must not be interpreted to restrict access by the public and press to information contained in public records.
- S.C. CODE ANN. § 60-4-10 (2007) - library user records are confidential.
- **Motor Vehicle Records**
 - S.C. CODE ANN. § 30-4-160 (2007). Sale of Social Security number or driver's license photograph or signature. (A) This chapter does not allow the Department of Motor Vehicles to sell, provide, or otherwise furnish to a private party Social Security numbers in its records, copies of photographs, or signatures, whether digitized or not, taken for the purpose of a driver's license or personal identification card. (B) Photographs, signatures, and digitized images from a driver's license or personal identification card are not public records.
 - S.C. CODE ANN. § 30-4-165 (2007). Privacy of driver's license information. (A) The Department of Motor Vehicles may not sell, provide, or furnish to a private party a person's height, weight, race, Social Security number, photograph, or signature in any form that has been compiled for the purpose of issuing the person a driver's license or special identification card. The department shall not release to a private party any part of the record of a person less than fifteen years of age who has applied for or has been issued a special identification card. (B) A person's height, weight, race, photograph, signature, and digitized image contained in his driver's license or special identification card record are not public records. (C) Notwithstanding another provision of law, a private person or private entity shall not use an electronically-stored version of a person's photograph, Social Security number, height, weight, race, or signature for any purpose, when the electronically-stored information was obtained from a driver's license record.
 - S.C. CODE ANN. § 56-9-330 (2007) The Department of Motor Vehicles, upon request, and the payment of a fee shall furnish any person a certified abstract of the operating record of any person subject to the provisions of this chapter, which abstract must also fully designate the motor vehicles, if any, registered in the name of that person, and, if there is no record of any conviction of that person for

violating any laws relating to the operation of a motor vehicle or of any injury or damage caused by that person, the department shall so certify. The department, upon request and the payment of a reasonable fee, shall furnish a monthly listing by magnetic or other electronic media of all drivers' license numbers that had driving violations posted on their records during the previous month. These abstracts are not admissible as evidence in any action for damages or criminal proceedings arising out of motor vehicle accidents.

- S.C. CODE ANN. § 56-3-2450 (2007) Certified copies of Department of Motor Vehicle records; use thereof as evidence. The Department of Motor Vehicles and such officers and employees of the Department as the Department may designate may prepare and deliver upon request a certified copy of any record of the Department relating to the registration and licensing of any vehicle, and every such certified copy shall be admissible in any proceeding in any court in like manner as the original thereof.
- **Vehicle Identification Numbers**
 - S.C. CODE ANN. § 56-29-30 (2007) - A person who knowingly alters, counterfeits, defaces, destroys, disguises, falsifies, forges, obliterates, or knowingly removes a vehicle identification number, or causes any of the above to be done, with the intent to misrepresent the identity or prevent the identification of a motor vehicle or motor vehicle part, is guilty of a felony and, upon conviction, must be imprisoned not more than five years or fined not less than five thousand nor more than ten thousand dollars, or both.
 - S.C. CODE ANN. § 56-29-40 (2007) - Violation of altering the VIN can lead to seizure by the police if there is a warrant or consent to search. Any tool, implement, or instrumentality, including but not limited to a motor vehicle or motor vehicle part, used or possessed in connection with any violation of § 56-29-30 may be seized by a member of a state or local law enforcement agency upon process issued by any court of competent jurisdiction.
- **Consumer Credit**
 - S.C. CODE ANN. § 37-6-605 (2007) - Consumer protection advocates have access to confidential consumer materials including state and insurance records if a proprietary agreement to keep records confidential is signed.
 - Security Breaches of personal information and Security Freeze.
 - Not codified law yet, BUT:
 - S. 453, 117st Sess. (S.C. 2008), *available at* 2007 S.C. R. 202
 - Financial Identity Fraud And Identity Theft Protection Act
- **Financial Records**
 - S.C. CODE ANN. § 34-28-410 (2007) - books and records of savings associations are confidential. May release with customer consent or if compelled by subpoena or court order.
 - S.C. CODE ANN. § 37-3-505 (2007) - Annual report of a bank is private, but acceptable to publish as a composite.
- **Employee Privacy**
 - S.C. CODE ANN. § 41-1-15 (2007) Establishment of drug prevention program in workplace; confidentiality of information concerning test results.
- **Electronic Surveillance**

- S.C. CODE ANN. § 16-17-470 (2007) Eavesdropping, peeping, voyeurism. Unlawful and is misdemeanor.
- S.C. CODE ANN. § 17-29-10 (2007) Definitions for pen register and trap and trace.
- S.C. CODE ANN. § 17-29-20 (2007) Installation of pen register or trap and trace device prohibited
- S.C. CODE ANN. § 17-29-30 (2007) Certain officials may make application for order authorizing or approving installation and use of pen register or trap and trace device
- S.C. CODE ANN. § 17-29-40 (2007) Issuance of court order authorizing installation of pen register or trap and trace device
- S.C. CODE ANN. § 17-29-50 (2007) Rights and duties of provider of wire or electronic communication service, landlord, etc. Upon the request of the attorney or an officer of a law enforcement agency authorized to install and use a pen register under this chapter, a provider of wire or electronic communication service, landlord, custodian, or other person shall furnish the law enforcement officer forthwith all information, facilities, and technical assistance necessary to accomplish the installation of the pen register unobtrusively and with a minimum of interference with the services that the person so ordered by the court accords the party with respect to whom the installation and use is to take place, if the assistance is directed by a court order
- S.C. CODE ANN. § 17-30-10 (2007) Interception of wire, electronic or oral communications authorized. Only as stated in this chapter.
- S.C. CODE ANN. § 17-30-15 (2007) Definitions. "Electronic communication" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, photooptical system, or any other device that affects intrastate, interstate, or foreign commerce, but does not include: (a) any wire or oral communication; (b) any communication made through a tone-only paging device; (c) any communication from an electronic or mechanical device which permits the tracking of the movement of a person or an object; or (d) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds.
- S.C. CODE ANN. § 17-30-20 (2007) Prohibited acts. Unless otherwise stated, unlawful to intentionally intercept, attempt to intercept, or procure any other person to intercept or attempt to intercept any wire, oral, or electronic communication or use or disclose an interception
- S.C. CODE ANN. § 17-30-25 (2007) Interception and disclosure of information by provider of wire or electronic communications service; exceptions where authorized by law
- S.C. CODE ANN. § 17-30-30 (2007) Interception by employee of Federal Communications Commission, by person acting under color of law, and where party has given prior consent is acceptable.
- S.C. CODE ANN. § 17-30-35 (2007) Other lawful interceptions of electronic communications by the public include radio communication, public frequencies, satellite transmission that isn't encrypted, etc.

- S.C. CODE ANN. § 17-30-40 (2007) Disclosure of content of communication by provider of electronic communication service
- S.C. CODE ANN. § 17-30-45 (2007) Use of pen register or trap and trace device
- S.C. CODE ANN. § 17-30-55 (2007) Mailing or manufacturing devices for unlawful interception of wire, oral or electronic communications.
- S.C. CODE ANN. § 17-30-60 (2007). Seizure and forfeiture.
- S.C. CODE ANN. § 17-30-65 (2007). Admissibility of contents of, or evidence derived from, intercepted communications; contents as public record.
- S.C. CODE ANN. § 17-30-70 (2007). Orders authorizing interception; application process; agencies and individuals authorized to conduct. Requires probable cause the intercepted person committed or is going to commit certain offenses enumerated here including murder, arson, kidnapping, etc.
- S.C. CODE ANN. § 17-30-75 (2007). Disclosure of content of intercepted communication.
- S.C. CODE ANN. § 17-30-80 (2007). Application for interception order; contents; establishing allegations of fact; additional evidence
- S.C. CODE ANN. § 17-30-85 (2007). Information to be specified in order.
- S.C. CODE ANN. § 17-30-90 (2007). Duration and termination of interception; reports to authorizing judge.
- S.C. CODE ANN. § 17-30-95 (2007). Interception prior to obtaining order; oral notification of judge in emergency.
- S.C. CODE ANN. § 17-30-100 (2007). Recording, sealing, custody and destruction of intercepted communications; notification. Within a reasonable time but not later than ninety days after the termination of the period of an order or extensions of the order, the issuing or denying judge must cause to be served on the persons named in the order or the application, and those other parties to intercepted communications an inventory
- S.C. CODE ANN. § 17-30-105 (2007). Providing copies of intercepted communications to parties as prerequisite to receiving evidence; ...
- S.C. CODE ANN. § 17-30-110 (2007). Pretrial motion to suppress; grounds; appeals by State; exclusive remedy.
- S.C. CODE ANN. § 17-30-115 (2007). Circumstance under which requirement that facilities from which or place of interception be specified
- S.C. CODE ANN. § 17-30-120 (2007). Determination of facility as prerequisite to interception where facility not specified in order
- S.C. CODE ANN. § 17-30-130 (2007). Reporting intercepted communications.
- S.C. CODE ANN. § 17-30-135 (2007). Civil action for wrongful interceptions.
- S.C. CODE ANN. § 17-30-140 (2007). Mobile tracking devices; contents of application for order authorizing use; standards for installation. The Attorney General or any solicitor may make application to a judge of competent jurisdiction for an order authorizing or approving the installation and use of a mobile tracking device by the South Carolina Law Enforcement Division or any law enforcement entity of a political subdivision of this State.
- S.C. CODE ANN. § 17-30-145 (2007). Surveillance training requirements. Any SLED agent or an individual operating under a contract with the South Carolina Law Enforcement Division authorized under the provisions of this chapter to

intercept wire, oral, or electronic communications must undergo training by SLED in conducting such surveillance with emphasis on techniques for minimizing the interception of communications that fall outside of the communications subject to interception pursuant to the provisions of this chapter.

- **Computer Statutes**

- S.C. CODE ANN. § 16-16-20 (2007). Computer crime offenses; penalties. (1) It is unlawful for a person to willfully, knowingly, maliciously, and without authorization or for an unauthorized purpose to: (a) directly or indirectly access or cause to be accessed a computer, computer system, or computer network for the purpose of: (i) devising or executing a scheme or artifice to defraud; (ii) obtaining money, property, or services by means of false or fraudulent pretenses, representations, promises; or (iii) committing any other crime. (b) alter, damage, destroy, or modify a computer, computer system, computer network, computer software, computer program, or data contained in that computer, computer system, computer program, or computer network or introduce a computer contaminant into that computer, computer system, computer program, or computer network.

- **Common Law**

- Erickson v. Jones St. Publ., 629 S.E.2d 653 (S.C. 2006) cited to the following cases to describe the state of the law:
 - Snakenberg v. Hartford Cas. Ins. Co., 383 S.E.2d 2 (S.C. Ct. App. 1989) - identifying three causes of action which may arise under rubric of invasion of privacy: wrongful appropriation of personality, wrongful publicizing of private affairs, and wrongful intrusion into private affairs
 - Brown v. Pearson, 483 S.E.2d 477 (S.C. Ct. App. 1997) - noting no South Carolina case has recognized a "false light" invasion of privacy claim

SOUTH DAKOTA PRIVACY LAW

- **State Constitutional Privacy Rights**
 - none
- **Search and Seizure**
 - S.D. CONST. art. VI, § 11 - protects against unreasonable search and seizure.
 - **Auto Exception**
 - State v. Weaver, 649 S.E.2d 479 (S.D. 2007).
 - **Open Fields**
 - State v. Frey, 440 N.W.2d 721 (S.D. 1989).
 - **Plain View**
 - State v. Gardner, 440 N.W.2d 721 (S.D. 1989).
 - *See also* State v. Lodermeier, 481 N.W.2d 614 (S.D. 1990) (describing the reasonable expectation of privacy in the curtilage of the home and other factors such as openness to public view).
- **Statutory Privacy Rights**
 - S.D. CODIFIED LAWS § 22-21-3 (2009). Unlawful peeking -- Penalty
 - S.D. CODIFIED LAWS § 22-21-4 (2009). Taking pictures without consent -- Violation is misdemeanor
 - S.D. CODIFIED LAWS § 22-19A-1 (2009). Stalking. No person may: (1) Willfully, maliciously, and repeatedly follow or harass another person; (2) Make a credible threat to another person with the intent to place that person in reasonable fear of death or great bodily injury; or (3) Willfully, maliciously, and repeatedly harass another person by means of any verbal, electronic, digital media, mechanical, telegraphic, or written communication. A violation of this section constitutes the crime of stalking.
 - S.D. CODIFIED LAWS § 22-40-8 (2009) Identity Theft Crimes. If any person, without the authorization or permission of another person and with the intent to deceive or defraud: (1) Obtains, possesses, transfers, uses, attempts to obtain, or records identifying information not lawfully issued for that person's use; or (2) Accesses or attempts to access the financial resources of that person through the use of identifying information; such person commits the crime of identity theft.
- **Individually Identifiable Government Records**
 - S.D. CODIFIED LAWS § 22-45-9 (2009) The attorney general and the state Medicaid fraud control unit, upon reasonable request, and the grand jury, upon subpoena therefore, shall have full access to all records held by a provider or by any other person on his behalf, which could be relevant in any manner to the determination of the existence of offenses under §§ 22-45-2 to 22-45-6, inclusive, or related crimes, or the existence of patient abuse, mistreatment or neglect, or the theft of patient funds.
- **Public Records**
 - S.D. CODIFIED LAWS § 28-1-51 (2009) - The secretary of Social Services may adopt reasonable and necessary rules to protect records and confidential information required by statutory law to be held confidential.
 - S.D. CODIFIED LAWS § 1-27-1 (2009) If the keeping of a record, or the preservation of a document or other instrument is required of an officer or public servant under any statute of this state, the officer or public servant shall keep the

record, document, or other instrument available and open to inspection by any person during normal business hours. Any employment examination or performance appraisal record maintained by the Bureau of Personnel is excluded from this requirement.

- Any subscription or license holder list maintained by the Department of Game, Fish and Parks may be made available to the public for a reasonable fee. State agencies are exempt from payment of this fee for approved state use. The Game, Fish and Parks Commission may promulgate rules pursuant to chapter 1-26 to establish criteria for the sale and to establish the fee for the sale of such lists.
 - Any list released or distributed under this section may not be resold or redistributed.
 - S.D. CODIFIED LAWS § 1-27-3 (2009) Public access statute shall not apply to such records as are specifically enjoined to be held confidential or secret by the laws requiring them to be so kept.
- **Motor Vehicle Records**
 - S.D. CODIFIED LAWS § 1-27-1 (2009) Any automobile liability insurer licensed in the state, or its certified authorized agent, may have access to the name and address of any person licensed or permitted to drive a motor vehicle solely for the purpose of verifying insurance applicant and policyholder information.
 - S.D. CODIFIED LAWS § 32-3-30.2 (2009) The department may upon written request and payment of a five dollar fee furnish a person a certified abstract of the title history which shall include the damage disclosure statements of any motor vehicle, trailer or semitrailer registered under the provisions of this chapter. The abstract may include all documents filed with the department to establish the title history of the vehicle.
 - S.D. CODIFIED LAWS § 32-5-90.1 (2009). Access to registration information. The department may upon written request and payment of a two dollar fee furnish a person a certified abstract regarding registration information of any motor vehicle, trailer or semitrailer registered under the provisions of this chapter.
 - S.D. CODIFIED LAWS § 32-12-61 (2009) - Records of conviction and accident reports are public record.
 - S.D. CODIFIED LAWS 32-12-17.8 (2009). Encrypted license information -- Medical condition. If a bar code, or other means by which information may be retrieved electronically, is placed on a license pursuant to § 32-12-17.10, the secretary of the Department of Public Safety may include information identifying the licensee's blood type, medical condition, allergies, medications, or other medical alert data, if the licensee requests such information to be included. Before such information may be included, the licensee shall submit a document clearly identifying this information to the department and the document shall be signed by the licensee and the licensee's physician.
 - S.D. CODIFIED LAWS § 32-12-17.10 (2009) Contents of license and permit. If a barcode, or other means by which information may be retrieved electronically, is placed on the license, the data field may contain the information printed on the license. No barcode, or other means by which information may be retrieved electronically, may contain the licensee's Social Security number.

- **Vehicle Identification Numbers**
 - S.D. CODIFIED LAWS § 32-4-9 (2009) - No person may intentionally remove, deface, alter, destroy, cover, or obscure any vehicle identification number or other distinguishing number of a motor vehicle or trailer or any part thereof in this state, without written authorization from the Department of Revenue and Regulation, nor may any person place or stamp in place of the original manufacturer's serial, motor, or other number or mark upon a vehicle, any number except one assigned by the department under the provisions of chapter 32-3 or authorized agency of another state.
- **Consumer Credit**
 - S.D. CODIFIED LAWS § 54-15-3 (2009) Any person who is a victim of identity theft and has submitted a valid police report to a consumer reporting agency may elect to place a security freeze on that person's report by making a request in writing by certified mail to a consumer reporting agency at an address designated by the consumer reporting agency to receive such requests. This section does not prevent a consumer reporting agency from advising a third party that a security freeze is in effect with respect to the consumer's credit report.
- **Financial Records**
 - S.D. CODIFIED LAWS § 13-63-26 (2009) § 13-63-26 (2009). Higher Education Savings Plan. Account holder and beneficiary identifying information confidential. Any Social Security numbers, taxpayer identification numbers, addresses, or telephone numbers of account holders and designated beneficiaries that come into the possession of the council are confidential, are not public records, and may not be released by the council except as required by federal law.
 - S.D. CODIFIED LAWS § 25-7A-56.9 (2009) The department shall enter into agreements with any financial institution conducting business within the state whereby the financial institution shall, on a quarterly basis, provide to the department the name, record address, Social Security number, or other taxpayer identification number, and other identifying information requested by the department for each obligor who owes past-due child support, and who maintains an account at the financial institution. Every financial institution shall also comply with any lien, levy, or order for withholding of income issued by the department against any account.
- **Employee Privacy**
- **Electronic Surveillance**
 - S.D. CODIFIED LAWS § 22-21-1 (2009) Trespassing with intent to eavesdrop-- Installation or use of unauthorized eavesdropping device. Trespasses on property with intent to subject anyone to eavesdropping or other surveillance in a private place; or installs in any private place, without the consent of the person or persons entitled to privacy there, any device for observing, photographing, recording, amplifying or broadcasting sounds or events in such place, or uses any such unauthorized installation is guilty of a misdemeanor.
 - S.D. CODIFIED LAWS § 23A-35A-1 (2009) Definition of terms. Doesn't specifically include electronic communication
 - S.D. CODIFIED LAWS § 23A-35A-2 (2009) Offenses for which order of interception of communications may be granted. Orders authorizing or approving

the interception of wire or oral communications may be granted, subject to the provisions of this chapter when the interception may provide or has provided evidence of the commission of, or of any conspiracy to commit, the following offenses as otherwise defined by the laws of this state: murder; kidnapping; gambling; robbery; bribery; theft; unlawful use of a computer; unauthorized manufacturing, distribution or counterfeiting of controlled substances or marijuana; and rape.

- S.D. CODIFIED LAWS § 23A-35A-3 (2009) Authority of attorney general or state's attorney to apply for order for interception of communications
- S.D. CODIFIED LAWS § 23A-35A-4 (2009) Application to intercept communications--form and contents
- S.D. CODIFIED LAWS § 23A-35A-5 (2009) Circuit judge to authorize interception
- S.D. CODIFIED LAWS § 23A-35A-6 (2009) Ex parte order authorizing wiretapping or eavesdropping--Probable cause required for entry
- S.D. CODIFIED LAWS § 23A-35A-7 (2009) Order to specify certain particulars
- S.D. CODIFIED LAWS § 23A-35A-8 (2009) Cooperation and technical assistance required of carriers, landlords, and others--Compensation
- S.D. CODIFIED LAWS § 23A-35A-9 (2009) Progress reports to issuing judge
- S.D. CODIFIED LAWS § 23A-35A-10 (2009) Lifespan of order--Extensions on application therefore-- Length of extension. Can't be longer than 30 days of interception
- S.D. CODIFIED LAWS § 23A-35A-11 (2009). Authority for eavesdropping -- Copy and retention of orders and papers
- S.D. CODIFIED LAWS § 23A-35A-12 (2009). Sealing of applications and orders by court -- Custody -- Disclosure
- S.D. CODIFIED LAWS § 23A-35A-13 (2009). Recording of intercepted communications -- Sealing of recordings
- S.D. CODIFIED LAWS § 23A-35A-14 (2009). Disclosures -- Inventory -- Inspection -- Postponing notice. Within ninety days after an application under § 23A-35A-3 is denied, or the period of an order or extensions thereof expires, the issuing or denying judge shall cause the persons named in the order or application and such other parties to intercepted communications as he may determine the interests of justice require, to be served with an inventory. Notification can be postponed by the judge for good cause.
- S.D. CODIFIED LAWS § 23A-35A-15 (2009). Disclosure of contents of intercepted communication
- S.D. CODIFIED LAWS § 23A-35A-16 (2009). Appropriate use of intercepted communication
- S.D. CODIFIED LAWS § 23A-35A-17 (2009). Disclosure of contents of intercepted communication in court or grand jury
- S.D. CODIFIED LAWS § 23A-35A-18 (2009). Interception of communications relating to offenses not specified in order -- Use of contents
- S.D. CODIFIED LAWS § 23A-35A-19 (2009). Privileged communications -- No loss of privilege
- S.D. CODIFIED LAWS § 23A-35A-22 (2009). Use of pen register or trap and trace device prohibited -- Violation as misdemeanor

- S.D. CODIFIED LAWS § 23A-35A-28 (2009). Time limitation on use of pen register or trap and trace device -- Extension
- S.D. CODIFIED LAWS § 23A-35A-29 (2009). Order sealed -- Prohibition on disclosure of existence of pen register or trap and trace device
- S.D. CODIFIED LAWS § 23A-35A-30 (2009). Required assistance in installation of pen register
- S.D. CODIFIED LAWS § 23A-35A-31 (2009). Required assistance for installation of trap and trace device -- Results given to law enforcement officer
- S.D. CODIFIED LAWS § 23A-35A-32 (2009). Compensation for assistance. A provider of a wire or electronic communication service, landlord, custodian or other person who furnishes facilities or technical assistance pursuant to this section shall be reasonably compensated for the reasonable expenses incurred in providing the facilities and assistance.
- S.D. CODIFIED LAWS § 23A-35A-33 (2009). Immunity for persons providing assistance
- **Computer Statutes**
 - S.D. CODIFIED LAWS § 43-43B-1 (2009). Unlawful use of a computer. Knowingly obtains the use of, accesses or exceeds authorized access to, a computer system; knowingly disrupts, denies, or inhibits access to software or data without the consent of the owner; or knowingly destroys or disables a computer system is a crime.
- **Common Law**
 - Montgomery Ward v. Shope, 286 N.W.2d 806 (S.D. 1979). Accepts the Restatement of Torts definitions for the four invasions of privacy torts - appropriation, intrusion, false light and disclosure.

TENNESSEE PRIVACY LAW

- **State Constitutional Privacy Rights**
 - **Express** - none
 - **Implied** - through TENN. CONST. art. I, § 7 (2009). Protection against unreasonable search and seizure.
- **Search and Seizure**
 - TENN. CONST. art. I, § 7 (2009). Protection against unreasonable search and seizure. Warrant requirement.
 - **Auto Exception**
 - State v. Sherwood, 2007 Tenn. Crim. App. LEXIS 58 (Tenn. Crim. App. 2007) - One such exception to the warrant requirement is the "automobile exception." Under the automobile exception, an automobile may be searched without a warrant if an officer has probable cause to believe that the vehicle contains contraband and if exigent circumstances require an immediate search. The rationale for the automobile exception is twofold: (1) the impracticability of obtaining a search warrant in light of the inherent mobility of an automobile; and (2) the reduced expectation of privacy with respect to one's automobile. If the police have probable cause to believe that an automobile contains contraband, the officers may either seize the vehicle and then obtain a warrant or they may search the vehicle immediately.
 - State v. Leveye, 796 S.W.2d 948 (Tenn. 1990) - recognized the automobile exception. A lawfully parked vehicle equates with a vehicle that is stopped in transit on a public way and relies upon the inherent mobility of a vehicle to create a conclusive presumption of exigency.
 - Distinctions may be made in future cases between vehicles parked in public places and elsewhere, or return to some particularized restriction on mobility, but at the very least a warrantless search of a vehicle parked in a public place, after a recent crime, is authorized, providing probable cause to believe the vehicle contains contraband, without any actual likelihood that the risk of delay to obtain a warrant is high.
 - The court held that whether considering a lawfully parked car or a car stopped in transit, a car's inherent mobility created a conclusive presumption of exigency. The court agreed with the appellate court's determination that the search was lawful because: 1) there was probable cause to believe that unrecovered stolen property was still in the car as defendant had been seen leaving the car with some property, but other stolen property had not been accounted for; and 2) there was evidence that another person might be an accomplice or could be in a position to move the car or its contents.
 - **Open Fields**
 - State v. Jennette, 706 S.W.2d 614 (Tenn. 1986) - Did not find it necessary in this decision to overrule the *Lakin* case, because it simply presented facts different from those here. It was recognized in that decision that the

individual, or in the case of a minor, without the prior effective consent of the minor's parent or guardian, if the photograph: (1) Would offend or embarrass an ordinary person if such person appeared in the photograph; and (2) Was taken for the purpose of sexual arousal or gratification of the defendant.

- TENN. CODE ANN. § 39-13-607 (2009) - Observation without consent. It is an offense for a person to knowingly spy upon, observe or otherwise view an individual, when the individual is in a place where there is a reasonable expectation of privacy, without the prior effective consent of the individual, if the viewing: (1) Would offend or embarrass an ordinary person if the person knew the person was being viewed; and (2) Was for the purpose of sexual arousal or gratification of the defendant.
- **Individually Identifiable Government Records**
 - TENN. CODE ANN. § 37-1-154 (2009) - Law enforcement records -- Inspection limited. The law enforcement records and files shall not be open to public inspection or their contents disclosed to the public if the records are for juveniles. Some exceptions apply.
- **Public Records**
 - TENN. CODE ANN. § 10-7-121; -123 (2009) - It is okay for agencies to keep records on electronic mediums and may allow public inspection as long as the record is not confidential.
 - TENN. CODE ANN. § 10-7-503 (2009) - Records open to public inspection. All state, county and municipal records shall be open to public inspection. All law enforcement personnel records shall be open for inspection, but the custodian will tell the law enforcement person that his/her records were inspected. Information made confidential by this chapter shall be redacted whenever possible. All records of any association or nonprofit corporation are open for inspection with some exceptions. All contingency plans of law enforcement agencies that deal with bomb threats and the like are not open for inspection. All records, employment applications, credentials and similar documents for a search for public school superintendent or another chief public admin officer are available for review.
 - TENN. CODE ANN. § 10-7-504 (2009) - Confidential Records. Confidential information described in this section is either redacted or the entire record is inaccessible. Includes medical records, TN Bureau of Investigation criminal records including stolen hand guns and vehicles or vehicle parts, National Guard personnel records, military staff studies and investigations, records of students in public educational institutions, certain books related to a proceeding and work product of the attorney general, state agency records regarding pending property transactions, proposals for gov contracts before the bids are decided, certain animal tracking data kept by the state veterinarian, personal information contained in motor vehicle records, mental health records kept for law enforcement professionals, all riot and emergency plans for state penitentiaries, information for rape crises centers, credit card numbers of persons doing business with the state or political subdivision thereof and any related personal identification numbers, private records of any utility, records that would allow a person to identify areas of structural or operational vulnerability of a utility service provider, personal records, Social Security numbers, or information of any state, county, municipal

or other public employee, or of any law enforcement officer, identities of executioners.

- Notwithstanding any provision of the law to the contrary, any confidential public record in existence more than seventy (70) years shall be open for public inspection by any person unless disclosure of the record is specifically prohibited or restricted by federal law or unless the record is a record of services for a person for mental illness or mental retardation.
 - TENN. CODE ANN. § 10-7-506 (2009) - Public records having commercial value. The agency may charge a fee for copies of these, and if from the county assessor of property, the property owner will be notified. A record having commercial value is a record requested for any purpose other than: (A) A non-business use by an individual; and (B) A news gathering use by the news media.
 - TENN. CODE ANN. § 10-7-515 (2009) - Must redact Social Security number on any agency-prepared documents, requests can be made to remove the number from electronic database.
 - TENN. CODE ANN. § 10-8-102 (2009) - Library records may not be inspected unless a court gives permission or the user gives permission.
- **Motor Vehicle Records**
 - TENN. CODE ANN. § 10-7-507 (2009) - Traffic violations of TN and any other state of a TN resident are available to be inspected.
 - TENN. CODE ANN. § 55-50-409 (2009) - Notification of traffic violations -- Furnishing driving record information. The department shall notify the driver licensing authority in the licensing state of the conviction, and the commercial driver's license information system for any violations of a holder of a commercial driver's license.
 - Notwithstanding any other law in this state, the department shall furnish full information regarding the driving record of any person to: The driver's license administrator of any other state, or province or territory of Canada, requesting that information; (2) The commercial driver's license information system; and (3) Any employer or prospective employer upon request and payment of a fee of five dollars (\$5.00).
 - TENN. CODE ANN. § 55-25-101 through -112 (2009) - Uniform Motor Vehicle Records Disclosure Act. Protect the interest of individuals in their personal privacy of prohibiting the disclosure and use of personal information contained in their motor vehicle records, except as authorized by these individuals or by law.
 - The department, and any officer, employee, agent or contractor thereof, shall not disclose personal information about any person obtained by the department in connection with a motor vehicle record.
 - There are exceptions for safety, environmental or federal compliance purposes. Also in research activities, and for use in producing statistical reports, so long as the personal information is not published, redisclosed, or used to contact individuals
 - TENN. CODE ANN. § 55-10-114 (2009) - Public inspection of reports relating to accidents. All accident reports made by any person or by garages shall be without prejudice to the individual so reporting, and shall be for the confidential use of the department or other state agencies having use of the records for accident

prevention purposes, or for the administration of the laws of this state. The department may disclose the identity of a person involved in an accident when the identity is not otherwise known or when the person denies having been present at the accident.

- **Vehicle Identification Numbers**

- TENN. CODE ANN. § 55-5-106 (2009) - All new motor vehicles, new motor vehicle engines and transmissions, new freight vehicles, and new livestock trailers, as specified herein, and manufactured in this state and intended for sale to the general public within this state, shall be required to have placed upon them a vehicle identification number.
- TENN. CODE ANN. § 55-5-111 (2009) - Any person who knowingly buys, receives, disposes of, sells, offers for sale, or has in that person's possession any motor vehicle, engine or transmission removed from a motor vehicle, from which the manufacturer's serial, engine or transmission number commits a felony.
- TENN. CODE ANN. § 55-5-204 (2009) - Acceptable for law enforcement to seize a vehicle with the VIN removed or any device used to remove VINs.

- **Consumer Credit**

- TENN. CODE ANN. § 47-18-2107 (2009) - Release of personal consumer information. "Personal information" means an individual's first name or first initial and last name, in combination with any one (1) or more of the following data elements, when either the name or the data elements are not encrypted: (i) Social Security number; (ii) Driver's license number; or (iii) Account number, credit or debit card number, in combination with any required security code, access code, or password that permits access to an individual's financial account.
 - Any information holder shall disclose any breach of the security of the system, following discovery or notification of the breach in the security of the data, to any resident of Tennessee whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
- TENN. CODE ANN. § 47-14-125 (2009) - Compliance with federal Consumer Credit Protection Act. Compliance with the requirements of the Consumer Credit Protection Act, being Public Law 90-321; 82 Stat. 146 et seq., commonly referred to as the federal "Truth in Lending Act," shall be deemed compliance with any requirements of the statutes of Tennessee relating to the disclosure of information in connection with credit transactions.

- **Financial Records**

- TENN. CODE ANN. § 45-10-101 through -118 (2009) - Financial Records Privacy Act. A financial institution may only disclose financial records to the individual owner of the record unless the customer has consented or there is a lawful subpoena. Exceptions exist for child support enforcement as well.

- **Employee Privacy**

- State v. Stoddard, 909 S.W.2d 454 (Tenn. Crim. App. 1994) - Appellate court affirmed the order denying the defendant city police officer's motion to suppress illegal drugs found in a suitcase in the trunk of the officer's police department-issued squad car. The suitcase was located in a vehicle belonging to the city's police department and contained equipment issued by the department. There was

an oral policy communicated to the department's officers concerning the department's inspections of their person, uniform, equipment, desk, locker, and vehicle. Even though the officer did not know about this policy, his subjective belief of reasonableness was not enough.

- TENN. CODE ANN. § 50-9-101 through -114 (2009) - Drug Free Workplace Act. Defines the rules of permissive drug testing of employees.
- TENN. CODE ANN. § 50-9-109 (2009) - Confidentiality of Records from employment drug and alcohol testing. All information, interviews, reports, statements, memoranda and drug or alcohol test results, written or otherwise, received by the covered employer through a drug or alcohol testing program are confidential communications and may not be used or received in evidence, obtained in discovery or disclosed in any public or private proceedings. *See also* TENN. COMP. R. & REGS. R. 0800-2-12-.14 (2008).
- **Electronic Surveillance**
 - TENN. CODE ANN. § 39-13-601 (2009) - Wiretapping and electronic surveillance. Intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication. Exceptions apply for law enforcement, court orders, normal course of employment of a telecommunications employee.
 - TENN. CODE ANN. § 39-13-604 (2009) - Interception of cellular or cordless telephone transmissions. Person commits an offense that, without the consent of at least one party to a communication, intentionally records or disseminates a communication transmitted between two cellular radio telephones, a cellular radio telephone and a landline telephone, or a cordless telephone and a cellular radio telephone. A person commits an offense that intentionally disseminates a communication transmitted between two cordless telephones or a cordless telephone and a landline telephone, if such dissemination is not authorized by a court order. Exceptions apply including as directed by a court for domestic relations purpose, for a criminal investigation if under a search warrant.
 - TENN. CODE ANN. § 39-13-606 (2009) - Electronic tracking of motor vehicles. Except as provided, it is an offense for a person to knowingly install, conceal or otherwise place an electronic tracking device in or on a motor vehicle without the consent of all owners of the vehicle for the purpose of monitoring or following an occupant or occupants of the vehicle. It shall not be a violation:
 - If installed by law enforcement officer in furtherance of a criminal investigation and is carried out in accordance with applicable state and federal law.
 - Or if placed by a parent in his/her car to track the movement of the vehicle when a minor is using the vehicle
 - Or if for the purpose of tracking the location of stolen goods being transported in the vehicle or for the purpose of tracking the location of the vehicle if it is stolen.
 - Also doesn't apply to a tracking system installed by the manufacturer of a motor vehicle.
 - TENN. CODE ANN. § 40-6-301 through -311 (2009) - Wiretapping and Electronic Surveillance Act of 1994. Order to protect the privacy of wire, oral, and electronic

communications, to protect the integrity of court and administrative proceedings, to define, on a uniform basis, the circumstances under which a district attorney general may apply to a court of competent jurisdiction for the interception, the general assembly defined the circumstances and conditions under which the interception of wire, oral and electronic communications may be lawful. In defining these circumstances, the general assembly seeks to strike a balance between an individual's right to privacy and society's legitimate concern in being protected from criminal activity. Basically codifies the requirements to get an order/warrant for electronic surveillance.

- "Electronic communication" means any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by the aid of wire, radio, electromagnetic, photooptical or photoelectronic facilities, but does not include: (A) The radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit; (B) Any wire or oral communication; (C) Any communication made through a tone-only paging device; or (D) Any communication from a "tracking device" as defined in 18 U.S.C. § 3117.

- **Computer Statutes**

- TENN. CODE ANN. § 39-14-601 through -606 (2009) - Tennessee Personal and Commercial Computer Act of 2003. Whoever knowingly, directly or indirectly, accesses, causes to be accessed, or attempts to access any telephone system, telecommunications facility, computer software, computer program, data, computer, computer system, computer network, or any part thereof, for the purpose of obtaining money, property or services; creating a false output to achieve the foregoing; causes a malicious input; makes or uses an unauthorized copy of software; otherwise causes disruptions to a computer network.
- TENN. CODE ANN. § 47-18-5201 through -5204 (2009) - Anti-Phishing Act of 2006. It shall be unlawful for any person to represent oneself, either directly or by implication, to be another person, without the authorization or permission of such other person, through the use of the Internet, electronic mail messages or any other electronic means, including wireless communication, and to solicit, request, or take any action to induce a resident of this state to provide identifying information or identification documents.

- **Common Law**

- **Appropriation**
 - West v. Media Gen. Convergence, Inc., 53 S.W.3d 640 (Tenn. 2001) - Alluding to the tort of appropriation, but not needing to decide the case on this issue. Further credence to recognizing all torts to the invasion of privacy was stated in West: "In *Scarborough v. Brown Group, Inc.*, the United States District Court for the Western District of Tennessee held that "although no Tennessee state court has recognized the [Restatement (Second)] distinctions, federal courts applying Tennessee law have used these categories in analyzing invasion of privacy claims." 935 F. Supp. 954, 963-64 (W.D. Tenn. 1995).
- **Disclosure**

- Lineberry v. Locke, 2000 Tenn. App. LEXIS 532 (Tenn. Ct. App. July 31, 2000) - Alluding to the four common law branches of the invasion of privacy, but only ruling on public disclosure. Public disclosure means "communicating it to the public at large, or to so many persons that the matter must be regarded as substantially certain to become one of public knowledge."
- **False Light**
 - West v. Media Gen. Convergence, Inc., 53 S.W.3d 640 (Tenn. 2001) - The Supreme Court of Tennessee agrees with the majority of jurisdictions that false light should be recognized as a distinct, actionable tort. While the law of defamation and false light invasion of privacy conceivably overlap in some ways, the differences between the two torts warrant their separate recognition.
- **Intrusion**
 - Roberts v. Essex Microtel Assocs., 46 S.W.3d 205 (Tenn. Ct. App. 2000) - Plaintiff specifically asked the court, "since it is unclear if the common law of invasion of privacy tort has been formerly adopted in Tennessee, the Plaintiff requests a determination as to whether the tort is recognized by Tennessee courts." We hold that Tennessee has adopted the common law tort of invasion of privacy. This seems to indicate all common law facets of the invasion of privacy are adopted, although this court only dealt with § 652B of the Restatement of Torts. That particular section deals with "One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another." Although vague about the other branches of the invasion of privacy common law, it is clear Tennessee adopts the branch of intrusion as actionable.

TEXAS PRIVACY LAW

- **State Constitutional Privacy Rights**
 - Express
 - none
 - Implied
 - Bell v. Low Income Women of Tex., 95 S.W.3d 253 (Tex. 2000) - implied right of privacy against governmental intrusions.
- **Search and Seizure**
 - TEX. CONST. Art. I, § 9 (2009) The people shall be secure in their persons, houses, papers and possessions, from all unreasonable seizures or searches, and no warrant to search any place, or to seize any person or thing, shall issue without describing them as near as may be, nor without probable cause, supported by oath or affirmation.
 - **Auto Exception**
 - Dixon v. State, 206 S.W.3d 613 (Tex. Crim. App. 1979)
 - **Open Fields**
 - Hurwitz v. State, 673 S.W.3d 347 (Tex. Ct. App. 1979)
 - **Plain View**
 - In re Bates, 555 S.W.3d 420 (Tex. 1977)
- **Statutory Privacy Rights**
 - TEX. PENAL CODE § 42.072 (2009) – Stalking. A person commits an offense if the person, on more than one occasion and pursuant to the same scheme or course of conduct that is directed specifically at another person, knowingly engages in conduct, including following the other person, that: (1) the actor knows or reasonably believes the other person will regard as threatening: (A) bodily injury or death for the other person; (B) bodily injury or death for a member of the other person's family or household; or (C) that an offense will be committed against the other person's property; OR has a similar effect on a member of that person's family.
 - TEX. BUS. & COM. CODE § 304.001 to .259 (2009) Texas Telemarketing Disclosure and Privacy Act (effective Apr 1, 2009). Prevents interference with caller ID systems, among other provisions regulating solicitation calls.
 - TEX. BUS. & COM. CODE § 501.001 (2009) Certain Uses of Social Security Number Prohibited
 - TEX. BUS. & COM. CODE § 501.101 (2009) Use of Consumer Driver's License or Social Security Number by Merchant or Certain Third Party. A merchant or a third party under contract with a merchant who requires a consumer returning merchandise to provide the consumer's driver's license or social security number may use the number or numbers provided by the consumer solely for identification purposes if the consumer does not have a valid receipt for the item being returned and is seeking a cash, credit, or store credit refund.
 - TEX. BUS. & COM. CODE § 503.001 (2009) Capture or Use of Biometric Identifier (a) In this section, "biometric identifier" means a retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry. (b) A person may not capture a biometric identifier of an individual for a commercial purpose unless the person: (1) informs the individual before capturing the biometric identifier; and (2)

receives the individual's consent to capture the biometric identifier. (c) A person who possesses a biometric identifier of an individual: (1) may not sell, lease, or otherwise disclose the biometric identifier to another person unless: (A) the individual consents to the disclosure; (B) the disclosure completes a financial transaction that the individual requested or authorized; (C) the disclosure is required or permitted by a federal statute or by a state statute other than Chapter 552, Government Code; or (D) the disclosure is made by or to a law enforcement agency for a law enforcement purpose; and (2) shall store, transmit, and protect from disclosure the biometric identifier using reasonable care and in a manner that is the same as or more protective than the manner in which the person stores, transmits, and protects any other confidential information the person possesses.

- **Public Records**

- TEX. GOV'T. CODE ANN. § 552.021 (2007) Availability of Public Information. Public information is available to the public at a minimum during the normal business hours of the governmental body.
- TEX. GOV'T. CODE ANN. § 552.022 (2007) Categories of Public Information; Examples including the name of each official and the final record of voting on all proceedings in a governmental body.
- TEX. GOV'T. CODE ANN. § 552.028 (2007). Request for Information From Incarcerated Individual
- TEX. GOV'T. CODE ANN. § 552.101 through § 148 (2007) - Confidential information including personally identifying information, Social Security numbers, student records, photographs of peace officers, personnel information, etc.

- **Motor Vehicle Records**

- TEX. TRANSP. CODE ANN. § 204.011 (2009) § 204.011. Subscriber or Purchaser Information. Except as provided by this section or a rule adopted by the commission under this section, the department may not disclose to any person the name, address, telephone number, Social Security account number, driver's license number, bank account number, credit or debit card number, or charge account number of a person who: (1) is or has been a subscriber to "Texas Highways"; or (2) has purchased from the department a promotional item described by Section 204.009.
- TEX. TRANSP. CODE ANN. § 521.032 (2009). Enhanced Driver's License or Personal Identification Certificate. (a) The department may issue an enhanced driver's license or personal identification certificate for the purposes of crossing the border between this state and Mexico to an applicant who provides the department with proof of United States citizenship, identity, and state residency. (b) The department shall implement a one-to-many biometric matching system for the enhanced driver's license or personal identification certificate. An applicant for an enhanced driver's license or personal identification certificate must submit a biometric identifier as designated by the department, which, notwithstanding any other law, may be used only to verify the identity of the applicant for purposes relating to implementation of the border crossing initiative established by this section. An applicant must sign a declaration acknowledging the applicant's understanding of the one-to-many biometric match. (c) The enhanced

driver's license or personal identification certificate must include reasonable security measures to protect the privacy of the license or certificate holders, including reasonable safeguards to protect against the unauthorized disclosure of information about the holders. If the enhanced driver's license or personal identification certificate includes a radio frequency identification chip or similar technology, the department shall ensure that the technology is encrypted or otherwise secure from unauthorized information access. (d) The department shall periodically review technological innovations related to the security of driver's licenses and personal identification certificates and amend the rules as appropriate, consistent with this section, to protect the privacy of driver's license and personal identification certificate holders.

- TEX. TRANSP. CODE ANN. § 521.044 (2009). Use of Social Security [from licenses] Number Information for Child Support Collection. (a) Information provided on a driver's license application that relates to the applicant's Social Security number may be used only by the department or disclosed only to: (1) the child support enforcement division of the attorney general's office; (2) another state entity responsible for enforcing the payment of child support; or (3) the United States Selective Service System as provided by Section 521.147. (b) The department shall enter an applicant's Social Security number in the department's electronic database but may not print the number on the applicant's driver's license. (c) On the request of a state entity responsible for investigating or enforcing the payment of child support, the department shall disclose information regarding an applicant's Social Security number. (d) Information disclosed under this section may be used by a state entity responsible for enforcing the payment of child support only to implement the duties of the state entity. (e) The department shall include in the department's legislative appropriations requests and budgets, in quarterly performance reports, and in audits of the department's local offices performance measures on the percentage of complete and correct Social Security numbers on driver's licenses.
- TEX. TRANSP. CODE ANN. § 521.045 (2009) Disclosure of Certain Information Relating to Individual Operator. On receipt of a written request and payment of a \$ 4 fee, the department may disclose information relating to an individual's date of birth, current license status, and most recent address, as shown in the department's records, to a person who (1) is eligible to receive the information under Chapter 730; and (2) submits to the department the individual's driver's license number or the individual's full name and date of birth.
- TEX. TRANSP. CODE ANN. § 521.046 (2009) Disclosure of Accident and Conviction Information. (a) In addition to the information authorized to be released under Section 521.045, on receipt of a written request and payment of a \$ 6 fee, the department may disclose that information and information regarding each reported motor vehicle moving violation, as defined by department rule, resulting in a traffic law conviction and each motor vehicle accident in which the individual received a citation, by date and location, within the three years preceding the date of the request, to a person who: (1) is eligible to receive the information under Chapter 730; and (2) submits to the department the individual's driver's license number or the individual's full name and date of birth.

- TEX. TRANSP. CODE ANN. § 521.047 (2009) The department may disclose information as recorded in department records that relates to: (1) the individual's date of birth; (2) the current license status of the individual; (3) the individual's most recent address; (4) the completion of an approved driver education course by the individual; (5) the fact of, but not the reason for, completion of a driver safety course by the individual; and (6) each of the individual's reported traffic law violations and motor vehicle accidents, by date and location.
- TEX. TRANSP. CODE ANN. § 521.0475 (2009). Disclosure of Abstract Record. (a) Except as provided by Subsection (b) or (c), the department shall provide a certified abstract of a complete driving record of a license holder, for a fee of \$ 20, to the license holder or a person eligible to receive the information under Sections 730.007(a)(2)(A), (D), and (I).
- TEX. TRANSP. CODE ANN. § 521.049 (2009) Information Supplied to Certain Governmental Entities. (a) The department shall disclose information relating to the name, date of birth, and most recent address as shown in department records to the Texas Department of Health during an emergency or epidemic declared by the commissioner of health to notify individuals of the need to receive certain immunizations. (b) The department may not charge a fee for information disclosed to a law enforcement agency or other governmental agency for an official purpose, except that the department may charge its regular fees for information provided to those governmental agencies in bulk for research projects.
- TEX. TRANSP. CODE ANN. § 521.050 (2009) Sale of License Information. (a) In addition to the provisions of this subchapter relating to the disclosure of driver's license information on an individual, the department may provide a purchaser with a magnetic tape of the names, addresses, and dates of birth of all license holders that are contained in the department's basic driver's license record file if the purchaser certifies in writing that the purchaser is eligible to receive the information under Chapter 730. (b) The department may also periodically provide to the purchaser of the information any addition to that file.
- TEX. TRANSP. CODE ANN. § 521.052 (2009) Disclosure of Individual Information Prohibited. Except as provided by Sections 521.045, 521.046, 521.0475, 521.049(c), and 521.050, and by Chapter 730, the department may not disclose information from the department's files that relates to personal information, as that term is defined by Section 730.003.
- TEX. BUS. & COM. CODE § 504.002 (2009) Prohibition on Use for Solicitation or Sale of Information. (a) A person who possesses crime victim or motor vehicle accident information that the person obtained or knows was obtained from a law enforcement agency may not: (1) use the information to contact directly any of the following persons for the purpose of soliciting business from the person: (A) a crime victim (B) a person who was involved in a motor vehicle accident; or (C) a member of the family of a person described by Paragraph (A) or (B); or (2) sell the information to another person for financial gain.
- **Vehicle Identification Numbers**
- TEX. TRANSP. CODE ANN. § 547.615 (2009) "Recording device" means a feature that is installed by the manufacturer in a motor vehicle and that does any of the following for the

purpose of retrieving information from the vehicle after an accident in which the vehicle has been involved.

- **Consumer Credit**
 - TEX. BUS. & COM. CODE § 325.001 through § 325.001 (2009) Anti-phishing Act of 2006
- **Financial Records**
 - TEX. FIN. CODE § 59.006 (2009) Discovery of Customer Records. (a) This section provides the exclusive method for compelled discovery of a record of a financial institution relating to one or more customers but does not create a right of privacy in a record. This section does not apply to and does not require or authorize a financial institution to give a customer notice of: (1) a demand or inquiry from a state or federal government agency authorized by law to conduct an examination of the financial institution; (2) a record request from a state or federal government agency or instrumentality under statutory or administrative authority that provides for, or is accompanied by, a specific mechanism for discovery and protection of a customer record of a financial institution, including a record request from a federal agency subject to the Right to Financial Privacy Act of 1978 (12 U.S.C. Section 3401 et seq.), as amended, or from the Internal Revenue Service under Section 1205, Internal Revenue Code of 1986; (3) a record request from or report to a government agency arising out of the investigation or prosecution of a criminal offense; (4) a record request in connection with a garnishment proceeding in which the financial institution is garnishee and the customer is debtor; (5) a record request by a duly appointed receiver for the customer; (6) an investigative demand or inquiry from a state legislative investigating committee; (7) an investigative demand or inquiry from the attorney general of this state as authorized by law other than the procedural law governing discovery in civil cases; or (8) the voluntary use or disclosure of a record by a financial institution subject to other applicable state or federal law.
- **Employee Privacy**
 - TEX. GOV'T. CODE ANN. § 552.102 (2007). Exception: Personnel Information. Information is excepted from the requirements of Section 552.021 if it is information in a personnel file, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy, except that all information in the personnel file of an employee of a governmental body is to be made available to that employee or the employee's designated representative as public information is made available under this chapter. Specifically, transcripts from an institution of higher education maintained in the personnel file of a professional public school employee are not public.
 - Martinez v. State, 880 S.W.2d 72 (Tex. App. 1994) - held that an employee, lacking a possessory interest in his or her place of employment, has no expectation of privacy in the employer's premises under the Fourth Amendment. *See also* McInnis v. State, 657 S.W.2d 113 (Tex. Crim. App. 1983).
 - Lown v. State, 172 S.W.3d 753 (Tex. App. 2005), Affirming the defendant's conviction for theft of property, based on his having run an illegal Ponzi scheme bilking investors in an alleged titanium mining operation in New Guinea, the court held that the defendant had no reasonable expectation of privacy in the

information stored in his employer's computers, which were within the employer's offices, so that the defendant did not have standing to challenge, under the Fourth Amendment, the acquisition by the police of backup disks for the employer's computer system prepared by an independent technician.

- **Electronic Surveillance**

- TEX. CODE CRIM. PROC. ANN. art. 18.20 (2009) Interception and use of wire, oral, or electronic communications. "Electronic communication" means a transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photo-optical system. The term does not include: (A) a wire or oral communication; (B) a communication made through a tone-only paging device; or (C) a communication from a tracking device.
 - A judge of competent jurisdiction may issue an order authorizing interception of wire, oral, or electronic communications only if the prosecutor applying for the order shows probable cause to believe that the interception will provide evidence of the commission of certain crimes listed in this section (by statute section).
 - The Dept of Public Safety is permitted to install interception devices and may apply for them via state prosecutors to a judge in the jurisdiction.
 - There are provisions for emergency installations without court orders.
 - Within a reasonable time but not later than 90 days after the date an application for an order is denied or after the date an order or the last extension, if any, expires, the judge who granted or denied the application shall cause to be served on the persons named in the order or the application and any other parties to intercepted communications, if any, an inventory.
 - Within 30 days after the date an order or the last extension, if any, expires or after the denial of an order, the issuing or denying judge shall report to the Administrative Office of the United States Courts.
 - The exceptions listed in TEX. PENAL CODE ANN. § 16.02 (2009) also apply to this code section for law enforcement, common carriers and consent.
- TEX. CODE CRIM. PROC. ANN. art. 18.21 (2009) Pen registers and trap and trace devices; access to stored communications; mobile tracking devices. "Mobile tracking device" means an electronic or mechanical device that permits tracking the movement of a person, vehicle, container, item, or object. The term does not include a device designed, made, adapted, or capable of: (A) intercepting the content of a communication; or (B) functioning as a pen register, ESN reader, trap and trace device, or similar equipment.
- TEX. PENAL CODE ANN. § 16.01 (2009) Unlawful Use of Criminal Instrument
- TEX. PENAL CODE ANN. § 16.02 (2009) Unlawful Interception, Use, or Disclosure of Wire, Oral, or Electronic Communications. Cross lists definitions from TEX. CODE CRIM. PROC. ANN. art. 18.20 (2009).
 - Intentionally intercepts, endeavors to intercept, or procures another person to intercept or endeavor to intercept a wire, oral, or electronic communication; or uses or discloses.

- Exceptions for switchboard common carriers, law enforcement, FCC employees, consent of one party, public radio frequencies
- TEX. PENAL CODE ANN. § 16.03 (2009) Unlawful Use of Pen Register or Trap and Trace Device
- TEX. PENAL CODE ANN. § 16.04 (2009) Unlawful Access to Stored Communications
- TEX. PENAL CODE ANN. § 16.05 (2009) Illegal Divulgence of Public Communications. A person who provides electronic communications service to the public commits an offense if the person knowingly divulges the contents of a communication to another who is not the intended recipient of the communication.
- TEX. PENAL CODE ANN. § 16.06 (2009) Unlawful Installation of Tracking Device. Electronic or mechanical tracking device" means a device capable of emitting an electronic frequency or other signal that may be used by a person to identify, monitor, or record the location of another person or object. Unlawful unless done with consent of the person, or for law enforcement purposes with authorization from the court.
- **Computer Statutes**
 - TEX. PENAL CODE § 33.02 (2009) - Unlawful to knowingly access a computer or computer system without the consent of the owner. It is a felony to do so with the intent to defraud or harm another.
 - TEX. BUS. & COM. CODE § 325.004 (2009) Internet Fraud. A person may not, with the intent to engage in conduct involving the fraudulent use or possession of identifying information of another person: (1) create a web page or Internet domain name that is represented as a legitimate online business without the authorization of the registered owner of that business; and (2) use that web page or a link to that web page, that domain name, or another site on the Internet to induce, request, or solicit another person to provide identifying information for a purpose that the other person believes is legitimate.
- **Common Law**
 - Billings v. Atkinson, 489 S.W.2d 858 (Tex. 1973) - Intrusion
 - Industrial Foundation of the South v. Tex. Indus. Accident Bd., 540 S.W.2d 668 (Tex. 1976) - Public disclosure
 - Kimbrough v. Coca-Cola, 521 S.W.2d 719 (Tex. Civ. App. 1975) - Appropriation
 - Turner v. KTRK TV, Inc., 38 S.W.3d 103 (Tex. 2001). - Rejects false light.

UTAH PRIVACY LAW

- **State Constitutional Privacy Rights**
 - none
- **Search and Seizure**
 - UTAH CONST. art. I, §14 unreasonable search and seizure prohibited.
 - **Auto Exception**
 - State v. James, 13 P.3d 576 (Utah 2001).
 - **Open Fields**
 - State v. Shreve, 667 P.2d 590 (Utah 1983).
 - **Plain View**
 - State v. Kelly, 718 P.2d 385 (Utah 1986).
- **Statutory Privacy Rights**
 - UTAH CODE ANN. § 26-45-101 through -106 (2008) - Genetic Testing Privacy Act. Employers can't inquire or require any genetic testing by an individual, with some exception for health issues that may pose an unjustifiable safety risk. Health care providers also can't inquire into the results of genetic testing as contingent on renewing a policy or for any other reason besides billing for the tests done. Other exceptions apply.
 - UTAH CODE ANN. § 13-45-301 (2008) Except as allowed by other law, a person may not display a Social Security number in a manner or location that is likely to be open to public view. The state, or a branch, agency, or political subdivision of the state, may not employ or contract for the employment of an inmate in any Department of Corrections facility or county jail in any capacity that would allow any inmate access to any other person's personal information.
 - UTAH CODE ANN. § 45-3-1 through -5 (2008) - Abuse of Personal Identity Act. An advertisement is published in which the personal identity of that individual is used in a manner which expresses or implies that the individual approves, endorses, has endorsed, or will endorse the specific subject matter of the advertisement without consent.
 - UTAH CODE ANN. § 76-9-402 (2008) Privacy violation. A person is guilty of privacy violation if, except as authorized by law, he: (a) Trespasses on property with intent to subject anyone to eavesdropping or other surveillance in a private place; or (b) Installs in any private place, without the consent of the person or persons entitled to privacy there, any device for observing, photographing, recording, amplifying, or broadcasting sounds or events in the place or uses any such unauthorized installation; (c) same as b but installs outside for the purpose of hearing inside the private place.
 - UTAH CODE ANN. § 76-9-403 (2008) Communication Abuse. Illegal to Intercept, without the consent of the sender or receiver, a message by telephone, telegraph, letter, or other means of communicating privately.
 - UTAH CODE ANN. § 76-9-404 (2008) Criminal defamation. (1) A person is guilty of criminal defamation if he knowingly communicates to any person orally or in writing any information which he knows to be false and knows will tend to expose any other living person to public hatred, contempt, or ridicule.

- UTAH CODE ANN. § 76-9-406 (2008) Injunctive relief against privacy offenses-- Damages. Any person can have a cause of action. Relatives of a deceased person can bring a cause of action.
- UTAH CODE ANN. § 76-9-407 (2008) Crime of abuse of personal identity-- Penalty--Defense-- Permitting civil action. Any person is guilty of a class B misdemeanor who knowingly or intentionally causes the publication of an advertisement in which the personal identity of an individual is used in a manner which expresses or implies that the individual approves, endorses, has endorsed, or will endorse the specific subject matter of the advertisement without the consent for such use by the individual.
- UTAH CODE ANN. § 76-5-106.5 (2008) - A person is guilty of stalking who intentionally or knowingly engages in a course of conduct directed at a specific person and knows or should know that the course of conduct would cause a reasonable person: (a) to fear for the person's own safety or the safety of a third person; or (b) to suffer other emotional distress. OR violates a protective order. Aggravated crime if repeated after a conviction or with a deadly weapon.
- *See also Jeppson v. United Television, Inc.*, 580 P.2d 1087 (Utah 1978) - Airing a person's phone number and name on TV is an invasion of privacy if unconsented.
- *Donahue v. Warner Bros. Pictures*, 272 P.2d 177 (Utah 1954) - Privacy statute only applies to advertising to sell goods or services.
- **Public Records**
 - UTAH CODE ANN. § 63G-2-201 (2008) - Right to access public records. States that a record that is private, controlled, or protected under Sections 63G-2-302, 63G-2-303, 63G-2-304, and 63G-2-305.
 - UTAH CODE ANN. § 63G-2-202 (2008). Access to private, controlled, and protected documents available to the subject of the record, guardian or legal representative.
 - UTAH CODE ANN. § 63G-2-302 (2008) Private records include health history, unemployment benefits, library records; contain Social Security number, etc.
 - UTAH CODE ANN. § 63G-2-303 (2008) Private information concerning certain government employees.
 - UTAH CODE ANN. § 63G-2-304 (2008) Controlled records include mental health history, or the government has otherwise classified the record.
 - UTAH CODE ANN. § 63G-2-305 (2008) Protected records include commercial information or nonindividual financial information, trade secrets, etc.
 - *Redding v. Brady*, 606 P.2d 1193 (Utah 1980) Information on names of employees and their salaries are public records.
- **Motor Vehicle Records**
 - UTAH CODE ANN. § 41-1a-116 (2008) All motor vehicle title and registration records of the division are protected unless the division determines based upon a written request by the subject of the record that the record is public. (b) In addition to the provisions of this section, access to all division records is permitted for all purposes described in the federal Driver's Privacy Protection Act of 1994, 18 U.S.C. Chapter 123. A record designated as public under Subsection (1) (a) may be used for advertising or solicitation purposes.

- Utah Code Ann. § 41-6a-404 (2008) - Accident reports are confidential, certain exceptions apply.
- Utah Code Ann. § 41-12a-202 (2008) - Accident reports may be disclosed to those injured.
- Utah Code Ann. § 41-1a-301 (2008) - Requires registration of all commercial interstate vehicles.
- **Vehicle Identification Numbers**
 - State v. Larocco, 794 P.2d 460 (Utah 1990) - Observing a VIN from outside the car is acceptable, but opening the door to inspect is a search.
- **Consumer Credit**
 - UTAH CODE ANN. § 13-44-202 (2008) - A person who owns or licenses computerized data that includes personal information concerning a Utah resident shall, when the person becomes aware of a breach of system security, conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused for identity theft or fraud purposes.
 - UTAH CODE ANN. § 13-45-201 (2008) - Consumer may elect to place a security freeze on his credit report.
- **Financial Records**
 - State v. Thompson, 810 P.2d 415 (Utah 1991) - There is an expectation of privacy in bank and other financial records as against unreasonable search and seizure.
 - UTAH CODE ANN. § 7-3-39 (2008) - Shareholders have a right to look a records, but individual records must be protected. Must have a legitimate interest.
 - UTAH CODE ANN. § 7-1-1001 through -1007 (2008) - Financial Privacy Act. Written consent or court order for disclosure by financial institution -- Exception. Except as provided in Section 7-1-1006 [official investigations by certain entities], an individual acting in behalf of a governmental entity may not request, obtain by subpoena, or otherwise obtain information from a state or federally chartered financial institution that constitutes a record reflecting the financial condition of any person without first obtaining:(a) written permission from the person that is named or referenced in the record to be examined; or (b) an order from a court of competent jurisdiction permitting access to the record.
 - "Nonprotected record" means a record maintained by the financial institution to facilitate the conduct of its business regarding a person or account, including: (i) the existence of an account; (ii) the opening and closing dates of an account; (iii) the name under which an account is held; and (iv) the name, address, and telephone number of an account holder.
 - Can't introduce evidence from a financial institution without informing the person first, unless the proceeding is between the person and the financial institution.
 - Government entities can obtain court orders to view records, but the record holder must be given notice.
- **Employee Privacy**
 - UTAH CODE ANN. § 34-38-13 (2008) - Drug and alcohol testing program of employees is acceptable. Results are confidential and may not be entered into evidence in a criminal proceeding.

- **Electronic Surveillance**
 - UTAH CODE ANN. § 77-23a-1 (2008) Short title. "Interception of Communications Act."
 - UTAH CODE ANN. § 77-23a-3 (2008) Definitions. "Electronic communication" means any transfer of signs, signals, writings, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photo-optical system, but does not include: (a) the radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit; (b) any wire or oral communications; (c) any communication made through a tone-only paging device; or (d) any communication from an electronic or mechanical device that permits the tracking of the movement of a person or object.
 - UTAH CODE ANN. § 77-23a-4 (2008) Offenses--Criminal and civil--Lawful interception. Intentionally or knowingly intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept any wire, electronic, or oral communication or uses or discloses such communication. Exceptions for law enforcement, common carriers, acts under a court order, consent, public frequencies and channels.
 - UTAH CODE ANN. § 77-23a-5 (2008) Traffic in intercepting devices--Offenses--Lawful activities. Can't advertise or mail an interception product without having a lawful purpose.
 - UTAH CODE ANN. § 77-23a-6 (2008) Seizure and forfeiture of intercepting devices.
 - UTAH CODE ANN. § 77-23a-7 (2008) Evidence--Exclusionary rule
 - UTAH CODE ANN. § 77-23a-8 (2008) Court order to authorize or approve interception-- Procedure. If there is probable cause to suspect the person is committing or will commit such acts is grounds for an attorney general or county attorney to petition the court.
 - UTAH CODE ANN. § 77-23a-9 (2008) Disclosure or use of intercepted information
 - UTAH CODE ANN. § 77-23a-10 (2008) Application for order--Authority of order--Emergency action--Application--Entry--Conditions--Extensions--Recordings--Admissibility or suppression--Appeal by state
 - UTAH CODE ANN. § 77-23a-15.5 (2008) (1) As used in this section, "mobile tracking device" means an electronic or mechanical device emitting only an electronic locator signal which permits the tracking of the movement of a person or an object. An investigative or law enforcement officer may make application to a district judge.
- **Computer Statutes**
 - UTAH CODE ANN. § 63D-2-100 through -104 (2008) Governmental Internet Information Privacy Act. A governmental entity may not collect personally identifiable information related to a user of the governmental entity's governmental website unless the governmental entity has taken reasonable steps to ensure that on the day on which the personally identifiable information is collected the governmental entity's governmental website contains a privacy policy statement that discloses: the identity of the governmental website operator; how the governmental website operator may be contacted, and details

about how the personal information will be used and how it will be protected.
Court websites must not post personally identifiable information.

- UTAH CODE ANN § 76-6-703 (2008) - Unauthorized computer access criminalized.
- **Common Law**
 - **Appropriation**
 - Cox v. Hatch, 761 P.2d 556 (Utah 1988)
 - **Disclosure**
 - No case law.
 - **False Light**
 - Russell v. Thompson Newspapers, 842 P.2d 896 (Utah 1992)
 - **Intrusion**
 - Turner v. General Adjustment Bureau, 832 P.2d 62 (Utah Ct. App. 1992)

VERMONT PRIVACY LAW

- **State Constitutional Privacy Rights**
 - none
- **Search and Seizure**
 - VT. CONST. ch. I, art. 11 (2009) - That the people have a right to hold themselves, their houses, papers, and possessions, free from search or seizure; and therefore warrants, without oath or affirmation first made, affording sufficient foundation for them, and whereby by any officer or messenger may be commanded or required to search suspected places, or to seize any person or persons, his, her or their property, not particularly described, are contrary to that right, and ought not to be granted.
 - State v. Neil, 958 A.2d 1173 (Vt. 2008) A search that is lawful under the Fourth Amendment is not necessarily lawful under VT. CONST. ch. I, art. 11.
 - **Auto Exception**
 - State v. Savva, 616 A.2d 774 (Vt. 1991) - There is a lesser expectation of privacy in a car since it can't escape public scrutiny because its occupant and contents are in plain view and because the car's inherent mobility makes losing evidence an issue. But cannot search closed containers.
 - State v. Neil, 958 A.2d 1173 (Vt. 2008) - Recognized the automobile exception to the 4th Amendment, but did not permit law enforcement to search the pocket of the driver under this exception.
 - **Open Fields**
 - State v. Kirchoff, 587 A.2d 988 (Vt. 1991) Defendant had an expectation of privacy in the area in which the marijuana was found because of his extensive postings indicating that privacy was exactly what was sought. Therefore, the public was excluded from such "open fields." The evidence, which resulted from such warrantless search, could not be used against him at trial. This is probably a different outcome than federal doctrine.
 - State v. Bryant, 950 A.2d 467 (Vt. 2008) - The Supreme Court held that the warrantless aerial surveillance violated defendant's constitutionally protected privacy right. Vermont citizens had a constitutional right to privacy that ascended into the airspace above their homes and property. Defendant showed that he had a subjective expectation of privacy in his back yard by taking precautions to exclude others from his yard. The actions of law enforcement, which flew only 100 feet above the ground for up to thirty minutes over defendant's home, were an unreasonable intrusion of privacy.
 - **Plain View**
 - State v. Richardson, 603 A.2d 378 (Vt. 1992) - Accepts the plain view exception to the Fourth Amendment and Article 11.
- **Statutory Privacy Rights**
 - VT. STAT. ANN. tit. 13, § 1061 through 1063 (2009) Stalking. "Stalk" means to engage in a course of conduct which consists of following, lying in wait for, or harassing, and: (A) serves no legitimate purpose; and (B) would cause a reasonable person to fear for his or her physical safety or would cause a reasonable person substantial emotional distress.

- VT. STAT. ANN. tit. 9, § 2440 (2009) - Social Security number protection. Unlawful to publicly display, require input on a website that is not secure or encrypted, or to mail anything that contains the SSN on the front.
- **Individually Identifiable Government Records**
 - VT. STAT. ANN. tit. 32, § 3102 (2009) Tax records are confidential. Certain exceptions apply.
- **Public Records**
 - VT. STAT. ANN. tit. 1, § 316 (2009) - Public records are available for inspection.
 - VT. STAT. ANN. tit. 1, § 317 (2009) - Personal documents relating to an individual are not public records.
 - VT. STAT. ANN. tit. 11, § 2894 (2009) - Replies to interrogatories are not public, unless required by law.
- **Motor Vehicle Records**
 - VT. STAT. ANN. tit. 23, § 104 (2009) The records of the registration of motor vehicles, snowmobiles, and motorboats, licensing of operators and registration of dealers, all original accident reports, and the records showing suspension and revocation of licenses and registrations and the records regarding diesel fuel, gasoline, and rental vehicle taxes shall be deemed official and public records, and shall be open to public inspection at all reasonable hours.
 - VT. STAT. ANN. tit. 23, § 109 (2009) Lists of registrations to enforcement officers and others; lists of suspensions (a) Annually, the commissioner shall cause to be prepared a list of registered motor vehicles, arranged serially according to the registration numbers assigned thereto which shall contain in addition the names and addresses of registered owners and a brief description of the vehicle registered, and the name and address of each person to whom is assigned a dealer's registration number. One copy of such list shall be furnished, in such form as the commissioner may determine, free to each inspector of the motor vehicle department, sheriff, state's attorney, district judge and police department in the state. The list may be also furnished to any person on request and upon the payment of the required fee. (b) Each month, the commissioner shall cause to be prepared a list of all persons whose operating license, nonresident operating privileges, or privilege of an unlicensed operator to operate a vehicle, is suspended or revoked in this state at the time the list is prepared. Names on the list shall be arranged by county of residence or zip code. Notwithstanding chapter 5 of subchapter 3 of Title 1, the list shall be available on request in such form as the commissioner may determine. The list shall be available in an electronic format for law enforcement officers with computer access through the department of public safety.
- **Vehicle Identification Numbers**
 - VT. STAT. ANN. tit. 23, § 1601 (2009) - The commissioner, his deputies, and all enforcement officers may at all times, with or without process, stop any motor vehicle to examine identification numbers and marks thereon and raise the hood or engine cover if necessary to accomplish their purpose, and may demand and inspect the driver's license, registration certificate and permits. They may also at all times, with or without process, enter public garages, parking places and public buildings where motor vehicles are stored or kept, for the purpose of examining

identification numbers and marks thereon and may also, in like manner, examine any motor vehicle standing in any public place or way. They may in like manner examine any motor vehicle to ascertain whether its equipment complies with the requirements of law relating to motor vehicles.

- **Consumer Credit**

- VT. STAT. ANN. tit. 9, § 2480e (2009) - Credit reports are confidential unless consumer consents or there is a court order.
- VT. STAT. ANN. tit. 9, § 2480b (2009) - Agency must disclose to a consumer on request, all information about him/her.
- VT. STAT. ANN. tit. 9, § 2435 (2009) - Notice of security breach containing personal information.
- VT. STAT. ANN. tit. 9, § 2480b (2009). Disclosures to consumers. (a) A credit reporting agency shall, upon request and proper identification of any consumer, clearly and accurately disclose to the consumer all information available to users at the time of the request pertaining to the consumer, including: (1) any credit score or predictor relating to the consumer, in a form and manner that complies with such comments or guidelines as may be issued by the Federal Trade Commission; (2) the names of users requesting information pertaining to the consumer during the prior 12-month period and the date of each request; and (3) a clear and concise explanation of the information.
- VT. STAT. ANN. tit. 9, § 2480m (2009) Limitations on use of Social Security numbers in credit reports. Prior to posting or requiring the posting of a document in a place of general public circulation, an agency, board, department, commission, committee, branch, instrumentality, or authority of the state or an agency, board, committee, department, branch, instrumentality, commission or authority of any political subdivision of the state shall take all reasonable steps to redact any Social Security numbers from the document.

- **Financial Records**

- VT. STAT. ANN. tit. 8, § 514 (2009) - Financial statements for retirement facilities are public.
- VT. STAT. ANN. tit. 8, § 2530 (2009) Authority to conduct examinations and investigations. The commissioner may examine any person at any time the commissioner determines it is prudent for the protection of the residents of this state. The cost of such examination shall be borne by the licensee or by any person examined that is subject to this chapter or is required to be licensed under this chapter, in accordance with section 18 of this title. Information obtained during an examination or investigation under this chapter shall be confidential and privileged.

- **Employee Privacy**

- VT. STAT. ANN. tit. 21, § 514; 516 (2009) - Drug testing results of employees or prospective employees are confidential. Certain exceptions apply.

- **Electronic Surveillance**

- State v. Geraw, 795 A.2d 1219 (Vt. 2002) - Suppressed a wired police recording conducted inside the defendant's home citing the home as the place of utmost privacy. The police should have obtained a warrant.

- State v. Brooks, 601 A.2d 963 (Vt. 1991) - The use of informants, wired or not, intrudes upon privacy, and the use of recording technology does not alter the essential nature of the state's act. The widespread and unrestricted use of government informants is surely one of the basic characteristics of a totalitarian state. The use of informants in law enforcement, however, has long been accepted as a necessary compromise between the ideals of a perfectly private society and a perfectly safe one. Therefore, warrantless electronic participant monitoring of face-to-face conversations, in cases where a defendant, located in a public parking lot, has no reasonable expectation of privacy, does not violate the protections of the Vermont Constitution.
- State v. Blow, 602 A.2d 552 (Vt. 1991) - Warrantless electronic monitoring conducted in the home is unconstitutional.
- State v. Kirchoff, 587 A.2d 988 (Vt. 1991) Privacy expectations will not decline as technology advances and people become more accustomed to their diminished privacy in this state.
- **Computer Statutes**
 - VT. STAT. ANN. tit. 13, § 4102 (2009). Unauthorized access
 - VT. STAT. ANN. tit. 13, § 4103 (2009). Access to computer for fraudulent purposes
 - VT. STAT. ANN. tit. 13, § 4104 (2009). Alteration, damage, or interference
 - VT. STAT. ANN. tit. 13, § 4105 (2009). Theft or destruction
- **Common Law**
 - Hodgdon v. Mt. Mansfield, 624 A.2d 1122 (Vt. 1992) Intrusion, but requires repeated events.
 - Staruski v. Continental Tel. Co., 581 A.2d 266 (Vt. 1990) Use of name or likeness.
 - Lemnah v. American Breeder's Serv., 482 A.2d 700 (Vt. 1984) False light and public disclosures of hidden facts.

VIRGINIA PRIVACY LAW

- **State Constitutional Privacy Rights**
 - **Express** - None
 - **Implied** - None
- **Search and Seizure**
 - VA CONST. art I, §10 (2009). Protects against granting of general warrants for search and seizure.
 - Marlborough v. Commonwealth, 655 S.E.2d 1 (Va. 2008).
 - *Seizure?* The test is whether a reasonable person would feel free to disregard the police and go about his business, as would show whether particular encounter was seizure within meaning of Fourth Amendment or consensual encounter, is objective, and presumes an innocent person rather than one laboring under a consciousness of guilt.
 - *Or Consensual Encounter?* A consensual encounter between a citizen and a police officer becomes a seizure only when the officer, by means of physical force or show of authority, has in some way restrained the liberty of a citizen.
 - Jones v. Commonwealth, 670 S.E.2d 31 (Va. App. 2008).
 - *When Seizure is Reasonable?* An officer may, consistent with the Fourth Amendment, conduct a brief, investigatory stop when the officer has a reasonable, articulable suspicion that criminal activity is afoot.
 - To justify an investigatory stop, an officer's suspicion that criminal activity is afoot must be based on more than just a guess or a hunch.
 - To determine if there is sufficient cause to justify an investigatory stop and subsequent frisk, a court must look to the totality of the circumstances and use objective standards rather than the detaining officer's subjective intent.
 - Mere presence in a high-crime area is insufficient as a matter of law to provide reasonable suspicion for an investigative stop.
 - When an officer, without reasonable suspicion or probable cause, approaches an individual, the individual has a right to ignore the officer and go about his business.
 - Middlebrooks v. Commonwealth, 664 S.E. 2d 499 (Va. App. 2008).
 - *Fourth Amendment jurisprudence* recognizes three categories of police-citizen [contacts]: (1) consensual encounters, (2) brief, minimally intrusive investigatory detentions based upon specific, articulable facts, commonly referred to as *Terry* stops, and (3) highly intrusive arrests and searches founded on probable cause.
 - *Consensual or Seizure?* An encounter with a police officer is “consensual,” [and not a seizure] as would allow the officer to stop and ask questions, unless a reasonable person would not feel free to decline an officer's requests or would not feel free to leave.
 - *Basis for Terry stopping?* To determine whether a police officer had a particularized and objective basis for suspecting that the person stopped may be involved in criminal activity, a court must consider the totality of the circumstances.
 -

- Jackson v. Commonwealth, 470 S.E.2d 138 (Va. App. 1996).
 - Police officer may stop automobile, without probable cause, for investigatory purposes if officer possesses reasonable and articulable suspicion that motorist is unlicensed, that automobile is not registered, or that either automobile or occupant is otherwise subject to seizure for violation of law.
- Epperson v. Commonwealth, No. 2056-91-1, 1993 Va. App. LEXIS 358 (Va. Ct. App. 1993). The expectation of privacy must be an objective reasonableness.
- Baldwin v. Commonwealth, 413 S.E.2d 645 (Va. App. 1990)
 - Police officer may effect seizure by arrest only when the officer has probable cause to believe that person seized has committed or is committing criminal offense.
 - In determining whether police detention of person constitutes seizure by investigatory stop, totality of the circumstances must be considered.
 - We conclude that a person has been “seized” within the meaning of the Fourth Amendment only if, in view of all of the circumstances surrounding the incident, a *reasonable person* would have believed that he was not free to leave.
- Josephs v. Commonwealth, 390 S.E.2d 491 (Va. App. 1990), *overruled on other grounds by* Young v. Commonwealth, 659 S.E.2d 308 (Va. 2008).
 - Overrule was in regard to the inference of guilty knowledge/intent when a person is in possession of contraband.
 - Look at the totality of the circumstances to determine whether there is a reasonable expectation of privacy. Some factors to be considered are: whether the defendant had a possessory interest in the thing seized or the place searched, had the right to exclude others from that place, had exhibited a subjective expectation that the place searched would remain free from governmental invasion, took normal precautions to maintain privacy, and was legitimately on the premises.
 - Held that a person has no expectation of privacy in a stolen vehicle, so there is no standing to assert a 4th Amendment challenge.
- **Vehicle Check Points**
 - Wright v. Commonwealth, 663 S.E.2d 108 (Va. App. 2008)
 - Vehicle checkpoints with the primary objective of enforcing safety requirements are constitutional under the Fourth Amendment.
 - Fourth Amendment requires that a seizure must be carried out pursuant to a plan embodying explicit, neutral limitations on the conduct of individual police officers.
 - Stopping a vehicle at a police checkpoint constitutes a seizure within the meaning of the Fourth Amendment.
 - Seizure of defendant at vehicle checkpoint for driving a vehicle with a defective brake light did not violate defendant's Fourth Amendment right against unreasonable seizures; officers directly involved in stopping vehicles at checkpoint did not possess unfettered discretion, in that guidelines for checkpoint were preapproved, controlled checkpoint's placement, imposed a two-hour time limit on checkpoint, listed specific

officers assigned to checkpoint, provided for an on-site supervisor, ordered pre-checkpoint briefing for all patrol officers, and required officers to stop every vehicle passing through checkpoint.

- Cites *Caballes v. Illinois*, 543 U.S. 405 (2005) with approval for using a narcotics dog sniff at a legit traffic stop even if there is no reasonable, articulable suspicion of narcotics ONLY IF the stop doesn't take longer than the time it would typically take to write a summons.
- *Crandol v. City of Newport News*, 386 S.E.2d 113 (Va. 1989).
 - Sobriety checkpoint is an invasion of privacy; however, the public interest in highway safety outweighs the potential invasion of personal privacy.
- **Auto Exception**
 - *Jackson v. Commonwealth*, 470 S.E.2d 138 (Va. App. 1996).
 - citing *McCary v. Commonwealth* with approval
 - searched the suspect's car after a patdown and after observing defendants' suspicious activities from a reasonable distance.
 - suggests that reasonable, articulable suspicion might be all that's required to search a car - a suspicion that falls short of probable cause. "The combined effect of the old and new information provided [the police officers] with sufficient reasonable and articulable suspicion that the occupants and/or vehicle were subject to seizure."
 - *McCary v. Commonwealth*, 321 S.E.2d 637 (Va. 1987).
 - An automobile may be searched without a warrant if there is probable cause to believe the car contains evidence of a crime and exigent circumstances exist.
 - An automobile's mobility and likelihood that evidence will be lost or destroyed if the automobile is permitted to continue on its way present exigent circumstances justifying an exception to the search warrant requirement.
 - Where police have secured or seized an automobile to be searched, risk of removal of the car or its contents may still exist and justify an immediate warrantless search; moreover, exigent circumstances may exist even if there is no risk of removal of the vehicle or its contents.
 - *Delong v. Commonwealth*, 362 S.E.2d 669 (Va. 1987).
 - There is no legitimate expectation of privacy in the portion of an automobile that may be viewed from the outside of the vehicle
 - But there must be probable cause that the item seized is evidence of criminal activity.
- **Open Fields**
 - *Hill v. Commonwealth*, 624 S.E.2d 666 (Va. 2007).
 - explaining that the curtilage of a home (which is protected by the 4th Amendment) is different than the curtilage of a business (which is not given the same amount protection given the lesser expectation of privacy)
 - allowed state inspectors to enter a home without a warrant to inspect the goat cheese making facilities therein.
 - *Wellford v. Commonwealth*, 315 S.E.2d 235 (Va. 1984).

- A reasonable expectation of privacy must have been exhibited by a person, and society must be prepared to recognize it as reasonable. There is no reasonable expectation of privacy in open fields, but there is in home or curtilage (the land associated with the home).
 - Therefore the 4th Amendment does not apply to open fields and the police may enter to search them without a warrant.
 - Despite no-trespassing signs surrounding the field, it was permissible for the police to fly over the cornfield in a helicopter to observe the marijuana growing there. The court ruled that the field was not curtilage of the home and the search was not unreasonable.
 - Cook v. Commonwealth, 216 S.E.2d 48 (Va. 1975).
 - What a person knowingly exposes to the public is not a subject of protection by the constitutional protection against unreasonable searches.
 - There can be little, if any, expectation of privacy when one parks his automobile on a public street and leaves therein, openly exposed to view, items of contraband or other evidence of crime.
 - A search ‘implies a prying into hidden places.’
- **Plain View**
 - Cost v. Commonwealth, 657 S.E.2d 505 (Va. 2008).
 - An item may not be retrieved under the plain view exception to warrant requirement unless it is immediately apparent to the officer that the item is evidence of a crime.
 - Gibson v. Commonwealth, 653 S.E.2d 626 (Va. App. 2007).
 - Plain view doctrine provides that, with respect to searches, no reasonable expectation of privacy attaches to objects exposed to plain view.
 - Police observation of objects in plain view does not implicate the Fourth Amendment so long as the police are legitimately in the place where they viewed the objects.
 - Hamlin v. Commonwealth, 534 S.E.2d 363 (Va. App. 2000).
 - Defendant gave up any expectation of privacy when he brought bag of white powder into officer's plain view by trying to conceal bag beneath passenger seat of lawfully stopped vehicle in which defendant was passenger, and thus, Fourth Amendment was not implicated in warrantless seizure of bag of suspected cocaine.
 - For seizure to be permissible under plain view doctrine, two requirements must be met: (1) officer must be lawfully in position to view and seize item, and (2) it must be immediately apparent to officer that item is evidence of a crime, contraband, or otherwise subject to seizure.
 - Carson v. Commonwealth, 404 S.E.2d 919 (Va. App. 1991), *affirmed by* 421 S.E. 2d 415 (Va. 1992).
 - Officer's approach of narcotics defendant's automobile as it stopped at public toll booth was not a seizure; officer did not stop car or restrain its movement in any way before observing and taking cut-off straw from seat between driver's legs (which he recognized as drug paraphernalia).

- Blair v. Commonwealth, 303 S.E.2d 881 (Va. 1983).
 - Virginia accepts the plain view doctrine.
- **Statutory Privacy Rights**
 - Privacy Protection Act of 1976, VA. CODE ANN. §§ 2.1-377 through 2.1-386
 - *repealed by* 2001 Virginia Laws Ch. 844 (effective Oct. 1, 2001).
 - Note that any reference in the Code of Virginia or the Acts of Assembly to the Privacy Protection Act of 1976 shall be construed to mean the “Government Data Collection and Dissemination Practices Act.”
 - *replaced by* Government Data Collection and Dissemination Practices Act, VA. CODE ANN. §§ 2.2-3800 through 2.2-3809 (2009).
 - acknowledges the vast amount of information now available electronically
 - takes steps to ensure the protection of privacy in the Commonwealth and keeping individuals informed how their information will be disseminated
 - also provides a cause of action if information is used or acquired improperly, allots for attorneys fees and injunctive relief for individuals aggrieved under this act.
 - VA. CODE ANN. § 2.2-3800 provides guidelines for recordkeeping agencies of the Commonwealth. Some examples include:
 - there shall be no record keeping system that is secret
 - information shall not be collected unless there is clearly established need for it stated in advance.
 - any information used from these sources must be current
 - there shall be an effective way for an individual to correct any collected information
 - Commonwealth or any agency or political subdivision thereof shall not collect personal information except as explicitly or implicitly authorized by law.
 - VA. CODE ANN. § 2.2-3801 lists certain information-system definitions for the act. The definitions will only be effective *until July 1, 2009*
 - Note that VA. CODE ANN. § 2.2-3808.2 was *repealed by* 2007 Virginia Laws Chs. 548 & 626 and *replaced by* Posting and availability of certain information on the Internet; prohibitions, VA. CODE ANN. § 17.1-293.
 - This section prevents the posting online of any info that includes social security numbers, an actual signature, names of minor children, etc.
 - There are exceptions for law enforcement, land records, certain types of historic documentation, and anything from before 1907.

- Insurance Information and Privacy Protection, VA. CODE ANN. §§ 38.2-600 through -620 (2009)
 - Establish standards for the collection, use, and disclosure of information gathered in connection with insurance transactions by insurance institutions, agents or insurance-support organizations;
 - Maintain a balance between the need for information by those conducting the business of insurance and the public's need for fairness in insurance information practices, including the need to minimize intrusiveness;
 - Establish a regulatory mechanism to enable natural persons to ascertain what information is being or has been collected about them in connection with insurance transactions and to have access to such information for the purpose of verifying or disputing its accuracy;
 - Limit the disclosure of information collected in connection with insurance transactions; and
 - Enable insurance applicants and policyholders to obtain the reasons for any adverse underwriting decision.
- Sale of purchaser information, VA. CODE ANN. § 59.1-442 (2009).
 - Merchants may not sell information about a purchaser without the purchaser's consent. Notice to the purchaser under this section may be a sign or another reasonable method.
 - If the purchaser requests that the information not be sold, then the merchant must not do so.
 - **Exceptions to § 59.1-442.** VA. CODE ANN. § 59.1-443 (2009).
 - Include information gathered under the VA FOIA or information gathered that is incidental to a sale.
- Virginia Telephone Privacy Protection Act, VA. CODE ANN. § 59.1-510 (2009) – deals with solicitation of private citizens using the telephone.
- **Individually Identifiable Government Records**
 - *see* Statutory Privacy Rights, above.
- **Public Records**
 - Virginia Freedom of Information Act (FOIA), VA. CODE ANN. §§ 2.1-340 through 2.1-342
 - *repealed by* 2001 Virginia Laws Ch. 844 (effective Oct. 1, 2001)
 - *replaced by* VA. CODE ANN. §§ 2.2-3700 through 2.2-3706 (2009).
 - General Assembly ensures the people of the Commonwealth have ready access to public records in the custody of a public body or its officers and employees, and free entry to meetings of public bodies wherein the business of the people is being conducted. Also provides a procedure for accessing this FOIA information
 - This does not apply to grand juries, VA parole board, state crime commission, voter registration.
 - The current version also has organized the exceptions to FOIA in §§ 2.2-3705.1 through 3705.8. The section titles for exemptions include: general, public safety, administrative investigations, certain records of educational institutions, health and social

- services, proprietary records and trade secrets, and specific public bodies. There are about 87 exceptions in all.
- There are also limitations on criminal record disclosure in 2.2-3706
- Commissions, Boards and Institutions, VA. CODE ANN. § 9-170
 - *repealed by* 2001 Virginia Laws Ch. 844 (effective Oct. 1, 2001)
 - *replaced by* VA. CODE ANN. § 9.1-102 (2009).
 - adopt regulations per the Va. ADA concerning the privacy, confidentiality, and security of the criminal justice system
 - and *replaced by* VA. CODE ANN. § 9.1-127 (2009).
 - establishes a state-wide criminal justice information system
 - for the exchange of criminal history record information among the criminal justice agencies of the Commonwealth and its political subdivisions
 - Domestic Relations, VA. CODE ANN. § 20-87.1
 - *repealed by* 2003 Virginia Laws Ch. 467
 - *replaced by* VA. CODE ANN. § 63.2-1902 (2009).
 - allows the Dept to enter into cooperative agreements with individuals and agencies including law-enforcement agencies to complete department responsibilities, which include:
 - locating non-custodial parents
 - assess parents' ability to pay child support
 - provisions for establishing paternity
- **Motor Vehicle Records**
 - VA. CODE ANN. § 46.2-210 (2009). Lists of registration and title information may not be made available to the public or a third party.
 - VA. CODE ANN. § 46.2-208 (2009). All records in the office of the Department of Motor Vehicles containing driver or vehicle information are privileged. Certain exceptions for twenty-six reasons apply. Exceptions range from environmental enforcement, criminal warrants and at a physician's request.
 - **Vehicle Identification Numbers**
 - VA. CODE ANN. § 46.2-1530 (2009) - requires a vehicle identification number on the buyer's order.
 - **Consumer Credit**
 - Virginia Credit Service Business Act, VA. CODE ANN. §§ 59.1-335.2 through 59.1-335.7 (2009).
 - **Financial Records**
 - Personal Information Privacy Act, VA. CODE ANN. §§ 59.1-442 through 59.1-443 (2009).
 - **Employee Privacy**
 - Privacy Protection Act, VA. CODE ANN. §§ 2.1-377 through 2.1-386
 - *repealed by* 2001 Virginia Laws Ch. 844 (effective Oct. 1, 2001)
 - *replaced by* Government Data Collection and Dissemination Practices Act, VA. CODE ANN. §§ 2.2-3800 through 2.2-3809 (2009).
 - **Electronic Surveillance**
 - Interception of Wire, Electronic or Oral Communications, VA. CODE ANN. §§ 19.2-61 through 19.2-70.3 (2009).

- Except as provided in this chapter any interceptions of wire, electronic or oral communication is punishable as a misdemeanor or class six felony depending on what the individual does with the information.
- But the covered transmissions do not include “any communication from an electronic or mechanical device which permits the tracking or the movement of a person or object.”
- **Computer Statutes**
 - Computer Invasion of Privacy, VA. CODE ANN. § 18.2-152.5 (2009).
 - A person is guilty of the crime of computer invasion of privacy when he uses a computer or computer network and intentionally examines without authority any employment, salary, credit or any other financial or identifying information...if the offender knows or should know that he is without authority to view the information displayed. This is a misdemeanor.
 - If the person who views this information then disseminates it to others, he is guilty of a class six felony.
 - However, law enforcement officers may use computers to gather information. *See* § VA. CODE ANN. 18.2-152.5:1.
 - Uniform Electronic Transactions Act, VA. CODE ANN. § 59.1-479 through -501 (2009). Deals with parties who conduct business over electronic mediums. Allows the retention of electronic information for certain purposes including keeping records for evidentiary, audit, or like purposes. The statute allows laws to be put in place for electronic records to be expunged for certain reasons. These records may only be transferred with the consent of the person of whom the record was issued.
 - Uniform Computer Information Transactions Act, VA. CODE ANN. § 59.1-501.1 through -509.2 (2009). Deals with parties who conduct business over computer mediums. Includes “loss of privacy” as actionable for damages.
 - Control of an Electronic Document, VA. CODE ANN. § 8.7-106 (2009).
- **Common Law**
 - WJLA-TV v. Levin, 564 S.E.2d 383 (Va. 2002).
 - The common law torts of invasion of privacy are (1) unreasonable intrusion upon the plaintiff’s seclusion, or solitude, or into his private affairs; (2) public disclosure of true, embarrassing private facts about the plaintiff; (3) publicity which places the plaintiff in a false light in the public eye; and (4) misappropriation of plaintiff’s name or likeness for commercial purposes.
 - By codifying only the last of these torts, the Virginia General Assembly has implicitly excluded the remaining three as actionable torts in Virginia.
 - Lavery v. Automation Management Consultants, 360 S.E. 2d 336 (Va. 1987). The most recent case. Accepts the tort of appropriation of one’s name, portrait, or picture for advertising or trade purposes

WASHINGTON PRIVACY LAW

- **State Constitutional Privacy Rights**
 - **Express**
 - WASH. CONST. art. I, § 7 (2009) - Invasion of private affairs or home prohibited. No person shall be disturbed in his private affairs, or his home invaded, without authority of law.
- **Search and Seizure**
 - WASH. CONST. art. I, § 7 (2009).
 - City of Seattle v. Mesiani, 755 P.2d 775 (Wash. 1988) - Sobriety checkpoints at which all oncoming motorists are stopped constitutes an unconstitutional search and seizure. *** This is different from most states and SCOTUS.
 - State v. Boland, 800 P.2d 1112 (Wash. 1990) - Searching curbside garbage without a warrant is unconstitutional.
 - **Auto Exception**
 - State v. Patterson, 774 P.2d 10 (Wash. 1989) - Accepts the auto exceptions but slightly stricter than federal precedent. Still requires exigency not automatically provided by the mobility of the car.
 - **Open Fields**
 - State v. Cord, 693 P.2d 81 (Wash. 1985).
 - **Plain View**
 - State v. Meyers, 815 P.2d 761 (Wash. 1991).
- **Statutory Privacy Rights**
 - WASH. REV. CODE ANN. § 9.73.010 (2009). Divulging telegram, prohibited barring some exceptions
 - WASH. REV. CODE ANN. § 9.73.020 (2009). Opening sealed letter, prohibited barring some exceptions
 - WASH. REV. CODE ANN. § 9A.46.110 (2009). Stalking. Intentionally and repeatedly harasses or repeatedly follows another person; and the person being harassed or followed is placed in fear that the stalker intends to injure the person, another person, or property of the person or of another person. The feeling of fear must be one that a reasonable person in the same situation would experience under all the circumstances and the stalker Intends, knows or should know the actions will frighten, intimidate, or harass the person.
 - WASH. REV. CODE ANN. § 42.56.590 (2009). Personal information -- Notice of security breaches (a) Any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of this state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection (3) of this section, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.
- **Individually Identifiable Government Records**
 - WASH. REV. CODE ANN. § 10.97.010 through .140 (2009) - Washington State Criminal Records Privacy Act - Provide for the completeness, accuracy,

confidentiality, and security of criminal history record information and victim, witness, and complainant record information as defined in this chapter.

- WASH. REV. CODE ANN. § 42.48.020 (2009) State will provide access to personal records for research purposes that are properly vetted by the state agency and if there is informed consent.
- **Public Records**
 - WASH. REV. CODE ANN. § 42.56.070 (2009) - Unless otherwise provided, all governmental records are open to the public.
 - WASH. REV. CODE ANN. § 42.56.140 through .160 (2009) Provides exemptions to disclosure including library records, public utilities and health care records, etc.
 - WASH. REV. CODE ANN. § 42.56.050 (2009). Invasion of privacy, when: A person's "right to privacy," "right of privacy," "privacy," or "personal privacy," as these terms are used in this chapter, is invaded or violated only if disclosure of information about the person: (1) Would be highly offensive to a reasonable person, and (2) is not of legitimate concern to the public. The provisions of this chapter dealing with the right to privacy in certain public records do not create any right of privacy beyond those rights that are specified in this chapter as express exemptions from the public's right to inspect, examine, or copy public records.
 - WASH. REV. CODE ANN. § 42.56.230 (2009). Personal information exempt from disclosure under this chapter includes: (1) Personal information in any files maintained for students in public schools, patients or clients of public institutions or public health agencies, or welfare recipients; (2) Personal information in files maintained for employees, appointees, or elected officials of any public agency to the extent that disclosure would violate their right to privacy; (3) Information required of any taxpayer in connection with the assessment or collection of any tax if the disclosure of the information to other persons would (a) be prohibited to such persons by RCW 84.08.210, 82.32.330, 84.40.020, or 84.40.340 or (b) violate the taxpayer's right to privacy or result in unfair competitive disadvantage to the taxpayer; (4) Credit card numbers, debit card numbers, electronic check numbers, card expiration dates, or bank or other financial account numbers, except when disclosure is expressly required by or governed by other law; and (5) personal information that appears on a driver's license.
 - WASH. ADMIN. CODE § 44-06-080 (2008) - In accordance with requirements of chapter 42.17 RCW that agencies prevent unreasonable invasions of privacy, protect public records from damage or disorganization, and prevent excessive interference with essential functions of the agency, public records may be inspected or copies of such records may be obtained.
 - WASH. ADMIN. CODE § 44-06-110 (2008) - Pursuant to RCW 42.17.260, the office reserves the right to delete identifying details when it makes available or publishes any public record, in any cases when there is reason to believe that disclosure of such details would be an invasion of personal privacy protected by chapter 42.17 RCW.
- **Motor Vehicle Records**

- WASH. REV. CODE ANN. § 46.12.380 (2009) The names and addresses of individual vehicle owners may be provided to requesting parties who agree not to use the information for making an unsolicited business contact.
- WASH. REV. CODE ANN. § 46.12.130 (2009) Certified abstracts of driving records may only be provided to the person in the record, an employer, prospective employer, insurance carrier, or other certain exceptions.
- WASH. REV. CODE ANN. § 46.61.470 (2009) Electronic or mechanical devices to monitor the speed of vehicles may be used in the state.
- WASH. REV. CODE ANN. § 46.20.202. Enhanced drivers' licenses and identicards for Canadian border crossing. The department shall implement a one-to-many biometric matching system for the enhanced driver's license or identicard. An applicant for an enhanced driver's license or identicard shall submit a biometric identifier as designated by the department. The biometric identifier must be used solely for the purpose of verifying the identity of the holders and for any purpose set out in RCW 46.20.037. Applicants are required to sign a declaration acknowledging their understanding of the one-to-many biometric match. (c) The enhanced driver's license or identicard must include reasonable security measures to protect the privacy of Washington state residents, including reasonable safeguards to protect against unauthorized disclosure of data about Washington state residents. If the enhanced driver's license or identicard includes a radio frequency identification chip, or similar technology, the department shall ensure that the technology is encrypted or otherwise secure from unauthorized data access.
- **Vehicle Identification Numbers**
 - State v. Simpson, 622 P.2d 1199 (Wash. 1990) - If a person can show a legitimate expectation of privacy in a VIN then it may not be searched. *See also* State v. Zake, 834 P.2d 1046 (Wash. 1992).
- **Consumer Credit**
 - WASH. REV. CODE ANN. § 19.182.080 (2009) Consumer reporting agencies must disclose their credit reports to the consumer. Consumers may not recover from consumer reporting agencies unless they furnish others with false information with willful intent to injure the consumer.
 - WASH. REV. CODE ANN. § 19.255.010 (2009) Notice of security breach of consumer personal information. Any person or business that conducts business in this state and that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of this state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection (3) of this section, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.
 - WASH. REV. CODE ANN. § 19.182.170 (2009) - Acceptable for a consumer to place a security freeze on his/her credit report.
- **Financial Records**

- WASH. REV. CODE ANN. § 42.56.270 (2009) Financial, commercial, and proprietary information is exempt from disclosure.
- WASH. REV. CODE ANN. § 82.32a.005 (2009) - The legislature recognizes that in collecting revenue, the state should protect privacy rights.
- **Employee Privacy**
 - WASH. REV. CODE ANN. § 50.13.010 through .910 (2009) This chapter defines a right of privacy and confidentiality as regards individual and employing unit records maintained by the department of employment security (unemployment compensation information). The legislature further recognizes that there are situations where this right of privacy and confidentiality is outweighed by other considerations. Therefore, this chapter also defines certain exceptions to the right of privacy and confidentiality, such as under a condition of government funding or to the county clerk for certain statutory purposes.
- **Electronic Surveillance**
 - WASH. REV. CODE ANN. 9.73.030 (2009) Intercepting, recording, or divulging private communication--Consent required--Exceptions. Unlawful to intercept private communication transmitted by telephone, telegraph, radio, or other device between two or more individuals between points within or without the state by any device electronic or otherwise designed to record and/or transmit said communication regardless of how such device is powered or actuated, without first obtaining the consent of all the participants in the communication.
 - WASH. REV. CODE ANN. § 9.73.040 (2009). Intercepting private communication -- Court order permitting interception -- Grounds for issuance -- Duration -- Renewal. May be issued by any superior court judge.
 - WASH. REV. CODE ANN. § 9.73.070 (2009). This chapter does not apply to common carriers, 911 emergency services, or the FCC.
 - WASH. REV. CODE ANN. 9.73.110 (2009) Intercepting, recording, or disclosing private communications--Not unlawful for building owner--Conditions
 - WASH. REV. CODE ANN. 9.73.120 (2009) Reports--Required, when, contents
 - WASH. REV. CODE ANN. 9.73.130 (2009) Recording private communications-- Authorization-- Application for, contents
 - WASH. REV. CODE ANN. 9.73.140 (2009) Recording private communications-- Authorization of or application for--Inventory, contents, service--Availability of recording, applications, and orders
 - WASH. REV. CODE ANN. 9.73.200 (2009) Intercepting, transmitting, or recording conversations concerning controlled substances--Findings
 - WASH. REV. CODE ANN. 9.73.210 (2009) Intercepting, transmitting, or recording conversations concerning controlled substances--Authorization--Monthly report-- Admissibility--Destruction of information
 - WASH. REV. CODE ANN. 9.73.220 (2009) Judicial authorizations--Availability of judge required
 - WASH. REV. CODE ANN. 9.73.230 (2009) Intercepting, transmitting, or recording conversations concerning controlled substances--Conditions--Written reports required-- Judicial review--Notice--Admissibility--Penalties

- WASH. REV. CODE ANN. 9.73.240 (2009) Intercepting, transmitting, or recording conversations concerning controlled substances--Concurrent power of attorney general to investigate and prosecute
- WASH. REV. CODE ANN. 9.73.260 (2009) Pen registers, trap and trace devices
 - "Electronic communication" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photo-optical system, but does not include: (i) Any wire or oral communication; (ii) Any communication made through a tone-only paging device; or (iii) Any communication from a tracking device.
- **Computer Statutes**
 - WASH. REV. CODE ANN. §§ 9a.52.110 through 130 (2009) - It is a felony to intentionally gain access to a computer system or database without authorization, to damage or alter information contained therein, or to use a computer in the commission of another felony.
- **Common Law**
 - Mark v. Seattle Times, 635 P.2d 1081 (Wash. 1981) - Recognizes all four invasion of privacy torts per the Restatement of Torts.

WEST VIRGINIA PRIVACY LAW

- **State Constitutional Privacy Rights**
 - Roach v. Harper, 105 S.E.2d 564 (W. Va. 1958) - There is no explicit constitutional privacy provision; however, a legally protected privacy interest is recognized by the West Virginia Supreme Court.
- **Search and Seizure**
 - W. VA. CONST. art. III § 6 - protects against unreasonable search and seizure
 - **Auto Exception**
 - State v. Smith, 438 S.E.2d 554 (W. Va. 1993)
 - **Open Fields**
 - State v. Forshey, 386 S.E.2d 15 (W. Va. 1989)
 - **Plain View**
 - State v. Smith, 408 S.E.2d 1 (W. Va. 1991)
- **Statutory Privacy Rights**
 - W. VA. CODE § 61-2-9a (2008) Stalking. Any person who repeatedly follows another knowing or having reason to know that the conduct causes the person followed to reasonably fear for his or her safety or suffer significant emotional distress, is guilty of a misdemeanor and, upon conviction thereof, shall be incarcerated in the county or regional jail for not more than six months or fined not more than one thousand dollars, or both.
- **Public Records**
 - W. VA. CODE § 29B-1-1 (2008) Public records are accessible.
 - W. VA. CODE §§ 29B-1-3 through -4 (2008) Every person has the right to inspect public records unless its disclosure would constitute an unreasonable invasion of privacy or the record pertains to law enforcement investigation. There are other specific exemptions including trade secret, test questions, security plans, etc.
 - Child Prot. Group v. Cline, 350 S.E.2d 541 (W.Va. 1986) - In deciding whether the public disclosure of information of a personal nature would constitute an unreasonable invasion of privacy, the court adopts a five factor test: (1) whether disclosure would result in a substantial invasion of privacy and, if so, how serious, (2) the extent or value of the public interest, and the purpose or object of the individuals seeking disclosure, (3) whether the information is available from other sources, (4) whether the information was given with an expectation of confidentiality, and (5) whether it is possible to mould relief so as to limit the invasion of individual privacy.
- **Motor Vehicle Records**
 - W. VA. CODE ANN. § 17E-1-17 (2008) - Driving record information must be furnished to other state driver administration, any employer, insurer or credit reporting organization.
 - W. VA. CODE ANN. § 17A-3-22 (2008) Issuance and distribution of registration bulletins. The commissioner shall annually, following a renewal of registration, compile and publish in books or bulletins a list of all registered vehicles and shall thereafter compile and publish monthly supplements thereto. The list of registered vehicles shall be arranged serially according to the registration numbers assigned to registered vehicles and shall contain in addition the names and addresses of registered owners and a brief description of each vehicle.

- W. VA. CODE ANN. § 46A-2A-102 (2009). Notice of breach of security of computerized personal information. An individual or entity that owns or licenses computerized data that includes personal information shall give notice of any breach of the security of the system following discovery or notification of the breach of the security of the system to any resident of this State whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person and that causes, or the individual or entity reasonably believes has caused or will cause, identity theft or other fraud to any resident of this State. Except as provided in subsection (e) of this section or in order to take any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the system, the notice shall be made without unreasonable delay.
- W. VA. CODE ANN. § 46A-6L-102 (2008) - A consumer may place a security freeze on his/her consumer report.
- **Financial Records**
 - W. VA. CODE ANN. § 11-10-5d (2008). It is unlawful to disclose any part of a tax return of any individual, or to disclose information concerning personal affairs of the individual, except where required by court order, or other exception to the confidentiality rule, like child support enforcement.
- **Employee Privacy**
 - W. VA. CODE ANN. § 21-3-20 (2008) Use of video and other electronic surveillance devices by employers prohibited for the purpose of recording or monitoring the activities of the employees in areas designed for the health or personal comfort of the employees or for safeguarding of their possessions, such as rest rooms, shower rooms, locker rooms, dressing rooms and employee lounges.
 - W. VA. CODE ANN. § 21-5-5b (2008) Employer limitations on use of detection of deception devices or instruments. No employer may require or request either directly or indirectly, that any employee or prospective employee of the employer submit to a psychophysiological detection of deception examination, lie detector or other similar examination utilizing mechanical or electronic measures of physiological reactions to evaluate truthfulness, and no employer may knowingly allow the results of any examination administered outside this State to be utilized for the purpose of determining whether to employ a prospective employee or to continue the employment of an employee in this State.
- **Electronic Surveillance**
 - W. VA. CODE ANN. § 21-3-20 (2008) Use of video and other electronic surveillance devices by employers prohibited for the purpose of recording or monitoring the activities of the employees in areas designed for the health or personal comfort of the employees or for safeguarding of their possessions, such as rest rooms, shower rooms, locker rooms, dressing rooms and employee lounges.
 - W. VA. CODE ANN. § 62-1D-1 (2008) Short title. "West Virginia Wiretapping and Electronic Surveillance Act."
 - W. VA. CODE ANN. § 62-1D-2 (2008) Definitions. "Electronic communication" means any transfer of signs, signals, writing, images, sounds, data or intelligence

of any nature transmitted in whole or in part by a wire, radio, electro-magnetic, photoelectronic or photooptical system but does not include: (1) The radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit; (2) Any wire or oral communication; (3) Any combination made through a tone-only paging device.

- W. VA. CODE ANN. § 62-1D-3 (2008) Interception of communications Unlawful to intentionally intercept, attempt to intercept or procure any other person to intercept or attempt to intercept, any wire, oral or electronic communication or use or disclose unlawfully. Exceptions for common carriers, public frequencies, consent of one party, law enforcement.
- W. VA. CODE ANN. § 62-1D-4 (2008) Manufacture, possession or sale of intercepting device
- W. VA. CODE ANN. § 62-1D-5 (2008) Forfeiture of device
- W. VA. CODE ANN. § 62-1D-6 (2008) Admissibility of evidence
- W. VA. CODE ANN. § 62-1D-7 (2008) Designated judges
- W. VA. CODE ANN. § 62-1D-8 (2008) County prosecuting attorney or duly appointed special prosecutor may apply for order authorizing interception. Offenses include kidnapping, drug trafficking and other felonies.
- W. VA. CODE ANN. § 62-1D-9 (2008) Lawful disclosure or use of contents of communication. Limited to circumstances involving official duties of law enforcement or as testimony in court.
- W. VA. CODE ANN. § 62-1D-10 (2008) Pen registers and trap and trace devices. Require a court order.
- W. VA. CODE ANN. § 62-1F-1 (2008) Definitions
- W. VA. CODE ANN. § 62-1F-2 (2008) Electronic interception of conduct or oral communications in the home authorized. Must obtain a court order.
- W. VA. CODE ANN. § 62-1F-3 (2008) Application for an order authorizing interception. There is probable cause to believe that the home where the electronic interception is to occur is being used, or is about to be used, in connection with the commission of the offense, or offenses
- W. VA. CODE ANN. § 62-1F-4 (2008) Order authorizing interception
- W. VA. CODE ANN. § 62-1F-5 (2008) Recording of intercepted communications
- W. VA. CODE ANN. § 62-1F-6 (2008) Sealing of applications, orders and supporting papers
- W. VA. CODE ANN. § 62-1F-7 (2008) Investigative disclosure or use of contents of wire, electronic or oral communications or derivative evidence. May disclose to other law enforcement if necessary to fulfill official duties.
- W. VA. CODE ANN. § 62-1F-8 (2008) Interception of communications relating to other offenses
- W. VA. CODE ANN. § 62-1F-9 (2008) Retroactive authorization. Oral communications in the person's home may be electronically intercepted on an emergency basis if an application submitted in accordance with section three of this article is made to a magistrate or judge of the circuit within the county wherein the person's home is located as soon as practicable, but not more than three business days after the aforementioned determination.

- **Computer Statutes**

- W. VA. CODE ANN. § 61-3C-4 (2008). Computer fraud; access to Legislature computer; criminal penalties.
- W. VA. CODE ANN. § 61-3C-5 (2008). Unauthorized access to computer services.
- W. VA. CODE ANN. § 61-3C-6 (2008). Unauthorized possession of computer data or programs.
- W. VA. CODE ANN. § 61-3C-7 (2008). Alteration, destruction, etc., of computer equipment.
- W. VA. CODE ANN. § 61-3C-8 (2008). Disruption of computer services.
- W. VA. CODE ANN. § 61-3C-9 (2008). Unauthorized possession of computer information
- W. VA. CODE ANN. § 61-3C-10 (2008). Disclosure of computer security information.
- W. VA. CODE ANN. § 61-3C-12 (2008). Computer invasion of privacy. Any person who knowingly, willfully and without authorization accesses a computer or computer network and examines any employment, salary, credit or any other financial or personal information relating to any other person, after the time at which the offender knows or reasonably should know that he is without authorization to view the information displayed, shall be guilty of a misdemeanor.
- W. VA. CODE ANN. § 61-3C-11 (2008). Obtaining confidential public information. Any person who knowingly, willfully and without authorization accesses or causes to be accessed any computer or computer network and thereby obtains information filed by any person with the state or any county or municipality which is required by law to be kept confidential shall be guilty of a misdemeanor.
- **Common Law**
 - Crump v. Beckly Newspapers, Inc., 320 S.E.2d 70 (W.Va. 1983) - accepts the four strands of invasion of privacy torts per Prosser and the Restatement of Torts.

WISCONSIN PRIVACY LAW

- **State Constitutional Privacy Rights**
 - **Express**
 - WIS. CONST. art. I, § 9m (2008) - This state shall treat crime victims, as defined by law, with fairness, dignity and respect for their privacy. This state shall ensure that crime victims have all of the privileges and protections as provided by law.
- **Search and Seizure**
 - WIS. CONST. art. I, § 11 (2008) - The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures shall not be violated; and no warrant shall issue but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched and the persons or things to be seized.
 - **Auto Exception**
 - State v. Matejka, 621 N.W.2d 891 (Wis. 2001).
 - **Open Fields**
 - Conrad v. State, 218 N.W.2d 252 (Wis. 1974).
 - **Plain View**
 - State v. Monahan, 251 N.W.2d 421 (Wis. 1977).
- **Statutory Privacy Rights**
 - WIS. STAT. ANN. § 13.58 (2008) - Creates joint committee on information policy to review management practices to ensure the personal privacy of individuals who are subjects of state databases.
 - WIS. STAT. ANN. § 943.201 (2008) - Unauthorized use of an individual's personal identifying information or documents. Whoever, for any of the following purposes, intentionally uses, attempts to use, or possesses with intent to use any personal identifying information or personal identification document of an individual, including a deceased individual, without the authorization or consent of the individual and by representing that he or she is the individual, that he or she is acting with the authorization or consent of the individual, or that the information or document belongs to him or her is guilty of a Class H felony: (a) To obtain credit, money, goods, services, employment, or any other thing of value or benefit. (b) To avoid civil or criminal process or penalty. (c) To harm the reputation, property, person, or estate of the individual.
 - Note that personal identifying information includes biometric data
 - WIS. STAT. ANN. § 940.32 (2008) Stalking. The actor intentionally, knowingly or should knowingly, engages in a course of conduct directed at a specific person that would cause a reasonable person under the same circumstances to suffer serious emotional distress or to fear bodily injury to or the death of himself or herself or a member of his or her family or household.
 - WIS. STAT. ANN. § 196.207 (2008) Telephone caller identification services. Rules for caller identification and customer opt out provisions.
 - WIS. STAT. ANN. § 995.50 (2008) Right of Privacy. The right of privacy is recognized in this state. One whose privacy is unreasonably invaded is entitled to the following relief: equitable relief to prevent and restrain such invasion,

excluding prior restraint against constitutionally protected communication privately and through the public media; compensatory damages and attorney fees.

- The right of privacy recognized in this section shall be interpreted in accordance with the developing common law of privacy, including defenses of absolute and qualified privilege, with due regard for maintaining freedom of communication, privately and through the public media.
 - In this section, "invasion of privacy" means any of the following:
 - Intrusion upon the privacy of another of a nature highly offensive to a reasonable person, in a place that a reasonable person would consider private or in a manner which is actionable for trespass.
 - The use, for advertising purposes or for purposes of trade, of the name, portrait or picture of any living person, without having first obtained the written consent of the person or, if the person is a minor, of his or her parent or guardian.
 - Publicity given to a matter concerning the private life of another, of a kind highly offensive to a reasonable person, if the defendant has acted either unreasonably or recklessly as to whether there was a legitimate public interest in the matter involved, or with actual knowledge that none existed. It is not an invasion of privacy to communicate any information available to the public as a matter of public record.
 - Conduct that is prohibited under s. 942.09, regardless of whether there has been a criminal action related to the conduct, and regardless of the outcome of the criminal action, if there has been a criminal action related to the conduct.
 - WIS. STAT. ANN. § 19.68 (2008) - Sale of names or addresses. A government authority may not sell or rent a record containing an individual's name or address of residence, unless specifically authorized by state law. The collection of fees under s. 19.35 (3) is not a sale or rental under this section.
- **Individually Identifiable Government Records**
 - WIS. STAT. ANN. § 19.36 (2008) - Unless access is specifically authorized or required by statute, an authority shall not provide access to a record prepared or provided by an employer performing work on a project to which s. 66.0903 (municipal wages), 103.49 (state wage rate), or 103.50 (highway contracts) applies, or on which the employer is otherwise required to pay prevailing wages, if that record contains the name or other personally identifiable information relating to an employee of that employer, unless the employee authorizes the authority to provide access to that information. In this subsection, "personally identifiable information" does not include an employee's work classification, hours of work, or wage or benefit payments received for work on such a project.
 - WIS. STAT. ANN. § 16.61 (2008) - Shall create a registry, in a format that may be accessed by computer terminal, describing the records series maintained by state agencies that contain personally identifiable information by using, to the maximum extent feasible, information submitted to the board in retention schedules.

- WIS. STAT. ANN. §§ 19.62 through 19.65 (2008) "Personally identifiable information" means information that can be associated with a particular individual through one or more identifiers or other information or circumstances. This section lists rules for ensuring the confidentiality of personal records and ways to train government employees to adhere to these rules.
- WIS. STAT. ANN. § 19.67 (2008). Data collection. An authority that maintains personally identifiable information that may result in an adverse determination about any individual's rights, benefits or privileges shall, to the greatest extent practicable, do at least one of the following: (a) Collect the information directly from the individual. (b) Verify the information, if collected from another person.
- WIS. STAT. ANN. § 19.68 (2008) Collection of personally identifiable information from Internet users. No state authority that maintains an Internet site may use that site to obtain personally identifiable information from any person who visits that site without the consent of the person from whom the information is obtained. This section does not apply to acquisition of Internet protocol addresses.
- WIS. STAT. ANN. § 19.69 (2008) A state authority may not use or allow the use of personally identifiable information maintained by the state authority in a match under a matching program, or provide personally identifiable information for use in a match under a matching program, unless the state authority has specified in writing that the match program is acceptable.
- WIS. STAT. ANN. §§ 19.971(k) (2008) - The Dept of Administration must ensure that state data processing facilities implement proper privacy safeguards.
- **Public Records**
 - WIS. STAT. ANN. § 13.58 (2008) - An aim of the joint committee on information privacy is to review local and state agencies' data security and integrity, their protection of the personal privacy of individuals who are subjects of databases of state and local governmental agencies and their provision of access to public records under s. 19.35 (1).
 - WIS. STAT. ANN. § 19.35 (2008) - Except as otherwise provided by law, any requester has a right to inspect any record. Substantive common law principles construing the right to inspect, copy or receive copies of records shall remain in effect.
 - Any requester who is an individual or person authorized by the individual, has a right to inspect any record containing personally identifiable information pertaining to the individual that is maintained by an authority.
 - Overarching exception to disallow disclosure of any record containing personally identifiable information that would endanger an individual, disclose a confidence, endanger security of a population or agency, compromise the rehabilitation of an individual.
 - WIS. STAT. ANN. § 19.36 (2008) – Specific exemption for the disclosure of law enforcement records, trade secrets, informants, blueprints of state buildings, personal information in personnel records, financial information, etc. There is also a prohibition of disclosure of anything that is specifically exempt by state or federal law.
- **Motor Vehicle Records**

- WIS. STAT. ANN. § 343.027 (2008) - Any signature collected under this chapter (vehicle operator licenses) may be maintained by the department and shall be kept confidential, except that the department shall release a signature or a facsimile of a signature to the department of revenue for the purposes of administering state taxes and collecting debt or to the person to whom the signature relates.
- WIS. STAT. ANN. § 343.03 (2008) - The department shall, upon request, provide to the commercial driver license information system and the driver licensing agencies of other states any applicant or driver record information maintained by the department.
- *Otherwise, there does not seem to be any restriction of the department providing records to the public provided that providing these records would not conflict with the disclosure of public records statutes.*
- **Vehicle Identification Numbers**
 - WIS. STAT. ANN. § 342.30 (2008) No person may remove, alter or obliterate or intentionally make it impossible to read, as required under sub. (2), an identification number. This subsection does not apply to the obliteration of an identification number which occurs in the process of crushing a vehicle or vehicle part for scrap.
- **Consumer Credit**
 - WIS. STAT. ANN. § 186.53, 214.507, 215.26, 224.093 (2008) Customers have rights of access to their credit reports.
 - WIS. STAT. ANN. § 100.54 (2008) - Consumers may request a credit freeze.
 - WIS. STAT. ANN. § 134.68 (2008) - Notice of unauthorized acquisition of personal information. If an entity whose principal place of business is located in this state or an entity that maintains or licenses personal information in this state knows that personal information in the entity's possession has been acquired by a person whom the entity has not authorized to acquire the personal information, the entity shall make reasonable efforts to notify each subject of the personal information. The notice shall indicate that the entity knows of the unauthorized acquisition of personal information pertaining to the subject of the personal information.
- **Financial Records**
 - State v. Swift, 497 N.W.2d 713 (Wis. Ct. App. 1993) Bank customers have no protectable interest in the privacy of bank records relating to their accounts under the fourth amendment to the United States Constitution. He argues, however, that several Wisconsin cases have assumed without deciding that the Wisconsin Constitution affords bank customers greater protection of bank records relating to their accounts. His reliance on those cases is misplaced.
- **Employee Privacy**
 - WIS. STAT. ANN. § 230.86 (2008) Discipline based on surveillance - No appointing authority may take any disciplinary action based in whole or in part on wiretapping, electronic surveillance or one-way mirrors unless that surveillance produces evidence that the employee against whom disciplinary action is taken has committed a crime or unless that surveillance is authorized by the appointing authority and is conducted in accordance with the laws of this state.

- WIS. STAT. ANN. § 130.13 (2008) Every employer shall, upon the request of an employee, which the employer may require the employee to make in writing, permit the employee to inspect any personnel documents which are used or which have been used in determining that employees qualifications for employment, promotion, transfer, additional compensation, termination or other disciplinary action, and medical records, except as provided in subs. (5) and (6).
 - The right of the employee or the employees designated representative under sub. (3) to inspect personnel records under this section includes the right to inspect any personal medical records concerning the employee in the employer's files.
 - The employer does not have to provide employer references, records relating to a possible criminal investigation and the like.
- **Electronic Surveillance**
 - WIS. STAT. ANN. 968.27 (2008) Definitions. "Electronic communication" means any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature wholly or partially transmitted by a wire, radio, electromagnetic, photoelectronic or photooptical system. "Electronic communication" does not include any of the following: (a) The radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit. (b) Any wire or oral communication. (c) Any communication made through a tone-only paging device. (d) Any communication from a tracking device.
 - WIS. STAT. ANN. 968.28 (2008) Application for court order to intercept communications. An attorney general or district attorney may apply for a court order only if the interception may provide or has provided evidence of the commission of the offense of homicide, felony murder, kidnapping, commercial gambling, bribery, extortion, dealing in controlled substances or controlled substance analogs, a computer crime that is a felony under s. 943.70, or any conspiracy to commit any of the foregoing offenses.
 - WIS. STAT. ANN. 968.29 (2008) Authorization for disclosure and use of intercepted wire, electronic or oral communications.
 - WIS. STAT. ANN. 968.30 (2008) Procedure for interception of wire, electronic or oral communications. Contents should be recorded if possible. The interception can't last longer than 30 days. There must be probable cause that the person is committing or committed a crime listed in § 968.28. Within 90 days of filing the application, the intercepted person must be informed and provided with an inventory if the interception was completed and informed whether no information was found.
 - WIS. STAT. ANN. 968.31 (2008) Interception and disclosure of wire, electronic or oral communications prohibited. Intentionally intercepts, attempts to intercept or procures any other person to intercept or attempt to intercept, any wire, electronic or oral communication or uses or discloses said interception without authority. Exceptions include telecommunications provider in emergency situations.
 - WIS. STAT. ANN. 968.32 (2008) Forfeiture of contraband devices.
 - WIS. STAT. ANN. 968.33 (2008) Reports concerning intercepted wire or oral communications. In January of each year, the Department of Justice shall report to

the administrative office of the United States courts such information as is required to be filed by 18 USC 2519. A duplicate copy of the reports shall be filed, at the same time, with the office of the director of state courts.

- WIS. STAT. ANN. 968.34 (2008) Use of pen register or trap and trace device restricted.
- WIS. STAT. ANN. 968.35 (2008) Application for an order for a pen register or a trap and trace device.
- WIS. STAT. ANN. 968.36 (2008) Issuance of an order for a pen register or a trap and trace device.
- WIS. STAT. ANN. 968.37 (2008) Assistance in the installation and use of a pen register or trap and trace device.
- **Computer Statutes**
 - WIS. STAT. ANN. § 943.70 (2008) Computer Crime. Whoever willfully, knowingly and without authorization does any of the following may be penalized: 1. Modifies data, computer programs or supporting documentation; 2. Destroys data, computer programs or supporting documentation; 3. Accesses computer programs or supporting documentation; 4. Takes possession of data, computer programs or supporting documentation; 5. Copies data, computer programs or supporting documentation; 6. Discloses restricted access codes or other restricted access information to unauthorized persons.
- **Common Law**
 - WIS. STAT. ANN. § 895.01 (2008) In addition to the causes of action that survive at common law, all of the following also survive: Causes of action for invasion of privacy.
 - *See* WIS. STAT. ANN. § 995.50 (2008) - basically codifies the four strands from common law invasion of privacy, but explicitly leaves in place the common law cause of action: “The right of privacy recognized in this section shall be interpreted in accordance with the developing common law of privacy, including defenses of absolute and qualified privilege, with due regard for maintaining freedom of communication, privately and through the public media.”

WYOMING PRIVACY LAW

- **State Constitutional Privacy Rights**
 - none
- **Search and Seizure**
 - WYO. CONST. art. 1, § 4 (2008). Security against search and seizure. The right of the people to be secure in their persons, houses, papers and effects against unreasonable searches and seizures shall not be violated, and no warrant shall issue but upon probable cause, supported by affidavit, particularly describing the place to be searched or the person or thing to be seized.
 - **Auto Exception**
 - Holman v. State, 183 P.3d 368 (Wyo. 2008) - Recognized the automobile exception, but did not find for the officers in this case.
 - The inherent mobility of vehicles and the diminished expectation of privacy involved in the use and regulation of automobiles permit warrantless searches of automobiles in circumstances in which warrantless searches would not be reasonable in other contexts. This exception allows police to search an automobile without having a warrant when they have probable cause to believe that the car contains evidence of a crime or contraband. Probable cause justifying a search of a vehicle is established if, under the totality of the circumstances, there is a fair probability that the car contains contraband or evidence of a crime.
 - It is true that a driver of a vehicle has a diminished privacy interest in the contents of his vehicle. This does not mean, however, that the driver has no expectation of privacy. This lesser expectation of privacy does not give the police the license to stop and detain or enter at will. Some justification for a stop and greater justification for a search and seizure is required. In addition, there has to be some expectation of privacy in parts of the car shielded from public view, such as the trunk, glove compartment, and under the seats. While the importance of drug interdiction activities has been acknowledged, the Supreme Court of Wyoming has also expressed willingness to protect the privacy rights of citizens under Wyo. Const. art. 1, § 4, if police conduct is unreasonable under all the circumstances.
 - Note that the Wyo. Const. provides more protection than the Federal rules and inventorying a car subsequent to arrest can only be done if there is probable cause to search. “The United States Supreme Court held that, under the Fourth Amendment to the United States Constitution, an officer arresting an occupant of a vehicle may contemporaneously search the passenger compartment of that vehicle, incident to that arrest. In Vasquez v. State, 990 P.2d 476, 480-89 (Wyo. 1999), *we rejected the minimal protection that Belton's "bright-line rule" provides, and we held that Article 1, Section 4 of the Wyoming Constitution provides greater protection.* Specifically, we announced that Article 1, Section 4

requires the search of an arrestee's vehicle to be "reasonable under all of the circumstances."

- **Open Fields**
 - Goettl v. State, 842 P.2d 549 (Wyo. 2005) - Wyoming adopts the "open fields" doctrine.
 - *See also* Pellatz v. State, 711 P.2d 1138 (Wyo. 1986) Wyoming adopts the "open fields" doctrine.
- **Plain View**
 - Holman v. State, 183 P.3d 368 (Wyo. 2008) - Recognized the plain view doctrine as a search which results when an object is inadvertently in the plain view of police officers while they are where they have a right to be, but did not need to rule on this issue because the officers' inventory of the car was unlawful.
- **Statutory Privacy Rights**
 - WYO. STAT. ANN. § 6-2-506 (2008) - Person commits the crime of stalking if, with intent to harass another person, the person engages in a course of conduct reasonably likely to harass that person, including but not limited to any combination of the following: (i) Communicating, anonymously or otherwise, or causing a communication with another person by verbal, electronic, mechanical, telegraphic, telephonic or written means in a manner that harasses; (ii) Following a person, other than within the residence of the defendant; (iii) *Placing a person under surveillance by remaining present outside his or her school, place of employment, vehicle, other place occupied by the person, or residence other than the residence of the defendant;* or (iv) Otherwise engaging in a course of conduct that harasses another person. This section does not apply to an otherwise lawful demonstration, assembly or picketing.
 - WYO. STAT. ANN. § 6-3-901 (2008). Unauthorized use of personal identifying information; penalties; restitution. (a) Every person who willfully obtains personal identifying information of another person, and uses that information for any unlawful purpose, including obtaining, or attempting to obtain, credit, goods, services or medical information in the name of the other person without the consent of that person is guilty of theft of identity. (b) As used in this section "personal identifying information," means the name, address, telephone number, driver's license number, Social Security number, place of employment, employee identification number, tribal identification card number, mother's maiden name, demand deposit account number, savings account number, or credit card number of an individual person.
- **Individually Identifiable Government Records**
 - WYO. STAT. ANN. § 7-19-402 (2008) - Creates a DNA database of convicted felons that may be used in place of records with personal identifying information.
 - WYO. STAT. ANN. § 9-1-640 (2008) - Administrative subpoena authority for investigations of child exploitation. In any investigation relating to a state offense involving sexual exploitation of children under W.S. 6-4-303, and upon reasonable cause to believe that an Internet service account has been used in the exploitation or attempted exploitation of children, the attorney general or his chief deputy may issue in writing and cause to be served a subpoena requiring the

production and testimony described in this section including financial records, name, address, internet accounts, passwords, etc.

- **Public Records**

- WYO. STAT. ANN. § 16-4-202 through -205 (2008) - All public records shall be open for inspection by any person at reasonable times, except as provided in this act or as otherwise provided by law, but the official custodian of any public records may make rules and regulations with reference to the inspection of the records.
 - WYO. STAT. ANN. § 16-4-203 (2008) Exceptions include unwarranted invasions of personal privacy, law enforcement records, investigatory and work product records of agencies, court files of judicial proceedings (working memoranda), personal name/address records (motor vehicle records, health records, etc.), trade secrets, school district records, appraisals, bids, infrastructure or hazardous chemical storage information, archeological, endangered species, libraries, licensing exams, draft legislation, personnel files containing Social Security information, records of diagnoses of diseases, information if disclosed would give a reasonable likelihood of threatening the public safety by exposing a vulnerability in preventing, protecting against, mitigating, or responding to a terrorist act.
 - There is a catch-all exception for disclosures the public record custodian believes would cause substantial injury to the public interest.
- WYO. STAT. ANN. § 22-2-113 (2008) - The secretary of state shall furnish at a reasonable price registry lists to any candidate for a political office in the state. Information copied from campaign receipts and expenditure reports filed by state and local candidates may be used for political purposes but shall not be used for commercial purposes.
- 006-032-001 WYO. CODE R. § 2 (2009) - Information in all its forms is a valued asset to the State of Wyoming (State). Public information should be available to our citizens and to State government. Disclosure restrictions required by Wyoming law must be observed regardless of the media or characteristics of the record or transaction. The value of public information can be maximized through consistent delivery to and expanded use by the citizens of Wyoming and State government. To ensure continued confidence in and reliance on State agencies and the information they collect and maintain; State agencies must protect the privacy of citizens and ensure the integrity of State information in all forms.
- WYO. STAT. ANN. § 16-9-107 (2008). Confidentiality of information - The information obtained through a 911 system shall be considered a public record under W.S. 16-4-201(a) (v) and access to the information may be denied according to law.
- WYO. STAT. ANN. § 6-2-310 (2008). Names not to be released. After the filing of an information or indictment and absent a request to release the identity of a minor victim by the victim or acting on behalf of a minor victim, the trial court shall restrict the disclosure or publication of information reasonably likely to identify the minor victim of a sexual assault.

- **Motor Vehicle Records**

- WYO. STAT. ANN. Ann. § 31-7-309 (2008) - Notwithstanding any other provision of law, the department shall furnish full information regarding the driving record of any person: to the driver license administrator of any other state or province or territory of Canada requesting the information; to any employer or perspective employer upon request and payment of the required fee; to insurers upon request and payment of the required fee.
- WYO. STAT. ANN. § 31-1-202 (2008) - The department shall maintain records of vehicle registrations from all counties indexed by distinctive vehicle numbers assigned by the department, the name of the registered owner and vehicle identification numbers. The department shall maintain a record of all vehicle certificates of title from all counties. Records are public and open to inspection by the public during reasonable office hours.
- **Vehicle Identification Numbers**
 - WYO. STAT. ANN. § 31-11-103 (2008) - No person shall remove, change, alter or obliterate the vehicle identification number of a vehicle with intent to defraud by altering or disguising the identity of a vehicle.
 - WYO. STAT. ANN. § 31-11-108 (2008) - Every dealer shall examine, without charge, the vehicle identification number of every vehicle coming into his possession except those vehicles received by him for the express purpose of repairs that do not require the replacement of any component that bears a vehicle identification number. The dealer shall promptly notify the local sheriff's office if the vehicle identification number of the vehicle has been altered, changed or obliterated as to make the number indecipherable or if the vehicle identification number or the state registration license number of the vehicle does not correspond with the vehicle identification number of the vehicle state registration certificate.
 - WYO. STAT. ANN. § 31-11-111 (2008) - All officers, having probable cause, may take and hold possession of any vehicle for a reasonable time not to exceed ninety (90) days as may be necessary if the vehicle identification number of the vehicle has been altered, removed, changed or obliterated.
- **Consumer Credit**
 - WYO. STAT. ANN. § 40-12-501 through -509 (2008) - Credit Freeze Reports. An individual or commercial entity that conducts business in Wyoming and that owns or licenses computerized data that includes personal identifying information about a resident of Wyoming shall, when it becomes aware of a breach of the security of the system, notify that person in writing.
 - If a security freeze is in place, a consumer reporting agency may not release a consumer's credit report or information derived from the credit report to a third party that intends to use the information to determine a consumer's eligibility for credit or the opening of a new account without prior authorization from the consumer.
 - However, there are still exceptions in § 505 that permit the credit agency to release information about the consumer to a third party during the credit freeze.
- **Financial Records**
 - WYO. STAT. ANN. § 40-22-108 (2008) - Wyoming Money Transmitters Act. Application for a license to practice under this act requires disclosure of personal

financial statement and employment history for the past five (5) years among other inquiries.

- WYO. STAT. ANN. § 39-11-102 (2008) Administration; confidentiality; department of revenue. Taxpayer records shall be confidential.
- **Employee Privacy**
 - Defer to federal law for permissibility of random drug testing of public employees WYO. STAT. ANN. § 9-2-1022 (2008). Duties of department performed through human resources division cites the following “Validity, under federal constitution, of regulations, rules or statutes requiring random or mass drug testing of public employees or persons whose employment is regulated by state, local or federal government, 86 ALR Fed 420.”
- **Electronic Surveillance**
 - WYO. STAT. ANN. § 7-3-701 (2008) "Electronic communication" means any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce but does not include: (A) Any wire or oral communication; (B) Any communication made through a tone-only paging device; (C) Any communication made through a tracking device as defined in 18 U.S.C. § 3117; or (D) Electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds.
 - WYO. STAT. ANN. § 7-3-702 (2008) Prohibition against interception or disclosure of wire, oral or electronic communications; exceptions; penalties. Unlawful to intercept, attempt to intercept, or procure any other person to intercept or attempt to intercept any wire, oral or electronic communication or use or disclose. Exceptions for telecommunications operators, law enforcement, FCC, public frequencies.
 - "Electronic communication" means any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce but does not include: (A) Any wire or oral communication; (B) Any communication made through a tone-only paging device; (C) Any communication made through a tracking device as defined in 18 U.S.C. § 3117; or (D) Electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds.
 - WYO. STAT. ANN. § 7-3-703 (2008) Prohibition against manufacture and possession of wire, oral or electronic communication intercepting.
 - WYO. STAT. ANN. § 7-3-704 (2008) Seizure and forfeiture of wire or oral communication intercepting devices.
 - WYO. STAT. ANN. § 7-3-705 (2008) Authorization for interception of wire, oral or electronic communications. Attorney general or district attorney may apply for interception if wiretapping will garner information related to violations of the Wyoming Controlled Substances Act of 1971. Statute specifically allows intercepting information on other felonies including murder and kidnapping if incident to the wiretapping in relation to the Controlled Substances Act.

- WYO. STAT. ANN. § 7-3-706 (2008) Authorization for disclosure and use of intercepted communications.
- WYO. STAT. ANN. § 7-3-707 (2008). Procedure for interception of wire, oral or electronic communications. There needs to be probable cause and proof that normal investigative procedures proved insufficient. The order can't be longer than 30 days. Must record the interception if possible. Within a reasonable time, but not later than ninety (90) days after the denial of an application or the termination of the period of an order authorizing interception or extension thereof, the judge shall cause to be served upon each person named in the order an inventory.
- WYO. STAT. ANN. § 7-3-708 (2008). Order directing others to furnish assistance.
- WYO. STAT. ANN. § 7-3-709 (2008). Information furnished to attorney general by executing agency; report to legislature. The attorney general shall report to the joint judiciary interim committee no later than July 1 of each year. The report shall contain the information required by subsections (a) and (b) of this section, concerning type of application and success getting court approval.
- WYO. STAT. ANN. § 7-3-710 (2008). Recovery of civil damages for violations; good faith defense.
- WYO. STAT. ANN. § 7-3-801 (2008) Definitions for Pen Registers.
- WYO. STAT. ANN. § 7-3-802 (2008) General prohibition on pen register and trap and trace device use; exception. Must have a court order unless a telecommunications carrier is testing or doing maintenance and repair.
- WYO. STAT. ANN. § 7-3-803 (2008) Application for an order for a pen register or a trap and trace device. Made by the attorney general or district attorney and only for controlled substances violations.
- WYO. STAT. ANN. § 7-3-804 (2008) Issuance of an order for a pen register or a trap and trace device
- WYO. STAT. ANN. § 7-3-805 (2008) Assistance in installation and use of a pen register or a trap and trace device
- WYO. STAT. ANN. § 7-3-806 (2008) Reports concerning pen registers and trap and trace devices. The attorney general shall annually report to the joint judiciary interim committee on the number of pen register orders and orders for trap and trace devices applied for under this act. The report shall be provided no later than July 1 of each year.
- **Computer Statutes**
 - WYO. STAT. ANN. § 6-3-501 through -505 (2008) - Modifies data, programs or supporting documentation residing or existing internal or external to a computer, computer system or computer network; Destroys data, programs or supporting documentation residing or existing internal or external to a computer, computer system or computer network.
 - Unlawful to knowingly and without authorization: (i) Access a computer, computer system or computer network; (ii) Deny computer system services to an authorized user of the computer system services which, in whole or part, are owned by, under contract to, or operated for, on behalf of, or in conjunction with another.
- **Common Law**

- Houghton v. Franscell, 870 P.2d 1050 (Wyo. 1994) - Recognized Georgia's approach to the common law invasion of privacy strands (Georgia accepts all four strands), but explicitly stated that the court was accepting the approach only for the exemption to the disclosure of medical records. "We adopt Georgia's definition of invasion of privacy for purposes of exempting records from disclosure under the public records act."
- Blake v. Rupe, 651 P.2d 1096 (Wyo. 1982) - Referenced a Kansas case that dealt with causes of action in intrusion and seclusion, but did not rule on the issue.
- It remains unclear whether Wyoming would recognize the tort of public disclosure in other contexts, or if any of the other three strands of the common law would be given effect in this state.

STATE LAWS SUMMARY MATRIX

State	Express Privacy Guarantee	Implied Privacy Right	Constitutional Restriction - Searches and Seizures	Electronic Surveillance Statute	Electronic Surveillance Statute does not include	Invasion of Privacy Common Law Torts			
						Appropriation: using one's likeness for commercial purposes w/o permission	False Light: disseminating material falsehoods about a person	Intrusion: invading one's seclusion or privacy	Public Disclosure: disseminating true, but sensitive information about a person
Alabama			X	X		X	X	X	X
Alaska	X	X	X	X	tracking devices	X	X	X	X
Arizona	X	X	X	X	tracking devices, infrared signals	X	X	X	X
Arkansas		X	X			X	X	X	X
California	X		X	X	tracking devices**	X	X	X	X
Colorado			X	X	tracking devices	X	X	X	X
Connecticut			X	X		X	X	X	X
Delaware			X	X	X	X	X	X	X
District of Columbia			X	X		X	X	X	X
Florida	X		X	X	tracking devices***	X			X
Georgia			X	X		X	X	X	X
Hawaii	X		X	X	tracking devices***	X	X	X	X
Idaho		X	X	X	tracking devices	X	X	X	X
Illinois	X		X	X	tracking devices	X	X	X	X
Indiana		X	X	X		X	X	X	X
Iowa		X	X	X	tracking devices	X	X	X	X
Kansas			X	X	tracking devices	X	X	X	X
Kentucky			X			X	X	X	X
Louisiana	X	X	X	X	tracking devices	X	X	X	X
Maine		X	X			X	X	X	X
Maryland			X	X	tracking devices	X	X	X	X
Massachusetts			X	X		X	X	X	X
Michigan			X	X		X	X	X	X
Minnesota			X	X	tracking devices***	X		X	X
Mississippi			X			X	X	X	X
Missouri			X	X		X	X	X	X
Montana**	X	X	X	X			X		
Nebraska			X	X	tracking devices***	X	X	X	X
Nevada			X	X		X	X	X	X
New Hampshire		X	X	X		X	X	X	X
New Jersey		X	X	X	tracking devices	X	X	X	X
New Mexico			X			X	X	X	X
New York			X	X	tracking devices	No common law, but limited statutory privacy rights, see pg 181			
North Carolina			X	X	tracking devices	X		X	
North Dakota			X	X	tracking devices	X	X	X	X
Ohio			X	X	tracking devices	X	X	X	X
Oklahoma			X	X	tracking devices	X	X	X	X
Oregon			X	X	tracking devices***	X	X	X	X
Pennsylvania			X	X	tracking devices***	X	X	X	X
Rhode Island	X		X	X	tracking devices	No common law, but the torts are codified, see pg 217, 221			
South Carolina	X	X	X	X	tracking devices***	X		X	X
South Dakota			X			X	X	X	X
Tennessee			X	X	tracking devices***	X	X	X	X
Texas		X	X	X	tracking devices***	X		X	X
Utah			X	X	tracking devices***	X	X	X	
Vermont			pg 253	No, but electronic surveillance caselaw pg 255-56		pg 256	pg 256	pg 256	pg 256
Virginia			X	X	tracking devices	X			
Washington	X		X	X	tracking devices	X	X	X	X
West Virginia		X	X	X	tracking devices +++	X	X	X	X
Wisconsin		X	X	X	tracking devices	X	X	X	X
Wyoming			X	X	tracking devices+++	X	X	X	X
Overall Total of States	11	14	#REF!	#REF!	-	#REF!	#REF!	#REF!	#REF!

+++ note that these states require law enforcement to obtain a court order to install a tracking device

EVENT DATA RECORDER STATUTES

- **Arkansas**
 - Ark. Code Ann. § 23-112-107 (2009).
 - At the time of a new vehicle purchase by a consumer from a dealership, an owner of a motor vehicle shall be given written notice by the seller or manufacturer that includes the following:
 - (1) The presence of the motor vehicle event data recorder in the motor vehicle;
 - (2) The type of motor vehicle event data recorder in the motor vehicle; and
 - (3) The type of data that is recorded, stored, or transmitted on the motor vehicle event data recorder.
 - Except as specifically provided under subsections (d) and (f)-(I) of this section, the data on a motor vehicle event data recorder:
 - (1) Is private;
 - (2) Is exclusively owned by the owner of the motor vehicle; and
 - (3) Shall not be retrieved or used by another person or entity.
 - Exceptions to release data:
 - Consent by all owners of the vehicle
 - even if insurer or lienholder becomes the owner due to an accident with the vehicle, the owner at the time of the crash must give consent to obtain the data
 - The data from a motor vehicle event data recorder shall only be produced without the consent of the owner at the time of the accident if:
 - (1) A court of competent jurisdiction in Arkansas orders the production of the data;
 - (2) A law enforcement officer obtains the data based on probable cause of an offense under the laws of the State of Arkansas; or
 - (3) A law enforcement officer, a firefighter, or an emergency medical services provider obtains the data in the course of responding to or investigating an emergency involving physical injury or the risk of physical injury to any person.
 - To protect the public health, welfare, and safety, the following exceptions shall be allowed regarding the retrieval of data from a motor vehicle event data recorder:
 - (1) To determine the need or to facilitate emergency medical care for the driver or passenger of a motor vehicle that is involved in a motor vehicle crash or other emergency, including obtaining data from a company that provides subscription services to the owners of motor vehicles for in-vehicle safety and security communications systems;

- (2) To facilitate medical research of the human body's reaction to motor vehicle crashes if:
 - (A) The identity of the owner or driver is not disclosed in connection with the retrieved data; and
 - (B) The last four (4) digits of the vehicle identification number are not disclosed; or
 - (3) To diagnose, service, or repair a motor vehicle.
 - **California**
 - Cal. Veh. Code § 9951 (2010).
 - Applies to all motor vehicles manufactured on or after July 1, 2004.
 - A manufacturer of a new motor vehicle sold or leased in this state that is equipped with one or more recording devices commonly referred to as “event data recorders (EDR)” or “sensing and diagnostic modules (SDM),” shall disclose that fact in the owner's manual for the vehicle.
 - Data described in subdivision (b) that is recorded on a recording device may not be downloaded or otherwise retrieved by a person other than the registered owner of the motor vehicle, except under one of the following circumstances:
 - (1) The registered owner of the motor vehicle consents to the retrieval of the information.
 - (2) In response to an order of a court having jurisdiction to issue the order.
 - (3) For the purpose of improving motor vehicle safety, including for medical research of the human body's reaction to motor vehicle accidents, and the identity of the registered owner or driver is not disclosed in connection with that retrieved data. The disclosure of the vehicle identification number (VIN) for the purpose of improving vehicle safety, including for medical research of the human body's reaction to motor vehicle accidents, does not constitute the disclosure of the identity of the registered owner or driver.
 - (4) The data is retrieved by a licensed new motor vehicle dealer, or by an automotive technician as defined in Section 9880.1 of the Business and Professions Code, for the purpose of diagnosing, servicing, or repairing the motor vehicle.
- **Colorado**
 - Colo. Rev. Stat. Ann. § 12-6-402 (2009).
 - A manufacturer of a motor vehicle that is sold or leased in Colorado with an event data recorder shall in bold-faced type disclose, in the owner's manual, that the vehicle is so equipped and, if so, the type of data recorded. A disclosure made by means of an insert into the owner's manual shall be deemed a disclosure in the owner's manual.
 - Event data that is recorded on an event data recorder is the personal information of the motor vehicle's owner, and therefore, such information shall not be retrieved by a person who is not the owner of the motor vehicle, except in the following circumstances:

- (a) The owner of the motor vehicle or the owner's agent has consented to the retrieval of the data within the last thirty days;
- (b) The data is retrieved by a motor vehicle dealer or by an automotive technician to diagnose, service, or repair the motor vehicle at the request of the owner or the owner's agent;
- (c) The data is subject to discovery pursuant to the rules of civil procedure in a claim arising out of a motor vehicle accident;
- (d) A court or administrative agency having jurisdiction orders the data to be retrieved;
- (e) The event data recorder is installed after the manufacturer or motor vehicle dealer sells the motor vehicle; or
- (f) A peace officer retrieves the data pursuant to a court order as part of an investigation of a suspected violation of a law that has caused, or contributed to the cause of, an accident resulting in damage of property or injury to a person.
- A person authorized to download or retrieve data from an event data recorder may release such data in the following circumstances:
 - (I) The owner of the motor vehicle or the owner's agent has consented to the release of the data within the last thirty days;
 - (II) The data is subject to discovery pursuant to the rules of civil procedure in a claim arising out of a motor vehicle accident;
 - (III) The data is released pursuant to a court order as part of an investigation of a suspected violation of a law that has caused, or contributed to the cause of, an accident resulting in appreciable damage of property or injury to a person;
 - (IV) If the identity of the owner or driver is not disclosed, the data is released to a motor vehicle safety and medical research entity in order to advance motor vehicle safety, security, or traffic management; or
 - (V) The data is released to a data processor solely for the purposes permitted by this section if the identity of the owner or driver is not disclosed.
- Colo. Rev. Stat. Ann. § 12-6-403 (2009).
 - The above § shall apply to motor vehicles manufactured on or after May 1, 2007
- **Connecticut**
 - Conn. Gen. Stat. § 14-164aa (2009).
 - No person, except the registered owner of the motor vehicle that contains the event data recorder, or the registered owner's representative, may retrieve, obtain or use data stored on or transmitted from the event data recorder unless:
 - (A) The individual who is the registered owner or lessee of the motor vehicle at the time the data is retrieved, obtained or used, or the individual's representative, consents in writing;
 - (B) The data is retrieved or obtained by a peace officer, as defined in section 53a-3, pursuant to a search warrant issued by a judge of

the Superior Court or a judge trial referee under the provisions of section 54- 33a, or by any court of competent jurisdiction;

- (C) The data is used for the purpose of improving motor vehicle safety, security or traffic management, including the purpose of medical research on physical reaction to motor vehicle accidents, provided the identity of the registered owner, lessee, operator or other occupant of the motor vehicle is not disclosed with respect to the data, except that the disclosure of a vehicle identification number with the last six numbers deleted for such purposes shall not constitute disclosure of the identity of the registered owner, lessee, operator or other occupant;
- (D) The data is retrieved or obtained by a licensed new car dealer, as defined in section 14-51, a repairer, as defined in section 14-51, or the manufacturer, as defined in section 14-1, that manufactured the motor vehicle, and used for the purpose of diagnosing, servicing or repairing the motor vehicle; or
- (E) The data is retrieved or obtained pursuant to a legally proper discovery request or order in a civil action.
- Data from an event data recorder may be retrieved, obtained and used by a subscription service provider pursuant to a subscription agreement if the subscription agreement discloses that the data may be stored and transmitted.
- No person may knowingly alter or delete data on an event data recorder, or knowingly destroy an event data recorder, after a crash event that resulted in a death or a serious physical injury, as defined in section 53a-3, within a reasonable amount of time sufficient for a peace officer to obtain a search warrant.
- **Maine**
 - Me. Rev. Stat. Ann. tit. 29, § 1972 (2009).
 - Data recorded on an event data recorder may not be downloaded or otherwise retrieved by a person other than the owner of the motor vehicle at the time the data are accessed, except under the following circumstances:
 - A. The owner of the motor vehicle or the owner's agent or legal representative consents to the retrieval of the information;
 - B. A court of competent jurisdiction in this State orders the production of the data;
 - C. For purposes of improving motor vehicle safety, security or traffic management, including medical research on the human body's reaction to motor vehicle crashes, as long as the identity of the owner or driver is not disclosed in connection with that retrieved data. For the purposes of this paragraph, the disclosure of the vehicle identification number with the last 4 digits deleted does not constitute the disclosure of the identity of the owner or driver;

- D. The data are retrieved by a licensed motor vehicle dealer or by an automotive technician for the purpose of diagnosing, servicing or repairing the motor vehicle;
 - E. The data are retrieved for the purpose of determining the need for or facilitating emergency medical response in the event of a motor vehicle crash;
 - F. The data are retrieved by a law enforcement officer acting pursuant to authority recognized under applicable statutory or constitutional law; or
 - G. The data are requested as part of routine civil or criminal discovery.
- Release of data prohibited; exceptions. A person, including a service or data processor operating on behalf of such person, authorized to download or otherwise retrieve data from the event data recorder pursuant to subsection 1, paragraph C may not release the data except:
 - A. For the purpose of motor vehicle safety and medical research communities to advance motor vehicle safety, security or traffic management; or
 - B. To a data processor solely for the purposes permitted by this subsection only if the identity of the owner or driver is not disclosed.
- Me. Rev. Stat. Ann. tit. 29, § 1973 (2009).
 - A manufacturer of a new motor vehicle sold or leased in this State that is equipped with one or more event data recorders, including those known as “sensing and diagnostic modules,” shall disclose that fact in the owner's manual for the motor vehicle.
- **Nevada**
 - Nev. Rev. Stat. Ann. § 484.638 (2008).
 - A manufacturer of a new motor vehicle which is sold or leased in this State and which is equipped with an event recording device shall disclose that fact in the owner's manual for the vehicle.
 - Except as otherwise provided in this section, data recorded by an event recording device may not be downloaded or otherwise retrieved by a person other than the registered owner of the vehicle.
 - Exceptions to release data:
 - (a) If the registered owner of the vehicle consents to the retrieval of the data.
 - (B) Pursuant to the order of a court of competent jurisdiction.
 - (c) If the data is retrieved for the purpose of conducting research to improve motor vehicle safety, including, without limitation, conducting medical research to determine the reaction of a human body to motor vehicle accidents, provided that the identity of the registered owner or driver is not disclosed in connection with the retrieval of that data. The disclosure of a vehicle identification number pursuant to this paragraph does not constitute the

person other than the owner of the motor vehicle at the time the data is accessed, except under one of the following circumstances:

- (a) The owner of the motor vehicle or the owner's agent or legal representative consents to the retrieval of the information.
- (b) In response to an order of a court or other judicial or administrative authority having jurisdiction to issue the order.
- (c) For the purpose of improving motor vehicle safety, security or traffic management including for medical research of the human body's reaction to motor vehicle crashes, provided that the identity of the registered owner or driver is not disclosed in connection with that retrieved data. For purposes of this section the disclosure of the vehicle identification number (VIN) with the last four digits deleted, does not constitute the disclosure of the identity of the registered owner or driver.
- (d) The data is retrieved by a licensed new motor vehicle dealer as defined in section four hundred fifteen of this article or by an automotive technician trained in such retrieval and employed by a registered motor vehicle repair shop as defined in article twelve-A of this chapter, for the purpose of diagnosing, servicing, or repairing the motor vehicle.
- (e) The data is retrieved for the purpose of determining the need for or facilitating emergency medical response in the event of a motor vehicle crash.

- **North Dakota**

- N.D. Cent. Code. § 51-07-28 (2009).

- A manufacturer of a new motor vehicle sold or leased in this state which is equipped with a recording device commonly referred to as an event data recorder shall disclose by model year 2007 the presence, capacity, and capabilities of the event data recorder in the owner's manual for the vehicle. A motor vehicle dealer shall include within the purchase contract in a clear and conspicuous manner information on the possibility of a recording device.
- Data recorded on an event data recorder may not be downloaded or otherwise retrieved by a person other than the owner of the motor vehicle at the time the data is recorded, or through consent by the owner's agent or legal representative, except under any of the following circumstances:
 - a. The data is retrieved for the purpose of improving motor vehicle safety, including for medical research of the human body's reaction to motor vehicle accidents, and the identity of the registered owner or driver is not disclosed in connection with that retrieved data. The disclosure of the vehicle identification number, with the last four digits deleted, for the purpose of improving vehicle safety, including for medical research of the human body's reaction to motor vehicle accidents, does not constitute the disclosure of the identity of the registered owner or driver. A person authorized to download or otherwise retrieve data from a recording device under

this subdivision may not release that data, except to share the data among the motor vehicle safety and medical research communities to advance motor vehicle safety, and only if the identity of the registered owner or driver is not disclosed.

- b. The data is retrieved by a licensed motor vehicle dealer or by an automotive technician for the purpose of diagnosing, servicing, or repairing the motor vehicle.
 - c. By stipulation of the parties to the proceeding or by order of the court.
 - An insurer may not require as a condition of insurability consent of the owner for access to data that may be stored within an event data recorder and may not use data retrieved with the owner's consent before or after an accident for the purpose of rate assessment.
- **Oregon**
 - Or. Rev. Stat. Ann. § 105.928 (2009).
 - Except as specifically provided under ORS 105.925 to 105.945, the data on a motor vehicle event data recorder is exclusively owned by the owner of the motor vehicle and may not be retrieved or used by any person other than the owner of the motor vehicle without the written consent of the owner. If a motor vehicle is owned by more than one person, all owners must consent to the retrieval or use of the data from a motor vehicle event data recorder.
 - Or. Rev. Stat. Ann. § 105.925 (2009).
 - Owner" means a person:
 - (a) In whose name a motor vehicle is registered or titled;
 - (b) Who leases a motor vehicle for at least three months;
 - (c) Who is entitled to possession of a motor vehicle as the purchaser under a security agreement; or
 - (d) Who is the attorney in fact, conservator or personal representative for a person described in paragraphs (a) to (c) of this subsection.
 - Or. Rev. Stat. Ann. § 105.932 (2009).
 - (1) Data on a motor vehicle event data recorder does not become the property of a lienholder or insurer solely because the lienholder or insurer succeeds in ownership of a motor vehicle as a result of an accident.
 - (2) An insurer may not condition the payment or settlement of an owner's claim on the owner's consent to the retrieval or use of the data on a motor vehicle event data recorder.
 - (3) An insurer or lessor of a motor vehicle may not require an owner to consent to the retrieval or use of the data on a motor vehicle event data recorder as a condition of providing the policy or lease.
 - Or. Rev. Stat. Ann. § 105.935 (2009).
 - Data from a motor vehicle event data recorder may be retrieved or used without the consent of the owner after an accident if a court orders the production of the data based on a determination by the court that:

- (1) A law enforcement officer has probable cause to believe that a crime has occurred and that the data is relevant to the investigation of the crime; or
- (2) A law enforcement officer, firefighter or emergency medical services provider seeks to obtain the data in the course of responding to or investigating an emergency involving the physical injury or the risk of physical injury to any person.
- Or. Rev. Stat. Ann. § 105.938 (2009).
 - (1) Upon petition of an insurer, a court may order that data from a motor vehicle event data recorder be retrieved or used without the consent of the owner of the motor vehicle after an accident if the court determines that:
 - (a) The owner has a policy of insurance for the vehicle issued by the insurer;
 - (b) The data is necessary to reconstruct the facts of the accident and to allow the insurer to determine the obligations of the insurer under the insurance policy; and
 - (c) An accurate and timely determination of the facts of the accident cannot occur without the data.
 - (2) A petition under this section must be filed in the circuit court for the county in which the owner of the motor vehicle resides. The petition must be served on the owner in the manner provided by ORCP 7 not less than 30 days before a hearing on the petition. An insurer filing a petition under this section must pay the filing fee specified by ORS 21.110.
- Or. Rev. Stat. Ann. § 105.942 (2009).
 - (1) Data from a motor vehicle event data recorder may be retrieved or used without the consent of the owner to facilitate or determine the need for emergency medical care for the driver or passenger of a motor vehicle that is involved in a motor vehicle crash or other emergency, including the retrieval of data from a company that provides subscription services to the owner of a motor vehicle for in-vehicle safety and security communications systems.
 - (2) Data from a motor vehicle event data recorder may be retrieved or used without the consent of the owner to facilitate medical research of the human body's reaction to motor vehicle crashes if:
 - (a) The identity of the owner or driver is not disclosed in connection with the retrieved data; and
 - (b) The last four digits of the vehicle identification number are not disclosed.
 - (3) Data from a motor vehicle event data recorder may be retrieved or used without the consent of the owner to diagnose, service or repair a motor vehicle.
- Or. Rev. Stat. Ann. § 105.945 (2009).
 - ORS 105.925 to 105.945 do not apply to data that is stored or transmitted pursuant to a subscription service agreement for the use of a recording device to record a history of where a motor vehicle travels or for the transmission of data to a central communications system.

- **Texas**
 - Tex. Transp. Code Ann. § 547.615 (2009).
 - A manufacturer of a new motor vehicle that is sold or leased in this state and that is equipped with a recording device shall disclose that fact in the owner's manual of the vehicle.
 - Information recorded or transmitted by a recording device may not be retrieved by a person other than the owner of the motor vehicle in which the recording device is installed except:
 - (1) on court order;
 - (2) with the consent of the owner for any purpose, including for the purpose of diagnosing, servicing, or repairing the motor vehicle;
 - (3) for the purpose of improving motor vehicle safety, including for medical research on the human body's reaction to motor vehicle accidents, if the identity of the owner or driver of the vehicle is not disclosed in connection with the retrieved information; or
 - disclosure of a motor vehicle's vehicle identification number with the last six digits deleted or redacted is not disclosure of the identity of the owner or driver; and
 - retrieved information may be disclosed only:
 - (4) for the purpose of determining the need for or facilitating emergency medical response in the event of a motor vehicle accident.
- **Virginia**
 - Va. Code Ann. § 46.2-1088.6 (2009).
 - “Recording device” means an electronic system, and the physical device or mechanism containing the electronic system, that primarily, or incidental to its primary function, preserves or records, in electronic form, data collected by sensors or provided by other systems within the vehicle. “Recording device” includes event data recorders (EDRs), sensing and diagnostic modules (SDMs), electronic control modules (ECMs), automatic crash notification (ACN) systems, geographic information systems (GIS), and any other device that records and preserves data that can be accessed related to that vehicle.
 - Recorded data may only be accessed by the motor vehicle owner or with the consent of the motor vehicle owner or the owner's agent or legal representative; except under the following circumstances:
 - 1. The owner of the motor vehicle or the owner's agent or legal representative has a contract with a third-party subscription service that requires access to a recording device or recorded data in order to perform the contract, so long as the recorded data is only accessed and used in accordance with the contract;
 - 2. A licensed new motor vehicle dealer, or a technician or mechanic at a motor vehicle repair or servicing facility requires access to recorded data in order to carry out his normal and ordinary diagnosing, servicing, and repair duties and such recorded data is used only to perform such duties;

- 3. The recorded data is accessed by an emergency response provider and is used only for the purpose of determining the need for or facilitating an emergency response. Such persons are authorized to receive data transmitted or communicated by any electronic system of a motor vehicle that constitutes an automatic crash notification system and utilizes or reports data provided by or recorded by recording devices installed on or attached to a motor vehicle to assist them in performing their duties as emergency response providers;
- 4. Upon authority of a court of competent jurisdiction; or
- 5. The recorded data is accessed by law enforcement in the course of an investigation where constitutionally permissible and in accordance with any applicable law regarding searches and seizures upon probable cause to believe that the recording device contains evidence relating to a violation of the laws of the Commonwealth or the United States.
- The consent of the motor vehicle owner or the owner's agent or legal representative for use of recorded data for purposes of investigating a motor vehicle accident or insurance claim shall not be requested or obtained until after the event giving rise to the claim has occurred, and shall not be made a condition of the defense, payment or settlement of an obligation or claim.
- When the recording device and recorded data are not removed or separated from the motor vehicle, the ownership of the recording device and recorded data survives the sale of the motor vehicle to any nonbeneficial owner such as an insurer, salvage yard, or other person who does not possess and use the motor vehicle for normal transportation purposes.
-
- **Washington (Effective July 1, 2010)**
 - Wash. Rev. Code Ann. § 46.35.010 (2010).
 - "Recording device" includes event data recorders, sensing and diagnostic modules, electronic control modules, automatic crash notification systems, geographic information systems, and any other device that records and preserves data that can be accessed related to that motor vehicle. "Recording device" does not include onboard diagnostic systems whose exclusive function is to capture fault codes used to diagnose or service the motor vehicle.
 - Wash. Rev. Code Ann. § 46.35.020 (2010).
 - A manufacturer of a motor vehicle sold or leased in this state, that is equipped with one or more recording devices, shall disclose in the owner's manual that the motor vehicle is equipped with one or more recording devices and, if so, the type of data recorded and whether the recording device or devices have the ability to transmit information to a central communications system or other external device.

- If a recording device is used as part of a subscription service, the subscription service agreement must disclose the type of information that the device may record or transmit.
 - Disclosure made in writing is deemed a disclosure in the owner's manual.
 - If a recording device is to be installed in a vehicle aftermarket, the manufacturer or distributor of the device shall disclose in the product manual the type of information that the device may record and whether the recording device has the ability to transmit information to a central communications system or other external device.
 - Disclosure made in writing is deemed a disclosure in the product manual.
- Wash. Rev. Code Ann. § 46.35.030 (2010).
- Information recorded or transmitted by a recording device may not be retrieved, downloaded, scanned, read, or otherwise accessed by a person other than the owner of the motor vehicle in which the recording device is installed except:
 - Upon a court order or pursuant to discovery. Any information recorded or transmitted by a recording device and obtained by a court order or pursuant to discovery is private and confidential and is not subject to public disclosure;
 - With the consent of the owner, given for a specific instance of access, for any purpose;
 - For improving motor vehicle safety, including medical research on the human body's reaction to motor vehicle collisions, if the identity of the motor vehicle or the owner or driver of the motor vehicle is not disclosed in connection with the retrieved information;
 - The disclosure of a motor vehicle's vehicle identification number with the last six digits deleted or redacted is not a disclosure of the identity of the owner or driver; and
 - Retrieved information may only be disclosed to a data processor.
 - For determining the need for or facilitating emergency medical response if a motor vehicle collision occurs, provided that the information retrieved is used solely for medical purposes; or
 - For subscription services pursuant to an agreement in which disclosure required under RCW 46.35.020 of this act has been made, provided that the information retrieved is used solely for the purposes of fulfilling the subscription service.
 - Information that can be associated with an individual and that is recorded or transmitted by a recording device may not be sold to a third party unless the owner of the information explicitly grants permission for the sale.
 - Any person who violates this section is guilty of a misdemeanor.

FEDERAL CIRCUIT COURT DECISIONS

FIRST CIRCUIT PRIVACY LAW

- **Public Records**
 - Fed. Labor Relations Authority v. U.S. Dep't of Navy, 941 F.2d 49 (1st Cir. 1991) The court held also that the "routine use" exception to the Privacy Act did not permit disclosure in this case since there was no showing made of the nonexistence of adequate alternative means to communicate with the employees. Thus, the court held that the Privacy Act did not permit the disclosure of the employees' addresses.
 - United States v. Innamorati, 996 F.2d 456 (1st Cir. 1997) - The motor vehicle registry is not prima facie a public record.
- **Consumer Credit**
 - Sullivan v. Greenwood Credit Union, 520 F.3d 70 (1st Cir. 2008) Interpreting the Fair Credit Reporting Act, 15 U.S.C.S. § 1681 et seq., as ensuring fair and accurate credit reporting, promoting efficiency in the banking system, and protecting consumer privacy. The court found that a letter from a credit union did not guarantee Sullivan a loan, but did guarantee that he would not be disqualified from a loan on the basis of the pre-selection criteria. In turn, there was little invasion of consumer privacy. The credit union never received Sullivan's full credit report. It received only the plaintiff's contact information and that he met certain pre-selection criteria. This is a minimal invasion of privacy, offset by the value of the information in the letter to the plaintiff.
- **Financial Records**
 - Nuby v. South Boston Sav. Bank, No. 98-1294, 1998 U.S. App. LEXIS 26094 (1st Cir. 1998) - The bank customer filed an action against the bank alleging that the bank violated the Right to Financial Privacy Act, 12 U.S.C. § 3401(3), by permitting the state Department of Welfare to have access to his bank records. The court held that the Act defined the kind of "government authority" subject to the Act's requirements as limited to any agency or department of the United States, or any officer, employee, or agent thereof. Thus, requests for bank records by state agencies were not covered by the Act. As a result, the customer had no cause of action against the bank under the Act.
 - United States v. Connolly (In re Boston Herald, Inc.), 321 F.3d 174 (1st Cir. 2003) - The defendant in a highly publicized criminal trial applied for government funding of a portion of his attorneys' fees and costs under the CJA. He submitted financial affidavits and a document summarizing his total legal debt, and successfully moved to place the documents under seal. A newspaper tried to unseal the documents. The court held that there was no right of access to the defendant's financial documents under either U.S. Const. Amend. I or common law. Even if there was a common law presumption of access, the magistrate did not abuse its discretion by denying access because defendant had a strong interest in the privacy of his and his family's personal financial information outweighing any common law presumption.
 - Alinovi v. Worcester School Comm., 777 F.2d 776 (1st Cir. 1985) - Citing United States v. Miller with approval. "In Miller, for example, the Supreme Court held that a bank depositor has no legitimate expectation of privacy in financial information voluntarily conveyed to banks and exposed to their employees in the ordinary course of business. The Court emphasized: The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government. . . . This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed. 425 U.S. at 443. Thus, the court in Miller reasoned that because the depositor had "assumed the risk" of disclosure, it would be unreasonable for him to expect his financial records to remain private. The conclusion which can be drawn from this is that "the Fourth Amendment is implicated only if the authorities use information with respect to which the expectation of privacy has not already been frustrated." United States v. Jacobsen, 466 U.S. 109 (1984).
- **Electronic Surveillance**

- United States v. Rodriguez-Morales, 929 F.2d 780 (1st Cir. 1991) - The driver of a car on a public highway is considered to have a diminished expectation of privacy with regard to his vehicle.
- United States v. Johnson, 952 F.2d 565 (1st Cir. 1991) - The court affirmed and held that after reviewing the government's FISA applications, it was clear that the primary purpose of the surveillance was to obtain foreign intelligence information, not to collect evidence for any criminal prosecution. The court found that the surveillance was all directed to activities related to defendants' support of a political group's operations in Northern Ireland.
- United States v. Councilman, 418 F.3d 67 (1st Cir. 2005) An e-mail message does not cease to be an "electronic communication" during the momentary intervals, intrinsic to the communication process, at which the message resides in transient electronic storage. Although the text of the statute does not specify whether the term "electronic communication" includes communications in electronic storage, the legislative history of the ECPA indicates that Congress intended the term to be defined broadly. Furthermore, that history confirms that Congress did not intend, by including electronic storage within the definition of wire communications, to thereby exclude electronic storage from the definition of electronic communications. We therefore conclude that the term "electronic communication" includes transient electronic storage that is intrinsic to the communication process, and hence that interception of an e-mail message in such storage is an offense under the Wiretap Act. Moreover, the various doctrines of fair warning do not bar prosecution for that offense.
- Vega-Rodriguez v. Puerto Rico Tel. Co., 110 F.3d 174 (1st Cir. 1997) - holding that employees of a quasi-public telephone company had no legitimate expectation to be free from video-taping in "an open and undifferentiated work area."
- In re Application for Interception of Wire Communications, 2 F.Supp.2d 177 (D. Mass. 1998) - showing concern over the necessity of the "powerful, but intrusive weapon of electronic surveillance" and requiring that the government be completely forthright in its use of informants and the completeness of applications for such interceptions.
- United States v. Moore, 562 F.2d 106 (1st Cir. 1977) We and other courts have upheld the placing of beepers, without warrant, in contraband, stolen goods and the like on the theory that the possessors of such articles have no legitimate expectation of privacy in substances which they have no right to possess at all. But in legally possessed goods (although having the possibility the goods will be used for illegal purposes), there is a warrant requirement for beepers that track the movement objects that ultimately end up in a person's home, where there is a great expectation of privacy.
 - While we hold that both uses of beepers intruded to some degree upon defendants' reasonable privacy expectations, we believe that the privacy interest affected by using a beeper to maintain surveillance of a vehicle on public roads is much less than in the later instance. We hold, therefore, that given probable cause, no warrant was required for the vehicular surveillance. And the trespass involved in affixing the beepers to the underbody of the vehicles was, standing alone, so minimal as to be of little consequence. The key is probable cause. There is some expectation of privacy in not being monitored continuously while driving on a public road.
 - But the chemicals containing the transmitter were not contraband or otherwise wrongfully in appellees' possession, the Government had no right to determine their continued presence in the house by use of warrantless electronic surveillance. This is a Fourth Amendment violation, but requires more investigation whether suppressing this evidence really causes suppression of the whole case. The government could have formed an independent basis to get the warrant to search the house based on following the car and other external evidence like the smell of ether.
- United States v. Padilla, 520 F.2d 526, 527-28 (1st Cir. 1975), which held that the defendant's Fourth Amendment rights were violated when agents placed an audio recording device in the defendant's hotel room and recorded conversations between the defendant and another person who consented to the recordings. In reaching this conclusion, the First Circuit expressed concern that if law enforcement officers were permitted to leave a monitoring or recording device in a hotel for a lengthy period of time the officers would be tempted to monitor or record conversations that occurred when no consenting participant was present.

- **Computer Statutes**

- United States v. Czubinski, 106 F.3d 1069 (1st Cir. 1997) - The court reversed defendant's convictions for wire fraud and computer fraud under federal statutes. It held that the evidence was insufficient to support the guilty verdicts and that the unauthorized computer browsing of a taxpayers' files, although inappropriate, would not rise to the level of a federal felony charges.

SECOND CIRCUIT PRIVACY LAW

- **Public Records**
 - Motor vehicle records generally are public records. *See* United States v. Nanni, 59 F.3d 1425 (2d Cir. 1995).
 - Florio v. General Acci. Fire & Life Assurance Corp., 396 F.2d 510 (2d Cir. 1968) Noting that the existence of insurance coverage and the identity of the carrier are now a matter of public record and can readily be obtained from departments of motor vehicles.
- **Consumer Credit**
 - United States v. Tanimowo, No. 99-1029, 1999 U.S. App. LEXIS 28029 (2d Cir. 1999) - using a computer to access consumer credit information is a felony.
- **Public or Mass Transit**
 - Cassidy v. Chertoff, 471 F.3d 67 (2d Cir. 2006) - Plaintiffs challenged searches conducted on ferries per the Maritime Transportation Security Act of 2002 (MTSA), 46 U.S.C.S. §§ 70101-70119. The searches included the carry-on baggage of randomly selected passengers and inspecting randomly selected vehicles. The court found that the searches were minimally intrusive and the prevention of terrorist attacks on large vessels engaged in mass transportation and determined by the Coast Guard to be at heightened risk of attack constituted a special need.
 - MacWade v. Kelly, 460 F.3d 260 (2d Cir. 2006) - The disputed program, which was implemented in response to terrorist attacks on subways in other cities, was designed to deter terrorists from carrying concealed explosives onto the city's subway. The city program established daily inspection checkpoints at selected subway facilities where officers searched bags that met size criteria for containing explosives. Subway riders wishing to avoid a search were required to leave the station. The court found that the program was reasonable and therefore constitutional. In particular, the court found that preventing a terrorist attack on the subway was a special need, which was weighty in light of recent terrorist attacks on subway systems in other cities. In addition, the court found that the disputed program was a reasonably effective deterrent. Although the searches intruded on a full privacy interest, the court further found that such intrusion was minimal, particularly as inspections involved only certain size containers and riders could decline inspection by leaving the station.
- **Individual Privacy**
 - United States v. Amerson, 483 F.3d 73 (2d Cir. 2007) The Justice For All Act of 2004, Pub. L. No. 108-405, 118 Stat. 2260, requires federal offenders convicted of any felony to supply a sample of their DNA for analysis and storage in the Combined DNA Index System, a national database administered by the Federal Bureau of Investigation and the Bureau of Prisons. As a result, persons convicted of crimes that are neither violent nor sexual in nature are also required to deposit a DNA sample for analysis and storage. This is not violative of the Fourth Amendment. that the state likely already had a plethora of identifying information about defendants, in light of their status as convicted felons, the additional intrusion of privacy entailed by the taking of the DNA sample was small.
 - United States v. Lifshitz, 369 F.3d 173 (2d Cir. 2004) - Although the Fourth Amendment offers protection against searches of home computers, the "special needs" of the probation system are sufficient to justify conditioning Lifshitz's probation upon his agreement to submit to computer monitoring. The scope of the computer monitoring condition as it stands may, however, be overbroad because there were less intrusive ways (compared to the amount of information obtained) to monitor what websites Lifshitz visited.
 - Leventhal v. Knapek, 266 F.3d 64, 73 (2d Cir. 2001) - holding that an employee "had a reasonable expectation of privacy in the contents of his office computer."
- **Financial Records**
 - United States v. First Bank, 737 F.2d 269 (2d Cir. 1984) - Despite the fact that a Connecticut statute gave all co-owners of a bank account equal ownership of the account, the IRS was not required to give notice to co-owner of a summons if the co-owner was not identified in the summons.
 - Inner City Press/Community on the Move v. Bd. of Governors of the Fed. Reserve Sys., No. 05-6162-cv (L) & 05-6628-cv (XAP), 2006 U.S. App. LEXIS 28730 (2d Cir. 2006) - In the merger

application, the bank voluntarily included information about its relationships with subprime lenders. The district court held that the names of the bank's subprime-lending customers and the descriptions of other services the bank provided to these customers qualified as confidential commercial information under 5 U.S.C.S. § 552(b)(4). The § 552(b)(4) exemption did not apply to information that was already in the public domain.

- Young v. United States Dep't of Justice, 882 F.2d 633 (2d Cir. 1989) - we believe Congress intended the [Right to Financial Privacy Act] to regulate the release of customer information from financial institutions in circumstances where adequate controls did not already exist. The subpoena served on Chemical, "so-ordered" by a district court, was not in this category because it was subject to judicial review even before it was served. It thus received the same, if not higher, level of scrutiny given grand jury subpoenas. Construing the Act so as not to apply in such circumstances would be consistent with congressional intent.
- **Electronic Surveillance**
 - Tabbaa v. Chertoff, 509 F.3d 89 (2d Cir. 2007) All persons seeking entry into the United States are subject to search and detention by officers of the U.S. Bureau of Customs and Border Protection (CBP), and CBP, as a matter of standard operating procedure, may refer individuals for a secondary inspection that can include the collection of biometric information such as fingerprints or photographs.
 - In Re Site Cell Information, 396 F. Supp. 2d 294 (E.D.N.Y. 2005) - can't track a person using cell phone GPS without probable cause. The expectation of privacy is too high because the cell phone enters the home and other places with a reasonable expectation of privacy. The court reasoned that the government's planned use of a mobile telephone as a means for contemporaneously tracking the movements of its user impacted Congress's compromise between effective law enforcement and individual privacy rights and required a showing of probable cause.
 - United States v. Depalma, 2008 U.S. App. LEXIS 13733 (2d Cir. 2008) - upholding constitutionality of 18 U.S.C.S. § 2518 (11), the statute authorizing the use of "roving bugs." In this case the surveillance orders permitted the installation of a tracking device on the exterior of his cell phone. This comported with the requirements of the Fourth Amendment.
 - United States v. Myers, 692 F.2d 823 (2d Cir. 1982). A defendant was videotaped during a meeting with a government informant at a townhouse maintained by the FBI (ie one party consented, but wasn't wearing a wire). Rejecting the defendant's Fourth Amendment argument, the Court stated that the defendant's "conversations with undercover agents in whom he chose to confide were not privileged, and mechanical recordings of the sights and sounds to which the agents could have testified were proper evidence." Didn't matter that the video tape had the potential of recording persons who have not consented to communication.
- **Computer Statutes**
 - United States v. Irving, 452 F.3d 110 (2d Cir. 2004) court upheld the denial of a motion to suppress child pornography found on computer diskettes during a routine border search, ruling that the agents were "entitled to inspect the contents of the diskettes even absent reasonable suspicion. Indeed, any other decision effectively would allow individuals to render graphic contraband, such as child pornography, largely immune to border search simply by scanning images onto a computer disk before arriving at the border."

THIRD CIRCUIT PRIVACY LAW

- **Public Records**

- Pichler v. Unite 542 F.3d 380 (3d Cir. 2008) - The union, which sought to contact employees as part of a union organizing campaign, used license plate numbers on cars found in an employer's parking lots to access information in motor vehicle records. The Driver Privacy Protection Act provides redress for violation of a person's protected interest in the privacy of his or her motor vehicle records and the identifying information therein. A court will not engraft upon the DPPA a "labor exception" that would permit unions to acquire and use employees' personal information, obtained from motor vehicle records, to contact them during organizing campaigns. The United States Court of Appeals for the Third Circuit declines to recognize an exception to the statute for which Congress has not provided.
- United States v. Hardy, 2008 U.S. App. LEXIS 13242 (3d Cir. 2008) - Noting that with regard to the Commerce Clause argument, the United States Supreme Court had held that personal information contained in a Department of Motor Vehicles' record was a "thing" in interstate commerce, and that the Commerce Clause authorized Congress to regulate the sale or release of such information.

- **Individual Privacy & Technological Record Keeping**

- United States v. Hardy, 2008 U.S. App. LEXIS 13242 (3d Cir. 2008) - As probationer, Harvey's expectation of privacy is reduced below that of an ordinary citizen, and such rights were not violated by the requirement that he provide a DNA sample.
- Sultana v. AG of the United States, 2008 U.S. App. LEXIS 20538 (3d Cir. 2008) Permitting the Department of Homeland Security with to require Sultana, an alien, to submit her biometric information for their databases.
- United States v. Mitchell, 365 F.3d 215 (3d Cir. 2004) - Suggesting that widespread commercial use of biometric identification technology based on fingerprints. It is possible that commercial adoption of the method signals acceptance of its reliability.

- **Consumer Credit**

- Cushman v. Trans Union Corp., 115 F.3d 220 (3d Cir. 1997) - When a consumer disputes information that has been placed on her credit report, in the event the dispute is not resolved, the consumer may file a brief statement setting forth the nature of the dispute. 15 U.S.C.S. § 1681i(b). The statement or a summary must be included in the consumer's credit report.

- **Financial Records**

- Gannet v. First Nat'l State Bank, 546 F.2d 1072 (3d Cir. 1976) There is no legitimate expectation of privacy in the contents of records maintained by the banks under the mandate of the Bank Secrecy Act of 1970. Cited United States v. Miller, 435 U.S. 435 (3d Cir. 1976) with approval:
 - checks are not confidential communications but negotiable instruments to be used in commercial transactions. All of the documents obtained including financial statements and deposit slips, contain only information voluntarily conveyed to banks and exposed to their employees in the ordinary course of business. The lack of any legitimate expectation of privacy concerning the information kept in bank records was assumed by Congress in enacting the Bank Secrecy Act, the expressed purpose of which is to require records to be maintained because they 'have a high degree of usefulness in criminal, tax, regulatory investigations and proceedings.' . . .
 - "The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the government."

- **Electronic Surveillance**

- United States v. George, No. 08-1515, 2009 U.S. App. LEXIS 2749 (3d Cir. 2009) - no legitimate expectations of privacy with respect to the tracking device while driving his vehicle on public roadways.
- United States v. Lee, 359 F.3d 194 (3d Cir. 2004) The United States Court of Appeals for the Third Circuit does not agree with the United States Court of Appeals for the First Circuit that it is appropriate to suppress recordings of meetings between a defendant and a cooperating individual simply because the recording device was placed in a room rather than on the cooperating individual's person. Not a violation of the Fourth Amendment.

- To be sure, there are three circumstances in which this distinction would matter for Fourth Amendment purposes. First, if the defendant had an expectation of privacy in the premises at the time when the device was installed, the entry to install the device would constitute a search.
- Second, the cases involving consensual monitoring do not apply if recordings are made when the cooperating individual is not present.
- Third, the logic of those cases is likewise inapplicable if the placement of the recording device permits it to pick up evidence that the cooperating individual could not have heard or seen while in the room.
- Unless one of these circumstances is present, however, it does not matter for Fourth Amendment purposes whether the device is placed in the room or carried on the person of the cooperating individual. In either event, the recording will not gather any evidence other than that about which the cooperating witness could have testified.
- United States v. Mosley, 454 F.3d 249 (3d Cir. 2009) - Judicial precedent establishes a bright-line rule that any technical violation of a traffic code legitimizes a stop, even if the stop is merely pretext for an investigation of some other crime.
 - Passengers in cars, unlike owners or licensees, have no reasonable expectation of privacy in the interior of the vehicle in which they are riding. Passengers are generally held to lack standing to object to evidence discovered in a search of a vehicle.
 - Fourth Amendment rights are personal rights, and a search of a car does not implicate the rights of non-owner passengers: the car is treated conceptually like a large piece of clothing worn by the driver.
 - BUT it is settled law that a traffic stop is a seizure of everyone in the stopped vehicle. Thus, passengers in an illegally stopped vehicle have standing to object to the stop, and may seek to suppress the evidentiary fruits of that illegal seizure under the fruit of the poisonous tree doctrine. The dispositive legal issue is the causal relationship between the traffic stop and the discovery of the evidence: whether the evidence found in the car was fruit of the illegal stop.
- United States v. Whitted, 541 F.3d 480 (3d Cir. 2008) - customs officers were allowed to search Whitted's cabin of a cruise ship based on reasonable suspicion from Treasury Enforcement Communications System (TECS) indicated that authorities in San Juan, Puerto Rico had found defendant's behavior suspicious and entered a lookout for him into the TECS database.
- **Computer Statutes**
 - United States v. Olhovsky, No. 07-1642, 2009 U.S. App. LEXIS 7895 (3d Cir. 2009) - acceptable to seize computer and hard drive if there is probable cause.
 - United States v. Reyerros, 537 F.3d 270 (3d Cir. 2008) exceeding authorized access to a Customs computer was a violation of 18 U.S.C. § 1030(a)(2)(B).
 - United States v. Carlson, No. 05-3562, 2006 U.S. App. LEXIS 31740 (3d Cir. 2006) - Held that "Although the statute itself does not define "intentionally," this Court has defined it in the criminal context as performing an act deliberately and not by accident. Section 1030(e)(8) defines "damage" as "any impairment to the integrity or availability of data, a program, a system, or information. Accordingly, the Government was required to prove at trial that Carlson deliberately caused an impairment to the integrity or availability of data, a program, a system, or information.

FOURTH CIRCUIT PRIVACY LAW

- **Public Records**
 - nothing specifically on motor vehicle, driver records, or vehicle identification numbers.
- **Motor Vehicles**
 - United States v. Hargrove, 647 F.2d 411 (4 Cir. 1981) - Defendant has no reasonable expectation of privacy in a stolen car.
- **Consumer Credit**
 - Saunders v. Branch Banking & Trust Co., 526 F.3d 142 (4th Cir. 2008) - a creditor was properly denied a judgment as a matter of law because its failure to report to credit reporting agencies the disputed nature of a certain debt was misleading and inaccurate as a matter of law, and its failure to correct the error established that the FCRA violation was willful.
 - Hoke v. Retail Credit Corp., 521 F.2d 1079 (4th Cir. 1975) - Where an agency furnished a personal report requested to complete a customer's professional licensing approval, the report was for employment purposes and qualified as a consumer report subject to the Fair Credit Reporting Act.
- **Financial Records**
 - United States v. Hambrick, No. 99-4793, 2000 U.S. App. LEXIS 18665 (4th Cir. 2000) Citing *Miller* with approval. The Supreme Court concluded that the bank records subpoenaed in *Miller* were not "private papers" and that the defendant could assert neither ownership nor possession over these papers. Instead, the Supreme Court concluded that they were merely business records of the bank.
- **Public Transport**
 - United States v. Flowers, 912 F.2d 707 (4th Cir. 1990) - Noting that many cities have initiated drug interdiction programs in airports, train stations, and bus stations, similar to the one in Charlotte, North Carolina, that gave rise to the police conduct at issue here. These programs seek to assure the safety of passengers and to prevent public transport from becoming a haven for narcotics trafficking. They depend for their success upon voluntary interviews with passengers, searches of abandoned or unclaimed luggage, and/or searches pursuant to voluntary consent.
 - United States v. Whitehead, 849 F.2d 849 (4th Cir. 1988) - A police canine sniff of defendant's luggage on board a public train was constitutional where probable cause was not a prerequisite for the canine sniff and defendant's expectation of privacy was less when travelling on public transportation. Permitted police to enter Whitehead's sleeping compartment
 - Whitehead next contends that even if his expectation of privacy was no greater than that of an automobile occupant, the fourth amendment required the police to have more than a reasonable suspicion before they could bring their trained dogs into his compartment. He argues that probable cause must have supported the entry. Again, we disagree. Given Whitehead's reduced expectation of privacy in the roomette, the importance of the law enforcement interests at stake, and the minimal intrusiveness of the dog sniff, we conclude that probable cause was not a prerequisite for the dog sniff.
 - The governmental interest in preserving safe and efficient modes of public transportation necessarily leads to reduced expectations of privacy.
- **Electronic Surveillance**
 - United States v. Hammond, 286 F.3d 189 (4th Cir. 2002) - acceptable to tape inmates phone conversations under the law enforcement and consent exceptions to 18 U.S.C. §§ 2510 through 2519 (law enforcement wire, oral or electronic communications). The tapes can be used by law enforcement agencies if a subpoena is obtained, which does not require a showing of probable cause.
 - Brown v. Waddell, 50 F.3d 285 (4th Cir. 1995) - using a duplicate pager to intercept the numbers sent to a suspected drug dealer's pager was a "full-fledged eavesdropping device" and not just a pen register because the additional numeric characters sent to the pager could be used to convey coded messages.
 - The Production Of Real Time Cell Site Information, 402 F. Supp. 2d 597 (D. Md. 2005) - In furtherance of a criminal investigation, the government sought an order directing a wireless communications service provider to disclose "real time cell site information," which would reveal

the physical location of the person in possession of the cell phone whenever the phone was on. The issue presented was whether existing statutes allowed the government to obtain real time cell site information upon a showing of less than probable cause. The government's application was denied.

- United States v. Hambrick, No. 99-4793, 2000 U.S. App. LEXIS 18665 (4th Cir. 2000) While under certain circumstances, a person may have an expectation of privacy in content information, a person does not have an interest in the account information given to the internet service provider in order to establish the e-mail account, which is non-content information. Disclosure of this non-content information to a third party destroys the privacy expectation that might have existed previously.
- United States v. Watson, No. 06-4705; No. 06-4706, 2006 U.S. App. LEXIS 27293 (4th Cir. 2006) - affirming a district court's sentencing requirement that the conditions of supervised release include the conditions that, upon his release, he be subject to Global Positioning System ("GPS") electronic monitoring.
- United States v. Jones, 31 F.3d 1304 (4th Cir. 1994) - Defendant, while hauling United States mail, was suspected of stealing deposit envelopes from registered mail pouches. Postal inspectors placed an electronic transmitter in a deposit envelope; upon receiving a signal, defendant's private van was impounded under a warrant. A search of the van revealed the envelope with transmitter under the driver's seat. The court held that: 1) there was no Fourth Amendment search because the transmitter was concealed in a mail pouch, for which defendant had no expectation of privacy (the beeper was not planted in the van; it was concealed in a mail pouch which belonged to the government and in which Jones had no expectation of privacy whatsoever. The mail pouch with the beeper found its way into Jones' van only because Jones stole the pouch and hid it in the van himself.); 2) the warrant was supported by sufficient probable cause, and the inspectors' failure to keep within the precise scope of the warrant did not constitute the flagrant disregard needed for exclusion.
- **Computer**
 - United States v. Ickes, 393 F.3d 501 (4th Cir. 2005) - held that the need to be able to search for terrorist information trumps a defendant's interest in shielding "expressive materials" on a computer from border inspection, and that 19 U.S.C. § 1581, which authorizes inspection of "cargo" on "vessels or vehicles," allows the border inspection of computer files.

FIFTH CIRCUIT PRIVACY LAW

- **Public Records**
 - Innovative Database Sys. v. Morales, 990 F.2d 217 (5th Cir. 1993) - The court held that even though defendant state had a substantial interest in promoting the ethical standards of its licensed professionals, the laws totally banning use of lawfully obtained, public information to contact any person involved in a motor vehicle accident were too broad and insufficiently tailored to protect defendant's stated interests. The court held that the amendments were unconstitutional and affirmed the district court's grant of summary judgment in favor of plaintiff.
 - H.B. 922 prohibits the sale "for financial gain" of "motor vehicle accident information" obtained from the public records of a law enforcement agency. Plaintiffs argue that this also constitutes an unconstitutional restriction of commercial speech. The Supreme Court has repeatedly held that states may not prohibit the commercial publication of matters of public record.
 - Johnson v. Sawyer, 4 F.3d 369 (5th Cir. 1993) - government's publication of tax information was illegal under the Federal Tort Claims Act.
- **Consumer Credit**
 - Hood v. Dun & Bradstreet, Inc., 486 F.2d 25 (5th Cir. 1973) - The court reversed the decision of the district court, which granted appellee's motion for summary judgment in a libel action brought by appellant predicated upon allegedly false and defamatory statements published in a credit report. Matters of general and public interest did not include libelous and defamatory publications of such a commercial nature as credit reports, and appellee was not entitled to conditional privilege under Georgia law.
- **Financial Records**
 - Sandsend Financial Consultants, Ltd. v. Federal Home Loan Bank Bd., 878 F.2d 875 (5th Cir. 1989) - Plaintiff was not entitled to quash defendant's subpoena for financial records because it was a legitimate inquiry; the records were relevant to the inquiry; and defendant's service substantially complied with the statute.
- **Electronic Surveillance**
 - United States v. Cuevas-Sanchez, 821 F.2d 248 (5th Cir. 1987) - holding that installation of a surveillance camera on a power pole to videotape activities in a suspect's backyard constitutes a "search" within the meaning of the Fourth Amendment.
 - United States v. Mixon, 717 F. Supp. 1169 (E.D. La.), aff'd, 891 F.2d 904 (5th Cir. 1989) - required probable cause and a warrant for the installation of a beeper inside an aircraft to track its movements.
- **Computer Statutes**
 - White Buffalo Ventures, LLC v. Univ. of Texas, 420 F.3d 366 (5th Cir 2005) - an online dating service provider that targeted students at defendant public university, sought review of a summary judgment from the United States District Court for the Western District of Texas granted in favor of the university in the provider's action seeking to enjoin the university from blocking, pursuant to an anti-solicitation policy, the university's e-mail servers from receiving bulk commercial e-mails sent to students. Court held that commercial speech regulation was also permissible under U.S. Const. amend. I because of substantial state interest of user efficiency.

SIXTH CIRCUIT PRIVACY LAW

- **Public Records**
 - United States v. Tabaja, 2004 U.S. App. LEXIS 3596 (2004) - noting that motor vehicle registration is a public record available for judicial notice.
 - Northern Ky. Chiropractic v. Ramey, No. 95-5645, 1997 U.S. App. LEXIS 1734 (6th Cir. 1997) - It is doubtless true that by ending the practice of giving the general public access to accident reports, Kentucky made it much more difficult for Northern Kentucky Chiropractic to send targeted advertising materials to accident victims named in the reports. And if the Kentucky legislature had singled out advertisers such as Northern Kentucky Chiropractic for denial of access, a strong argument could be made that the statute should be analyzed as "a governmental erected obstruction to speech." But the Kentucky statute does not single out advertisers, it prohibits all citizens from having access to accident reports.
- **Consumer Credit**
 - Jones v. Federated Fin. Reserve Corp., 144 F.3d 961 (1998) - Directed verdict and jury instructions were improper where court did not apply apparent authority doctrine of liability to charges against defendant employer for willful and negligent noncompliance with Fair Credit Reporting Act.
- **Financial Records**
 - United States v. Sturman, 951 F.2d 1466 (6th Cir. 1991) - D maintains that, because of Switzerland's strict banking secrecy laws, he has a reasonable expectation of privacy protected by the Fourth Amendment. In support of his assertion of an expectation of privacy, he relies on the Swiss penalties of imprisonment or fine for revealing information and on the Treaty's goal of preserving the integrity of Swiss banking law.
 - In essence, the defendant argues a constitutional right created by the statutory rights granted him by a foreign country to records in that country. No such right of privacy in banking records is recognized in the United States.
 - United States v. Thomas, 878 F.2d 383 (6th Cir. 1989) Citizens have legitimate expectations of privacy in the contents of their safe deposit boxes. However, courts are not required to suppress evidence obtained as a result of the government's unauthorized access to a defendant's bank records.
 - In re Knoxville News-Sentinel Co., 723 F.2d 470 (6th Cir. 1983) BUT financial records are not public records. Congressional recognition of the confidentiality of financial records is illustrated in 5 U.S.C. § 552(b)(8). This provision exempts from disclosure under the Freedom of Information Act information compiled by government officials responsible for the regulation or supervision of financial institutions.
- **Electronic Surveillance**
 - United States v. Murdock, 63 F.3d 1391 (6th Cir. 1995) - 18 U.S.C. §§ 2510 through 2519 (interception wire, oral or electronic communications) appears to require suppression of illegally obtained evidence by the government and private parties. Circuits differ, but the principal exceptions for private parties to intercept communications without a warrant include: ordinary course of business exception if an employer believes and employee is revealing confidential information, interspousal wiretaps in preparation for divorce litigation, and family situations involving children.
 - Guest v. Leis, 255 F.3d 325, 333 (6th Cir. 2001) - asserting that "Users would logically lack a legitimate expectation of privacy in the materials intended for publication or public posting. They would lose a legitimate expectation of privacy in an e-mail that had already reached its recipient; at this moment, the e-mailer would be analogous to a letter-writer, whose expectation of privacy ordinarily terminates upon delivery of the letter."
 - United States v. Stewart, 746 F.2d 1480 (6th Cir. 1984) - Federal employee who used her private vehicle for the public purpose of delivering mail during work hours had no reasonable expectation of privacy in her vehicle during work hours. She was not entitled to suppress evidence discovered in her car.
- **Computer Statutes**

- United States v. Lewis, 872 F.2d 1030 (6th Cir, 1997) - requiring an intent to defraud when accessing a federally protected computer.

SEVENTH CIRCUIT PRIVACY LAW

- **Public Records**
 - Deicher v. City of Evansville, 545 F.3d 537 (7th Cir.) - The Driver's Privacy Protection Act prohibits anyone from obtaining or disclosing information from motor vehicle records, subject to certain exceptions. 18 U.S.C.S. § 2724(a). There is an exemption to Driver's Privacy Protection Act liability if the information was given to a third party for use in connection with any civil, criminal, administrative, or arbitral proceeding in any federal, state, or local court or agency or before any self-regulatory body, including the service of process, investigation in anticipation of litigation, and the execution or enforcement of judgments and orders, or pursuant to an order of a federal, state, or local court
- **Public Transit**
 - United States v. McDonald, 100 F.3d 1320 (7th Cir. 1996) - explaining the lesser expectation of privacy on a public bus because there is no guarantee the exterior of her bags would not be touched or felt by others when they were exposed on the overhead rack of a passenger bus. Nothing in the record indicated that the actions of investigating officers coerced defendant into abandoning her luggage.
- **Consumer Credit**
 - In re Trans Union Corp. Privacy Litig., No. 00 C 4729, 2002 U.S. Dist. LEXIS 17209 (N.D. Ill. 2002) - Nineteen individually named plaintiffs from several different states asserted a variety of claims against the consumer reporting agency. Plaintiffs asserted that the agency violated the FCRA and applicable state privacy laws by unlawfully disclosing private financial and confidential information to third parties for targeted marketing schemes. The court granted the agency's motion to dismiss the consumers' claims seeking injunctive relief because Congress had vested the power to obtain injunctive relief under the FCRA solely with the Federal Trade Commission.
- **Financial Records**
 - United States v. Residence Located at 218 Third Street, 805 F.2d 256 (7th Cir. 1986) - explaining that the Right to Financial Privacy Act represents a compromise between a bank customer's right of privacy in his financial records and law enforcement agencies' need to obtain financial records pursuant to legitimate investigations after the Supreme Court determined that there is no right of privacy in bank records in United States v. Miller. This case required a subpoena for bank records and search warrant for a safety deposit box.
- **Electronic Surveillance**
 - United States v. Myers, 692 F.2d 823 (2d Cir. 1982). A defendant was videotaped during a meeting with a government informant at a townhouse maintained by the FBI. Rejecting the defendant's Fourth Amendment argument, the Court stated that the defendant's "conversations with undercover agents in whom he chose to confide were not privileged, and mechanical recordings of the sights and sounds to which the agents could have testified were proper evidence." Didn't matter that the video tape had the potential of recording unconsented to communication.
 - Rahman v. Chertoff, 530 F.3d 622 (7th Cir. 2008) - The Government's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border. Searches made at the border, pursuant to the longstanding right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border. The United States is entitled to stop, and disassemble, any car or truck entering the United States at the border, without particularized suspicion. This includes utilizing biometric data in passports as the legislature deemed permissible.
- **Computer Statutes**
 - Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418 (7th Cir. 2006) - The employer lent the employee a laptop to use for work. The employee decided to quit the employer and go into business for himself, in breach of his employment contract. Before returning the laptop, the employee deleted all the data in it by transmitting a secure-erasure program to the computer, which was designed, by writing over the deleted files, to prevent their recovery. The court determined this was a violation

of 18 U.S.C. 1030 because it was intentional and because “damage” includes any impairment to the integrity or availability of data, a program, a system, or information

EIGHTH CIRCUIT PRIVACY LAW

- **Public Records**
 - Herald Co. v. McNeal, 553 F.2d 1125 (8th Cir. 1997) - noting that Missouri requires public records to be open for inspection and copying, and is applicable to parole records of the St. Louis Court of Criminal Corrections and to accident reports filed with the motor vehicle safety responsibility unit.
 - Foster v. General Motors Corp., 20 F.3d 838 (8th Cir. 1994) - finding that accident reports are public records and therefore admissible under the hearsay exception.
- **Public Transit**
 - United States v. Va Lerie, 424 F.3d 694 (8th Cir. 2005) - Law enforcement removed an untagged bag from the holding compartment of a Greyhound bus for further inspection. A majority of the en banc court held that no meaningful interference had occurred and also that the consent was not coerced. The court distinguished the seizure of the bag from the standard for searching the bag in the modern context of terrorist bombings and contraband transport.
- **Consumer Credit**
 - Davenport v. Farmers Ins. Group, 378 F.3d 839 (8th Cir. 2004) - Where state law is inconsistent with the Fair Credit Reporting Act (FCRA), 15 U.S.C.S. §§ 1681-1681x, with respect to the collection, distribution, or use of any information on consumers, the FCRA preempts state law, but only to the extent of the inconsistency. But in this case the state law did preempt because the allegation dealt with users of reports rather than creators of the reports.
- **Financial Records**
 - United States v. Riddick, 519 F.2d 645 (8th Cir. 1975) - Bank records obtained through lawful grand jury and trial subpoenas were not personal property of defendants and were not tantamount to private papers in which they had an expectation of privacy protected by the Constitution.
 - Metro N. State Bank v. Gaskin, 34 F.3d 589 (8th Cir. 1994) - There is no confidential or fiduciary relationship between a bank and a customer borrowing funds.
 - United States v. Gross, 416 F.2d 1205, 1213 (8th Cir. 1969) - Western Union customers have no privacy interest in Western Union records, as they are not the customers' property.
- **Electronic Surveillance**
 - United States v. Bentley, 706 F.2d 1498 (8th Cir. 1989) - permitting the use of a tracking device attached to a truck if there is probable cause and an issued warrant.
 - United States v. Mickelson, 433 F.3d 1050 (8th Cir. 2006) - affirming Mickelson's probation stipulation that he shall be tracked by GPS at the discretion of the probation office.
- **Computer Statutes**
 - United States v. Trotter, 478 F.3d 918 (8th Cir. 2007) - Defendant admitted that he had accessed the organization's computer network from his home, that he did not have authorization to do so, that he intentionally caused damage to the network, and that the network was connected to the Internet and used in interstate communications. Those admissions established that the organization's network met the statutory definition of a "protected computer" because the organization's computers were used in interstate communication. The organization's not-for-profit status was irrelevant for purposes of determining whether a violation of § 1030 had occurred.

NINTH CIRCUIT PRIVACY LAW

- **Public Records**
 - United States v. White, No. 94-10085, 1994 U.S. App. LEXIS 32928 (9th Cir. 1994) - Department of Motor Vehicles form showing defendant's driving record was admissible under the public records exception to the hearsay rule to prove that defendant's license was suspended or revoked.
 - United States v. Regner, 677 F.2d 754 (9th Cir. 1981) - accident reports could be considered business records or public records and are admissible under the hearsay exception.
- **Vehicles**
 - Company v. United States, 349 F.3d 1132 (9th Cir. 2003) - the FBI used GPS technology to intercept and listen to conversations between the two people in a moving BMW automobile. The court held the company to be an "other person," under § 2518(4) – that is, someone who provides "services" to the target and can be required to provide information, technical assistance, or facilities to law enforcement. Ultimately there was a defect in the court order, but this case arguably stands for the proposition that, if "bugging" through a wire or electronic service provider cannot be done without disrupting the service paid for by the subscriber, the "bugging" cannot be done at all. But this type of bugging seems certain to become more frequent as GPS technology advances.
 - Miller v. Reed, 176 F.3d 1202 (9th Cir. 1999) - Plaintiff driver sued the state Department of Motor Vehicles (DMV) to force it to issue him a renewal driver's license without the necessity of his revealing his Social Security number, as required by Cal. Veh. Code § 1653.5. The court concluded that by denying plaintiff a single mode of transportation, in a car driven by himself, the DMV did not unconstitutionally impede his right to interstate travel. It also concluded that plaintiff's free exercise of religion was not violated by the state's valid and neutral requirement that all driver's license applicants provide a Social Security number.
- **Consumer Credit**
 - Hansen v. Morgan, 582 F.2d 1214 (9th Cir. 1978) - provides there is a civil remedy available under the Fair Credit Reporting Act.
- **Financial Records**
 - United States v. Cormier, 220 F.3d 1103 (9th Cir. 2000) Citing Miller with approval. Recognizing that bank records are highly personal documents, the Supreme Court nevertheless found that "the depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government." The Court reaffirmed its view that a person does not have a privacy interest in information revealed to a third party and subsequently conveyed to governmental authorities, even if the information is revealed on the assumption that it will be used for a limited purpose and that the third party will not betray their confidence.
 - United States v. Mann, 829 F.2d 849 (9th Cir. 1987) - Congress, in response to Miller, enacted the Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3401-3422 (1982). The statutory rights granted by Congress, however, apply only to financial institutions within the United States. The rule of Miller, then, is in full force with respect to foreign banks where there is not expectation of privacy in financial records.
- **Electronic Surveillance**
 - United States v. Nerber, 222 F.3d 597 (9th Cir. 2000) - "Hidden video surveillance is one of the most intrusive investigative mechanisms available to law enforcement. The sweeping indiscriminate manner in which video surveillance can intrude upon us, regardless of where we are, dictates that its use be approved only in limited circumstances." Distinguished between silent videos and those that captured sound and visual images. Silent videos escape the scrutiny of 18 U.S.C. §§ 2510 through 2519 (wire, oral or electronic communications), but this court held that they are still regulated by the 4th Amendment and adopted four requirements, including: probable cause, normal investigative procedures have been tried and failed, and the surveillance can't last longer than 30 days.
 - United States v. Botero, 589 F.2d 430 (9th Cir. 1978) - permitted putting fluorescent powder and a tracking device in a package of cocaine. Customs officials are authorized to inspect incoming international shipments when they have a "reasonable cause to suspect" that the shipment contains

contraband. It was under this rule that the customs officers were permitted to put the tracking devices in the compartments carrying the contraband.

- United States v. Miroyan, 577 F.2d 489 (9th Cir. 1978) - permitted using a transponder to track an airplane suspected of carrying marijuana.
- **Computers**
 - United States v. Arnold, 454 F. Supp. 2d 999 (C.D. Cal. 2006) - In Arnold, government border agents at an airport, without reasonable suspicion, booted and inspected the contents of the defendant's computer and found what they believed to be child pornography. The trial court granted the defendant's motion to suppress this evidence, holding, "while it is appropriate to turn on or x-ray a laptop or other device to ensure that it functions and does not physically contain drugs or other dangerous substances, a search of the information contained therein requires a reasonable suspicion" the court found that some people might value the privacy of their computer files above physical privacy.
 - United States v. Heckenkamp, 482 F.3d 1142 (9th Cir. 2007) - Although the court held that defendant had an objectively reasonable expectation of privacy in his personal computer which was protected by a screensaver password, located in his dorm room, and subject to no policy allowing the university actively to monitor or audit his computer usage, the court agreed with the district court that the network administrator's limited warrantless remote search of defendant's computer was justified under the "special needs" exception to the Fourth Amendment warrant requirement. The special needs were that the administrator reasonably believed that the computer had been used to gain unauthorized access to confidential records and that the search was necessary to protect the security of the university's mail server.

TENTH CIRCUIT PRIVACY LAW

- **Public Records**
 - Lanphere & Urbaniak v. Colorado, 21 F.3d 1508, 1513 n.2 (10th Cir.), *cert. denied*, 130 L. Ed. 2d 544, 115 S. Ct. 638 (1994) - upheld the constitutionality of a Colorado statute denying access to criminal justice records where the records were "sought for the purpose of directly soliciting business for pecuniary gain."
- **Public Transportation**
 - United States v. Moore, 22 F.3d 241 (10th Cir. 1994) - the lesser expectation of privacy on a public train combined with the reasonable suspicion that the D was carrying contraband permitted DEA agents to briefly detain defendant's luggage and subject it to a dog sniff.
- **Personal Privacy**
 - Banks v. United States 490 F.3d 1178 (10th Cir. 2007) - Applying totality-of-the-circumstances test, the court held that the DNA Analysis Backlog Elimination Act of 2000, as amended by USA PATRIOT Act of 2001, as amended by Justice For All Act of 2004, was constitutional because government's interest in extracting DNA outweighed nonviolent offenders' interests in avoiding intrusions upon their privacy.
- **Consumer Credit**
 - Owner-Operator Indep. Drivers Ass'n v. USIS Commer. Serv., 537 F.3d 1184 (10th Cir. 2008) - district court did not err in concluding that employment history reports were not consumer reports pursuant to 15 U.S.C.S. § 1681a(d)(2)(A)(I) for purposes of the Fair Credit Reporting Act, 15 U.S.C.S. §§ 1681-1681x, because, while truck drivers may have interacted with third parties, their experiences were still first-hand for their employers.
 - Heath v. Credit Bureau of Sheridan, Inc., 618 F.2d 693 (10th Cir. 1980) - Critical component in determining violations of the Fair Credit Reporting Act regarding consumer reports is the determination of what the reporting credit bureau knew and expected concerning the use of information supplied.
- **Financial Records**
 - Anderson v. La Junta State Bank, 115 F.3d 756 (10th Cir. 1997) - An oral disclosure of customer banking information by a bank officer, following an oral request by a government investigator, without permitting visual inspection of the customer's records, violated the Right to Financial Privacy Act.
 - Taylor v. United States Air Force, No. 98-1405, 1999 U.S. App. LEXIS 8505 (10th Cir. 1999) - The financial privacy law under which plaintiffs sued did not apply to the release of records in response to a subpoena, thus barring plaintiffs' claim against defendants.
 - United States v. Jackson, 11 F.3d 953 (10th Cir. 1993) - The Right to Financial Privacy Act did not prohibit the government from using subpoenaed bank records to obtain a search warrant before returning those records to the grand jury.
 - National Commodity & Barter Assn. v. United States, 951 F.2d 1172 (10th Cir. 1991) - Subpoenas for commodity associations' bank accounts did not violate members' First Amendment rights where the government showed a compelling interest in the records which bore a substantial relationship to the investigation.
- **Electronic Surveillance**
 - United States v. Alonso, 790 F.2d 1489 (10th Cir. 1986) - Monitoring signals from an electronic tracking device that tells officers no more than that a specific aircraft is flying in the public airspace does not violate any reasonable expectation of privacy. Because this is so, no U.S. Const. Amend. IV violation results from such public detection. The movement of an airplane in the sky, like that of an automobile on a highway, is not something in which a person can claim a reasonable expectation of privacy.
- **Computer Statutes**
 - United States v. Willis, 476 F.3d 1121 (10th Cir. 2007) - Evidence that defendant gave another person a user name and password so she could use a financial information services website was sufficient to sustain his conviction for violating 18 U.S.C.S. §§ 2 and 1030, even though he did not know recipient would use the site to commit identify theft and did not know the value of information that was taken.

ELEVENTH CIRCUIT PRIVACY LAW

- **Public Records**
 - Speer v. Miller, 15 F.3d 1007 (11th Cir. 1994) - holding unconstitutional a Georgia statute that prohibited inspection or copying of law enforcement records for commercial solicitation.
 - United States v. Rodriguez, 524 F.2d 485 (11th Cir. 1975) - Vehicle registration is a matter of public record.
 - Statewide Detective Agency v. Miller, 115 F.3d 904 (11th Cir. 1997) - A preliminary injunction against state officials was proper because a state law criminalizing requests for public records for commercial solicitation purposes implicated constitutional free speech rights. The court held that Ga. Code. §§ 33-24-53(c) and (e), by criminalizing requests for public records for commercial solicitation purposes, implicated First Amendment concerns.
- **Consumer Credit**
 - Enwonwu v. Trans. Union, LLC, No. 05-13695, 2006 U.S. App. LEXIS 2301 (11th Cir. 2006) - In an FCRA case, the district court's grant of summary judgment in favor of a credit reporting agency was affirmed because the evidence did not support an inference that the inaccurate information included in the report was the cause of the debtor's inability to obtain satisfactory financing in the three transactions.
- **Financial Records**
 - Lopez v. First Union Nat'l Bank, 129 F.3d 1186 (11th Cir. 1998) - Federal law protected defendants from suits related to account information release pursuant to warrant, but did not protect its release on verbal authority, or without good faith nexus connecting it to suspicious activity.
 - Coronado v. BankAtlantic Bancorp, Inc., 222 F.3d 1315 (11th Cir. 2000) - Defendant bank was immune from liability under safe harbor provision in Annunzio-Wylie Act for disclosure of plaintiff customer's account records pursuant to facially valid grand jury subpoenas.
- **Electronic Surveillance**
 - United States v. Yonn, 702 F.2d 1341, 1346-47 & n. 5 (11th Cir. 1983) - the Fourth Amendment is not violated by the use of a fixed electronic device (i.e., not wearing a wire) to record a meeting between a defendant and a person who consents to the recording. Agents placed a microphone in a motel room and monitored and recorded the defendant's conversations when a person who consented to the surveillance was present. The Court held that "the location of the electronic equipment does not alter the irrefutable fact that Yonn had no justifiable expectation of privacy in his conversation with [the person who consented]."
 - The Court also specifically rejected the reasoning of *United States v. Padilla* (a First Circuit case), stating that it saw "no reason to suppress the recording of a clearly unprotected conversation merely because the monitoring technique employed poses a hypothetical risk that protected conversations may be intercepted."
- **Computer Statutes**
 - United States v. Steiger, 318 F.3d 1039 (11th Cir. 2003) - An anonymous source's hacking into defendant's computer to gain evidence of child pornography implicated neither the Fourth Amendment nor a federal statute prohibiting wiretapping and thus the evidence need not be suppressed.

D.C. CIRCUIT PRIVACY LAW

- **Public Records**
 - United States v. Coleman, 631 F.2d 908 (D.C. Cir. 1980) - Questioning whether accident reports are public records. In Palmer, the Supreme Court affirmed a ruling by the Second Circuit that an accident report prepared by a since-deceased railroad engineer and offered by the railroad in its defense in a grade-crossing collision case did not qualify as a business record since the report was "dripping with motivations to misrepresent." The doctrine has since been applied to deny the business records exception to any document prepared with an eye toward litigation when offered by the party responsible for making the record.
- **Public Transportation**
 - Hedgepeth v. Wash. Metro. Area Transit Auth., 386 F.3d 1148 (D.C. Cir. 2004) - DC enacted a strict no-eating policy in their subway stations. Adults were cited, and children arrested until their parents could come pick them up. The court, applying rational basis, found that there was a legitimate purpose of making sure parents knew what their kids were doing when they were arrested. The law prohibiting eating on subways was constitutional, too.
- **Consumer Credit**
 - Trans Union, LLC v. FTC, 295 F.3d 42 (D.C. Cir. 2002) FTC rule protecting privacy of consumer information was upheld against credit-reporting agency's ultra vires and First Amendment claims, since definition of terms, personally identifiable financial information and financial institution, was reasonable and commercial speech did not involve public concerns. In commercial speech cases, courts ask whether the asserted governmental interest is substantial. The governmental interest in protecting the privacy of consumer credit information is substantial. Laws restricting commercial speech must be tailored in a reasonable manner to serve a substantial state interest in order to survive First Amendment scrutiny.
 - Koropoulos v. Credit Bureau, Inc., 734 F.2d 37 (D.C. Cir. 1994) - Entry of summary judgment was not improper where question of fact existed as to whether defendant credit bureau took reasonable procedures to assure maximum accuracy of plaintiff debtor's technically accurate but potentially misleading credit report.
- **Financial Records**
 - Richardson v. District of Columbia Bar Ass'n, No. 97-7051, 1997 U.S. App. LEXIS 19078 (D.C. Cir. 1997) - An association's actions did not violate a party's privacy rights because the party had no constitutionally protected liberty or property interest in the check or bank records that were subpoenaed by the association.
- **Electronic Surveillance**
 - United States v. Gbemisola, 225 F.3d 753 (D.C. Cir. 2000) - A warrant is required to monitor the location of a tracking device in a private home because of the legitimate expectation of privacy within a home. However, no warrant is required for monitoring the device during the time it is en route to a house on a public road. The warrantless monitoring of an electronic tracking device does not violate the U.S. Const. amend. IV when it reveals no information that could not have been obtained through visual surveillance.
- **Computer Statutes**
 - Recording Indus. Ass'n of Am., Inc. v. Verizon Internet Servs., 351 F.3d 1229 (D.C. Cir. 2004) - An Internet service provider that was only a conduit through which its customers downloaded copyrighted music was held not to be subject to the music producers' subpoenas seeking the identity of the infringing users under the Digital Millennium Act.

FEDERAL CIRCUIT PRIVACY LAW

- **Public Records**
 - nothing in the transportation or personal privacy realm.
- **Consumer Credit**
 - nothing in the transportation or personal privacy realm.
- **Financial Records**
 - nothing in the transportation or personal privacy realm.
- **Electronic Surveillance**
 - In re: Directives, No. 08-01, 2008 U.S. App. LEXIS 27439 (Fed. Cir. 2008) - The directive required the provider to assist in warrantless surveillance of its customers whom the government reasonably believed to be outside the United States. The provider contended that collecting foreign intelligence was not excepted from the constitutional requirement for a warrant and, even if an exception existed, the surveillance mandated by the directive was an unreasonable invasion of its customers' privacy. The appellate court first held that the substantial interest in national security justified a foreign-intelligence exception to the warrant requirement when surveillance is conducted to obtain foreign intelligence and is directed against agents of foreign powers reasonably believed to be located outside the United States.
 - Further, the directive was reasonable since the procedures to secure the directive required a showing of particularity, a meaningful probable cause determination, a showing of necessity, and a reasonable durational limit. Also, the risks of error and abuse were within acceptable limits, effective procedures were in place to minimize incidental intrusions, and the vital interest in national security outweighed the customers' privacy interests. Note that the act was later repealed.
- **Computer Statutes**
 - Nothing of significance on identity theft, 18 U.S.C. § 1030 or personal privacy.

FEDERAL PRIVACY LAW

- **Constitutional Privacy Rights**
 - **Express**
 - none
 - **Implied**
 - U.S. CONST. amend. III. No Soldier shall, in time of peace be quartered in any house, without the consent of the Owner, nor in time of war, but in a manner to be prescribed by law.
 - U.S. CONST. amend. IV. The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.
 - U.S. CONST. amend. V. No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offence to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.
- **Search and Seizure**
 - U.S. CONST. amend. IV. Unreasonable searches and seizures. The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.
 - California v. Greenwood, 486 U.S. 35 (1988) - no reasonable expectation of privacy in opaque garbage bags placed on the curb for trash pickup.
 - Kyllo v. United States, 533 U.S. 27 (2001) - (1) use of sense-enhancing technology to gather any information regarding interior of home that could not otherwise have been obtained without physical intrusion into constitutionally protected area constitutes a “search,” and (2) use of thermal imaging to measure heat emanating from home was search.
 - United States v. Knotts, 460 U.S. 276 (1983) - held that monitoring the signal of a beeper placed in a container of chemicals that was being transported to the owner's cabin in a car did not invade any legitimate expectation of privacy on the cabin owner's part and, therefore, there was neither a “search” nor a “seizure” within the contemplation of the Fourth Amendment.
 - **Auto Exception**
 - California v. Acevedo, 500 U.S. 565 (1991) - police may search containers located in a vehicle passenger compartment if there is probable cause that the containers contain contraband or evidence.
 - Public Utilities Comm'n v. Pollak, 343 U.S. 451 (1952) - "However complete his right of privacy may be at home, it is substantially limited by the rights of others when its possessor travels on a public thoroughfare or rides in a public conveyance."
 - United States v. Ross, 456 U.S. 798 (1982) - police officers who had legitimately stopped automobile and who had probable cause to believe that contraband was concealed somewhere within it could conduct warrantless search of the vehicle as thorough as a magistrate could authorize by warrant, since scope of warrantless search of automobile is not defined by nature of container in which the contraband is secreted, but rather, it is defined by the object of the search and places in which there is probable cause to believe that it may be found.
 - Carroll v. United States, 267 U.S. 132 (1925) - stating the original reasons for allowing warrantless searches of automobiles. Carroll doctrine simply recognizes the obvious—that a moving automobile on the open road presents a situation ‘where it is not practicable to secure a warrant, because the vehicle can be quickly moved out of the locality or jurisdiction in which the warrant must be sought.’
 - **Open Fields**

- California v. Ciraolo, 476 U.S. 207 (1986) - Police officers' warrantless aerial observation, from altitude of 1,000 feet, of fenced-in backyard within curtilage of home, during which plants readily discernible to naked eye as marijuana were observed, did not violate homeowner's Fourth Amendment rights where homeowner's expectation that his backyard was protected from such observation was unreasonable and was not one that society was prepared to honor.
- Dow Chemical Co. v. United States, 476 U.S. 227 (1986) - EPA had statutory authority to use aerial photography to perform "site inspection" under Clean Air Act, and aerial photography of chemical company's industrial complex was not a "search" for Fourth Amendment purposes. Environmental Protection Agency's aerial photography of chemical company's 2,000-acre outdoor industrial complex, while EPA was lawfully within navigable air space, was not "search" for Fourth Amendment purposes; open areas of complex were more comparable to open field than to "curtilage" of dwelling for purposes of aerial surveillance.
- Illinois v. Caballes, 543 U.S. 405 (2005) - where lawful traffic stop was not extended beyond time necessary to issue warning ticket and to conduct ordinary inquiries incident to such a stop, another officer's arrival at scene while stop was in progress and use of narcotics-detection dog to sniff around exterior of motorist's vehicle did not rise to level of cognizable infringement on motorist's Fourth Amendment rights, such as would have to be supported by some reasonable, articulable suspicion.
- **Plain View**
 - Minnesota v. Dickerson, 508 U.S. 366 (1993) - Under "plain-view" doctrine, if police are lawfully in a position from which they view an object, if its incriminating character is immediately apparent, and if the officers have lawful right of access to the object, they may seize it without a warrant, but if the police lack probable cause to believe that an object in plain view is contraband without conducting some further search of the object, i.e., if its incriminating character is not immediately apparent, the "plain-view" doctrine cannot justify its seizure. (Note that this includes apperency from the sense of touch.)
- **Public Records**
 - 5 U.S.C. § 552 (2009) - Freedom of Information Act. Each agency is responsible for making records accessible to the public and for publishing the procedure for public inspection and copying.
 - Exceptions include records compiled for law enforcement purposes, trade secrets and commercial or financial information obtained from a person that is privileged or confidential, personnel and medical files and similar files, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy.
 - 5 U.S.C. § 552a (2009) - No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, unless disclosure of the record would be for law enforcement purposes, for the census, to the Comptroller General, to a consumer reporting agency, etc.
 - 5 U.S.C. § 9101 (2009). Access to criminal history records for national security and other purposes is allowed.
- **Statutory Privacy Protections**
 - 6 U.S.C. § 142 (2009) Information Analysis And Infrastructure Protection Information Security - The Secretary shall appoint a senior official in the Department, who shall report directly to the Secretary, to assume primary responsibility for privacy policy, including -- (1) assuring that the use of technologies sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of personal information; (2) assuring that personal information contained in Privacy Act systems of records is handled in full compliance with fair information practices as set out in the Privacy Act of 1974 [5 U.S.C. § 552a]; (3) evaluating legislative and regulatory proposals involving collection, use, and disclosure of personal information by the Federal Government; (4) conducting a privacy impact assessment of proposed rules of the Department or that of the Department on the privacy of personal information, including the type of personal information collected and the number of people affected; (5) coordinating with the Officer for Civil Rights and

Civil Liberties to ensure that the programs and policies implicating civil rights and liberties are addressed in a comprehensive manner.

- 49 U.S.C. § 114 (2009) - Transportation Security Administration. Nondisclosure of security activities. The Under Secretary shall prescribe regulations prohibiting the disclosure of information obtained or developed in carrying out security under authority of the Aviation and Transportation Security Act (Public Law 107-71) or 49 U.S.C. §§ 44901 et seq. if the Under Secretary decides that disclosing the information would- (A) be an unwarranted invasion of personal privacy; (B) reveal a trade secret or privileged or confidential commercial or financial information; or (C) be detrimental to the security of transportation.
- 18 U.S.C. § 1028(d)(7) (2009) Identity theft is a crime. The “means of identification” means any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including any-- (A) name, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number; (B) unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation; (C) unique electronic identification number, address, or routing code; or (D) telecommunication identifying information or access device.
- **Public Transportation**
 - 6 U.S.C. § 1138 (2009) - Public transportation research and development. The Secretary shall carry out a research and development program through the Homeland Security Advanced Research Projects Agency in the Science and Technology Directorate and in consultation with the Transportation Security Administration and with the Federal Transit Administration, for the purpose of improving the security of public transportation systems. The Secretary shall award grants or contracts to public or private entities to conduct research and demonstrate technologies and methods to reduce and deter terrorist threats or mitigate damages resulting from terrorist attacks against public transportation systems. Note that Secretary shall consult with the Chief Privacy Officer of the Department and the Officer for Civil Rights and Civil Liberties of the Department regarding the legality of these programs.
 - 46 U.S.C.S. §§ 70101-70119 (2009) The Maritime Transportation Security Act of 2002 (MTSA) requires the owners and operators of specified maritime vessels to implement a Coast-Guard approved security plan. Alternative Security Programs (ASP) are approved at a national level by the Coast Guard Commandant if he or she finds that they provide a level of security equivalent to that established by the agency's regulations. 33 C.F.R. §§ 101-105.
 - 49 U.S.C. § 114 (2009) - Transportation Security Administration - The Secretary of Homeland Security shall develop, prepare, implement, and update, as needed--(A) a National Strategy for Transportation Security; and (B) transportation modal security plans addressing security risks, including threats, vulnerabilities, and consequences, for aviation, railroad, ferry, highway, maritime, pipeline, public transportation, over-the-road bus, and other transportation infrastructure assets. (2) Role of Secretary of Transportation. The Secretary of Homeland Security shall work jointly with the Secretary of Transportation in developing, revising, and updating the documents required by paragraph (1). (3) Contents of National Strategy for Transportation Security. The National Strategy for Transportation Security shall include the following: (A) An identification and evaluation of the transportation assets in the United States that, in the interests of national security and commerce, must be protected from attack or disruption by terrorist or other hostile forces, including modal security plans for aviation, bridge and tunnel, commuter rail and ferry, highway, maritime, pipeline, rail, mass transit, over-the-road bus, and other public transportation infrastructure assets that could be at risk of such an attack or disruption.
 - 49 U.S.C. § 5331 (2009) Alcohol and controlled substances testing for public transportation employees. Includes guidelines for discretionary and mandatory tests.
- **Motor Vehicles**
 - 18 U.S.C. § 2721 (2009) - Driver's Privacy Protection Act of 1994 (DPPA). Prohibition on release and use of certain personal information from State motor vehicle records. A State department of motor vehicles, and any officer, employee, or contractor thereof, shall not knowingly disclose or otherwise make available to any person or entity personal information (defined as information that identifies an individual, including an individual's photograph, social security number, driver

identification number, name, address (but not the 5-digit zip code), telephone number, and medical or disability information, but does not include information on vehicular accidents, driving violations, and driver's status) OR or highly restricted personal information (defined as an individual's photograph or image, social security number, medical or disability information) without the express consent of the person to which the information applies or for some exceptions including for use in connection with matters of motor vehicle or driver safety and theft, motor vehicle emissions, motor vehicle product alterations, recalls, or advisories, performance monitoring of motor vehicles and dealers by motor vehicle manufacturers, and removal of non-owner records from the original owner records of motor vehicle manufacturers, law enforcement purposes, etc.

- 19 U.S.C. § 1581 (2009) - Any officer of the customs may at any time go on board of any vessel or vehicle at any place in the United States or within the customs waters or, as he may be authorized, within a customs-enforcement area established under the Anti-Smuggling Act, or at any other authorized place without as well as within his district, and examine the manifest and other documents and papers and examine, inspect, and search the vessel or vehicle and every part thereof and any person, trunk, package, or cargo on board, and to this end may hail and stop such vessel or vehicle, and use all necessary force to compel compliance.
- National Highway Traffic Safety Administration, Paper No. 05-0271, Evaluation of Event Data Recorders in Full Systems Car Crashes (2005), *available at* www-nrd.nhtsa.dot.gov/pdf/nrd-01/esv/esv19/other/Print%2009.pdf (listing automobiles tested). There is no Fourth Amendment limitation on the obtaining and use of EDR (event data recorders in automobiles) data by private parties, and although an EDR is owned by the automobile owner and its data is not otherwise subject to discovery, many insurers and automobile manufacturers, sellers, and lessors can place clauses requiring disclosure of EDR data as boilerplate in their agreements. Rental agencies may even be able to fine customers for speeding recorded by an EDR, if the agencies give adequate notice.
 - It is unsettled whether there are Fourth Amendment limitations on police use of EDR (event data recorders) in automobiles. However, the U.S. Department of Justice analyzed the potential applicability of several exceptions to the Fourth Amendment warrant requirement for searches of computers, and could be analogous.
- **Consumer Credit**
 - 15 U.S.C. §§ 1681 through 1681v (2009) - Accuracy and fairness in credit reporting. There is a need to ensure that consumer reporting agencies exercise their grave responsibilities with fairness, impartiality, and a respect for the consumer's right to privacy.
 - § 1681b. Permissible purposes of consumer reports - in response to a court order, in accordance to the written instructions of a consumer, to a person who intends to use the report in connection with extending credit, or for employment purposes, etc.
 - § 1681c. Requirements relating to information contained in consumer reports. Reports shall not report any bankruptcy older than 10 years, any tax lien or criminal records older than 7 years, the name, address, and telephone number of any medical information furnisher that has notified the agency of its status with some exceptions, etc.
 - § 1681c-1. Identity theft prevention; fraud alerts and active duty alerts. A consumer may put a fraud alert on their account if such fraud is suspected.
 - § 1681c-2. Block of information resulting from identity theft. Any information the consumer asserts is from identity theft will be put on block by the reporting agency.
 - § 1681d. Disclosure of investigative consumer reports. Investigative reports not allowed unless the consumer is notified and some other requirements are met. Also, a consumer reporting agency shall not furnish an investigative consumer report that includes information that is a matter of public record and that relates to an arrest, indictment, conviction, civil judicial action, tax lien, or outstanding judgment, unless the agency has verified the accuracy of the information during the 30-day period ending on the date on which the report is furnished.
 - § 1681f. Disclosures to governmental agencies. With some exceptions, a consumer reporting agency may furnish identifying information respecting any consumer, limited to

his name, address, former addresses, places of employment, or former places of employment, to a governmental agency.

- § 1681g. Disclosures to consumers. Certain prohibitions of consumer social security information and credit scores unless permitted by the consumer. Also lists affirmative provisions that the reporting agency must provide the consumer, like a list of those inquiring about the consumer.
 - § 1681k. Public record information for employment purposes is allowed.
 - § 1681l. Restrictions on investigative consumer reports. Whenever a consumer reporting agency prepares an investigative consumer report, no adverse information in the consumer report (other than information which is a matter of public record) may be included in a subsequent consumer report unless such adverse information has been verified in the process of making such subsequent consumer report, or the adverse information was received within the three-month period preceding the date the subsequent report is furnished.
 - § 1681m. Requirements on users of consumer reports. if any entity takes adverse action against a consumer as a result of an inquiry into their credit report, the entity will inform the consumer of that fact.
 - § 1681r. Unauthorized disclosures by officers or employees. Any officer or employee of a consumer reporting agency who knowingly and willfully provides information concerning an individual from the agency's files to a person not authorized to receive that information shall be fined under title 18, United States Code, imprisoned for not more than 2 years, or both.
 - § 1681s-1. Information on overdue child support obligations. consumer reporting agency shall include in any consumer report furnished by the agency in accordance with 15 USCS § 1681b, any information on the failure of the consumer to pay overdue support which-- (1) is provided--(A) to the consumer reporting agency by a State or local child support enforcement agency; or (B) to the consumer reporting agency and verified by any local, State, or Federal Government agency; and (2) antedates the report by 7 years or less.
 - § 1681u. Disclosures to FBI for counterintelligence purposes. Barring some exceptions, a consumer reporting agency shall furnish identifying information respecting a consumer, limited to name, address, former addresses, places of employment, or former places of employment, to the Federal Bureau of Investigation when presented with a written request, signed by the Director or the Director's designee in a position not lower than Deputy Assistant Director at Bureau headquarters
 - § 1681v. Disclosures to governmental agencies for counterterrorism purposes. A consumer reporting agency shall furnish a consumer report of a consumer and all other information in a consumer's file to a government agency authorized to conduct investigations of, or intelligence or counterintelligence activities or analysis related to, international terrorism when presented with a written certification by such government agency that such information is necessary for the agency's conduct or such investigation, activity or analysis. If provided for counterterrorism purposes, the reporting agency need not inform the consumer, and in some cases must not.
- 15 U.S.C. § 1681b(g) (2009)- prohibits consumer reporting agencies (CRAs) from furnishing medical information in connection with a credit transaction but for certain exceptions. Section (g)(2) prohibits creditors from obtaining or using medical information in connection with credit eligibility decisions. There are no exceptions for this provision.
 - 15 U.S.C. § 1681s-3 (2009) - an entity that receives consumer reports or experience information from an affiliate may not use that information to make a solicitation for marketing purposes about its products or services, unless: (i) it clearly and conspicuously disclosed that the information received from the affiliate may be used for marketing purposes; and (ii) the consumer is provided an opportunity and a simple method to prohibit (i.e., opt-out) of the marketing solicitation.
 - BUT there are several important exceptions, so that the section does not apply if: (i) the entity has a pre-existing business relationship with the consumer; (ii) the information is used to perform services on behalf of an affiliate, unless the affiliate could not send the solicitation itself because the consumer opted out; (iii) the information is used to respond

to a communication initiated by the consumer; and (iv) the information is used in response to solicitations authorized and requested by the consumer.

- **Financial Records**

- 12 U.S.C. § 3402 (2009) Access to financial records by Government authorities prohibited; exceptions. Except as provided, no Government authority may have access to or obtain copies of, the information contained in the financial records of any customer from a financial institution unless the financial records are reasonably described and-- (1) such customer has authorized such disclosure in accordance with 12 USC § 3404; (2) such financial records are disclosed in response to an administrative subpoena or summons which meets the requirements of 12 USCS § 3405; (3) such financial records are disclosed in response to a search warrant which meets the requirements of 12 USCS § 3406; (4) such financial records are disclosed in response to a judicial subpoena which meets the requirements of 12 USCS § 3407; (5) such financial records are disclosed in response to a formal written request which meets the requirements of 12 USCS § 3408.
- 12 U.S.C. § 3414 (2009) - Access to financial records for certain intelligence and protective purposes. A Government authority authorized to conduct foreign counter- or foreign positive-intelligence activities for purposes of conducting such activities; or the Secret Service for the purpose of conducting its protective functions or a Government authority authorized to conduct investigations of, or intelligence or counterintelligence analyses related to, international terrorism for the purpose of conducting such investigations or analyses may request and receive financial records without informing the person who owns the records.
- 15 U.S.C. § 6821 (2009) Fraudulent Access to Financial Information. Privacy protection for customer information of financial institutions. Prohibition against soliciting information about a customer under false pretenses or for using such information for an improper purpose.
 - Exceptions include obtaining such information for child support purposes, if the information is a public record, insurance fraud investigation, some purposes of the financial institution itself, etc.
- 15 U.S.C. §§ 6801 through § 6809 (2009). Commerce and Trade Privacy
 - § 6801. Protection of nonpublic personal information. It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information. In furtherance of this policy, each agency or authority described in section 15 USCS § 6805(a) shall establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards-- (1) to ensure the security and confidentiality of customer records and information; (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.
 - § 6802. Obligations with respect to disclosures of personal information.. Except as otherwise provided in this subtitle, a financial institution may not, directly or through any affiliate, disclose to a nonaffiliated third party any nonpublic personal information, unless such financial institution provides or has provided to the consumer a notice.
 - But it is acceptable for a financial institution to share personal information with a third party for marketing purposes related to the financial institution.
 - However, if this legal disclosure is allowed then the third party may not sell or reuse the personal information for their own purposes
 - A financial institution shall not disclose, other than to a consumer reporting agency, an account number or similar form of access number or access code for a credit card account, deposit account, or transaction account of a consumer to any nonaffiliated third party for use in telemarketing, direct mail marketing, or other marketing through electronic mail to the consumer.
 - § 6803. Disclosure of institution privacy policy. The financial institution must disclose in writing the privacy policy of the institution including the disclosure of non-public information.

- **Biometrics, Licensing and Other Technological Record Keeping**

- Federal Programs using biometrics include: Integrated Automated Fingerprint Identification System ("IAFIS"); Diversity Visa program (offers visas on lottery system to people from countries with low rates of immigration to the United States, and uses facial recognition technology to exclude persons who try to enter the lottery repeatedly); Biometric Visa system; Border Crossing Card (used at Mexican border); Passport Records Imaging System (new database covering seventy million Americans); Electronic passport (will contain biometric data including digital images); US-VISIT (intended to track entry and exit of foreigners, using fingerprints and digital images taken at airports and seaports); Border Patrol fingerprint system (links border posts to FBI database of forty-seven million fingerprint records); Transportation Worker ID Card (biometric entry control card for up to twelve million workers from transportation and port industries, initially using fingerprints and digital photos); Registered Traveler program (fingerprint or eye scans used to confirm person's identity to speed that person through airport security checkpoints). *See* STEVE POSNER, 1-2 PRIVACY LAW AND THE USA PATRIOT ACT § 2.37 (2007).
 - Note that not all of these specific programs have been codified in the USC, but were initiated by agency action. For example, 42 U.S.C. § 14616 gave the FBI and individual states license to organize an electronic information sharing system among the Federal Government and the States to exchange criminal history records for noncriminal justice purposes authorized by Federal or State law, such as background checks for governmental licensing and employment. Accordingly, IAFIS was created by the FBI.
- 8 U.S.C. § 1732 (2009) Biometric Identifiers and the Border. The Attorney General and the Secretary of State shall jointly establish document authentication standards and biometric identifiers standards to be employed on such visas and other travel and entry documents from among those biometric identifiers recognized by domestic and international standards organizations. Not later than October 26, 2005, the Attorney General, in consultation with the Secretary of State, shall install at all ports of entry of the United States equipment and software to allow biometric comparison and authentication of all United States visas and other travel and entry documents issued to aliens, and passports
- 8 U.S.C. §§ 1365a & 1365b (2009) - Biometric Entry and Exit Integrated System for U.S. borders. Includes land and sea entry ports and creates an electronic system that provides access to, and integrates, alien arrival and departure data. Helps identify, through on-line searching procedures, lawfully admitted non-immigrants who may have remained in the United States beyond the period authorized by the Attorney General. The entry and exit data system shall include a requirement for the collection of biometric exit data for all categories of individuals who are required to provide biometric entry data, regardless of the port of entry where such categories of individuals entered the United States. There was a requirement that all of these new provisions be implemented by December 31, 2003.
- 8 U.S.C. § 1379 (2009) The USA PATRIOT ACT added this section. Technology Standard to Confirm Identity. The Attorney General and the Secretary of State jointly, through the National Institute of Standards and Technology (NIST), and in consultation with the Secretary of the Treasury and other Federal law enforcement and intelligence agencies the Attorney General or Secretary of State deems appropriate and in consultation with Congress, shall within 15 months after the date of the enactment of this section [enacted Oct. 26, 2001], develop and certify a technology standard, including appropriate biometric identifier standards, that can be used to verify the identity of persons applying for a United States visa or such persons seeking to enter the United States pursuant to a visa for the purposes of conducting background checks, confirming identity, and ensuring that a person has not received a visa under a different name or such person seeking to enter the United States pursuant to a visa.
- 46 U.S.C. § 70105 (2009) Port Security. To enhance port security only those individuals with an issued biometric transportation security card can access vessels or other secured areas.
- 42 USCS § 14135a (2009) Collection and use of DNA identification information from certain Federal offenders. Does not require the felon be violent or sexual offender.
- Real ID Act of 2005, Pub. L. 109-13, 119 Stat. 302 - postponed until May 2011, but if implemented will require states to meet stricter guidelines for issuing driver's licenses, including requiring a litany of documents from the applicant.

- Limitation on the Issuance of Hazmat Licenses, USA PATRIOT Act, Pub. Law 107-56, 115 Stat. 272, § 1012 (codified 49 U.S.C. 5103a). State may not issue to any individual a license to operate a motor vehicle transporting in commerce a hazardous material unless the Secretary of Homeland Security has first determined, upon receipt of a notification [from the US Attorney General], that the individual does not pose a security risk warranting denial of the license.
- Transportation Worker Identification Credential (TWIC) Implementation in the Maritime Sector; Hazardous Materials Endorsement for a Commercial Driver's License, 71 Fed. Reg. 29396, 29400–15 (2006) - TSA established the TWIC program in response to identity management shortcomings and vulnerabilities identified in the transportation system. In some segments of the transportation system, it is not possible to positively identify individuals entering secure areas or assess the threat they may pose due to a lack of pertinent background information. Also, existing identity credentials are often vulnerable to fraud. To mitigate these weaknesses, TSA determined that an integrated, credential-based, identity management system for all transportation workers who need unescorted access to secure areas of the nation's transportation system would be necessary.
- **Electronic Surveillance**
 - 18 U.S.C. § 1801(2009) - Whoever, in the special maritime and territorial jurisdiction of the United States, has the intent to capture an image of a private area of an individual without their consent, and knowingly does so under circumstances in which the individual has a reasonable expectation of privacy, shall be fined under this title or imprisoned not more than one year, or both. This section does not prohibit any lawful law enforcement, correctional, or intelligence activity.
 - 18 U.S.C. § 2510 (2009) Definitions. "electronic communication" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photo-optical system that affects interstate or foreign commerce, but does not include-- (A) any wire or oral communication; (B) any communication made through a tone-only paging device; (C) any communication from a tracking device (as defined in section 3117 of this title [18 USCS § 3117]); or (D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds;
 - 18 U.S.C. § 2511 (2009) Interception and disclosure of wire, oral, or electronic communications prohibited. Intentionally intercepts/uses/discloses, endeavors to intercepts/uses/discloses, or procures any other person to intercepts/uses/discloses or endeavor to intercepts/uses/discloses, any wire, oral, or electronic communication. Exceptions if intercepted under federal law, or if a public frequency, or by a law enforcement officer, FCC employee or employee of a common carrier acting in the normal course of business.
 - 18 U.S.C. § 2512 (2009) Manufacture, distribution, possession, and advertising of wire, oral, or electronic communication intercepting devices prohibited.
 - 18 U.S.C. § 2515 (2009) Prohibition of use as evidence of intercepted wire or oral communications. No evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision if in violation of this chapter.
 - 18 U.S.C. § 2516 (2009) Authorization for interception of wire, oral, or electronic communications. The Attorney General, Deputy Attorney General, Associate Attorney General, or any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General or acting Deputy Assistant Attorney General in the Criminal Division or National Security Division specially designated by the Attorney General or any attorney for the government, may authorize an application for interception to a federal judge.
 - The offenses investigated can include those that are punishable by death or imprisonment for more than one year. This section explicitly lists the offenses including kidnapping, sabotage of a nuclear facility, assassination attempts, counterfeiting, etc.
 - Also allows surveillance for crimes associated with 18 U.S.C. § 2332f (2009), which was added by the USA PATRIOT Act and makes it a crime to conspire to bomb a public transportation facility.

- 18 U.S.C. § 2517 (2009) Authorization for disclosure and use of intercepted wire, oral, or electronic communications. If obtained properly, one law enforcement officer may disclose to another or another law enforcement agency if appropriate to the proper performance of the official duties of law enforcement.
 - The PATRIOT Act loosened who this information could be disclosed to and updated this section. Now disclosure can include federal law enforcement, and any intelligence, protective, immigration, national defense, or national security official to the extent that such contents include foreign intelligence. In situations where the information is extremely threatening, the information can be disclosed to any federal, state, local or foreign government official.
- 18 U.S.C. § 2518 (2009) Procedure for interception of wire, oral, or electronic communications. Must disclose the officer making the application and the police officer who set the application in motion, statement of facts, explanation of why the interception is necessary and why other attempts at investigation have failed, the period of time of the interception requested, proof of probable cause that the intercepted person is committing or committed the offense and other details.
 - The judge's order may not exceed 30 days of interception and shall be conducted to minimize intrusion.
 - The contents of the interception will be put under seal and within ninety days after the termination of the order, the judge will notify the person who was intercepted, the order and the fact of interception.
 - There is an exclusionary rule for wire or oral communication, but does not include electronic communications.
 - This section also permits roving wiretaps if the application contains a full and complete statement as to why such specification of a surveillance site is not practical.
- 18 U.S.C. § 2519 (2009) Reports concerning intercepted wire, oral, or electronic communications. Within thirty days of the expiration or denial of an order the judge must report to the Administrative office of the US to inform regarding the order. In January each year the Attorney General must inform the office of a compilation of orders and the success of the interceptions. In April each year the director of the administrative office will so inform Congress.
- 18 U.S.C. §§ 3121 through 3127 (2009) Pen register and trap and trace device use. Generally prohibited without a court order. Even with a court order, cannot use a pen register to record conversations. The requirements for getting a court order include: the requesting person needs to be an attorney for the government and there needs to be certification that the information is likely to be found. The police may also require assistance from a landlord or another entity to implant the register device.
- 18 U.S.C. § 2701 (2009). Unlawful access to stored communications. unlawful to intentionally access without authorization a facility through which an electronic communication service is provided; or intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided.
- 18 U.S.C. § 2702 (2009). Voluntary disclosure of customer communications or records. A person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service, but exceptions allow disclosure to the rightful recipient, to law enforcement in some cases, to a government entity if there is reasonable certainty death or severe bodily injury will result if not disclosed, etc.
- 18 U.S.C. § 2703 (2009). Required disclosure of customer communications or records. Allowed if there is a warrant and the communication has been in storage for less than 180 days and under an administrative subpoena if more than 180 days with notice to the customer.
- 18 U.S.C. § 2709 (2009). Counterintelligence access to telephone toll and transactional records. A wire or electronic communication service provider shall comply with a request for subscriber information and toll billing records information, or electronic communication transactional records in its custody or possession made by the Director of the Federal Bureau of Investigation under subsection (b) of this section [are relevant to an authorized investigation to protect against

international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected under the First Amendment.] Note that library records are not included under this section.

- 18 U.S.C. § 2710 (2009). Wrongful disclosure of video tape rental or sale records. Cant disclose personally identifiable information to anyone except the consumer, pursuant to a warrant, under the written direction of the consumer, to anyone in the ordinary course of business of the consumer, etc.
- 47 U.S.C. § 1002 (2009) - Assistance capability requirements. Communications carriers must have the ability to enable the government, pursuant to a court order or other lawful authorization, to intercept, to the exclusion of any other communications, all wire and electronic communications carried by the carrier within a service area or to and from certain equipment.
- 47 U.S.C. § 1004 (2009) Systems security and integrity. A telecommunications carrier shall ensure that any interception of communications or access to call-identifying information affected within its switching premises can be activated only in accordance with a court order or other lawful authorization and with the affirmative intervention of an individual officer or employee of the carrier acting in accordance with regulations prescribed by the Commission.
- 47 U.S.C. § 1007 (2009) Enforcement orders. To obtain a warrant that would mandate a common carrier to divulge communications requires that alternate ways of obtaining this information are not available and it is possible using current technology to obtain the information requested.
- 50 U.S.C. § 1801 (2009) Definitions. "Electronic surveillance" means-- (1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes; (2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States, but does not include the acquisition of those communications of computer trespassers (3) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; or (4) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.
- 50 U.S.C. §§ 1802 through 1812 (2009) - FISA. Electronic surveillance authorization without court order; certification by Attorney General. Notwithstanding any other law, the President, through the Attorney General, may authorize electronic surveillance without a court order under this title to acquire foreign intelligence information for periods of up to one year if the Attorney General certifies in writing under oath that- (A) the electronic surveillance is solely directed at-- (i) the acquisition of the contents of communications transmitted by means of communications used exclusively between or among foreign powers, or the acquisition of technical intelligence, other than the spoken communications of individuals, from property or premises under the open and exclusive control of a foreign power AND doesn't include communications by US citizens. Note that a judge does not need to find that there is probable cause that the surveillance will lead to finding foreign intelligence information. The order can be no longer than 120 days.
- **Computers**
 - 18 U.S.C. § 1030 (2009). Fraud and related activity in connection with computers. Having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data. Intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains-- (A) information contained in a financial record of a financial institution, or of a card issuer or

contained in a file of a consumer reporting agency on a consumer; (B) information from any department or agency of the United States; or (C) information from any protected computer, OR accesses a computer and obtains anything of value or attempts to commit extortion, causes damage to the computer or the computer network, affects foreign or interstate commerce, etc.

- 18 U.S.C. § 2511 (2009) - permits the interception of wire or electronic communications by a computer trespasser if the communications are through a protected computer and the investigation is engaged lawfully.
- 49 U.S.C. § 145 (2009). Cyber Security Enhancement Act of 2002. permits the study of computer crimes under 18 U.S.C § 1030 and whether those provisions are adequate to prevent and deter crimes.
- 6 USCS § 143 - Non-Federal Cyber Security - as appropriate, the Under Secretary for Intelligence and Analysis shall provide technical assistance, upon request, to the private sector and other government entities, in coordination with the Under Secretary for Emergency Preparedness and Response, with respect to emergency recovery plans to respond to major failures of critical information systems.

APPENDIX B – PART 1
Table Information

This appendix contains the data from the ITSA survey used in the tables throughout the report. In developing an informative table, the responses to several questions were combined to create a more complete response. Listed below are the table numbers and questions used.

Table 3. Types of Information Collected

Personal Information:	Questions: 45, 46, 47, 48, 51
Vehicle Information:	Questions: 19, 20
Financial Information:	Questions: 18

Table 4. Are ITS Systems Built In a Manner “Visible” to Individuals?

Questions: 43, 48

Table 5. Does Your Business Disclose?

Questions: 45, all parts

Table 6. Are Data That the ITS Collects Secure?

Questions: 26, 28, 35, 37, 38, 43a, 43b, 48

Table 7. What Technique or Process Do You Use to Ensure Data are Secure?

Questions: 40, 41, 35

Table 8. Can People Choose to be Anonymous to Other Than Law Enforcement?

Questions: 43, 46, 47, 48

Table 9. What Kind of Information is Collected?

Questions: 17, 18, 19

Table 10. How Anonymity is Preserved.

Questions: 43, 46, 47, 48

Table 11. How Do ITS Businesses Handle Disclosure of ITS Data Collection Processes?

Question: 45

Table 12. Does Your ITS Business Comply With the “Fair Information and Privacy Principles?”

Questions: 35, 38, 40, 48

Part 2
ITS America Survey

ITS America Membership VTTI Privacy – Safety Project

1. Survey Background

This survey is sponsored by ITS America in cooperation with the Virginia Tech Transportation Institute (VTTI). We are gathering information from our members about current and emerging transportation technology and the privacy issues that may be associated with deployment. The information you submit will be treated as confidential and only aggregated data will be published.

The survey will take approximately 20 minutes to complete.

ITS America Membership VTTI Privacy – Safety Project**2. ITS Transportation Technology Survey**

The survey questions which begin on the next page are grouped according to the ITS architecture identified by the Federal Highway Administration.

They include questions about:

1. Advanced Traffic Management Systems (ATMS)
2. Maintenance and Construction Operations (MCO)
3. Advanced Public Transportation Systems (APTS)
4. Advanced Traveler Information Systems (ATIS)
5. Commercial Vehicle Operations (CVO)
6. Emergency Management (EM)
7. Archived Data (AD)
8. Advanced Vehicle Safety Systems (AVSS)

The survey is constructed to allow you to skip ITS functions and applications that you are not involved in as a researcher, designer, manufacturer, or operator. Please check YES only to those functions or applications that your business involves. Remember, you must check NO to skip a question.

ITS America Membership VTI Privacy – Safety Project

3. Advanced Traffic Management Systems (ATMS): Check boxes that apply to your...

Please check whether your company uses, researches, develops, deploys, and/or operates any of the eight following transportation applications related to surface transportation (highway, rail, transit, commercial freight, passenger rail). Check YES if your technology applies to this ITS application. Check NO if you wish to skip this question.

*** 1. Advanced Traffic Management Systems (ATMS). This question requires an answer**

Yes

No

ITS America Membership VTI Privacy – Safety Project

4. Advanced Traffic Management Systems (ATMS)

2. Advanced Traffic Management Systems (ATMS). Check each box that applies to your technology.

	Do you operate ITS Technology?	Do you conduct ITS Research?	Do you Deploy ITS Technology?	Do you build ITS Technology?	Is the technology for use in a vehicle?	Is the technology for use in the infrastructure?	Does the technology interact between vehicles and the infrastructure?
Network Surveillance	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Traffic Probe Surveillance	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Surface Street Control	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Freeway Control	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
HOV Lane Management	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Traffic Information Dissemination	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Regional Traffic Management	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Traffic Incident Management System	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Traffic Forecast and Demand Management	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Electronic Toll Collection	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Emissions Monitoring and Management	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Parking Facility Management	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Regional Parking Management	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Reversible Lane Management	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Speed Monitoring	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

ITS America Membership VTI Privacy – Safety Project

5. Maintenance and Construction Operations (MCO)

Please check whether your company uses, researches, develops, deploys, and/or operates any of the eight following transportation applications related to surface transportation (highway, rail, transit, commercial freight, passenger rail)

* 3. Maintenance and Construction Operations (MCO)

Yes

No

ITS America Membership VTTI Privacy – Safety Project

6. Maintenance and Construction Operations (MCO). Check each box that applies...

4. Maintenance and Construction Operations (MCO).

	Do you operate ITS Technology?	Do you conduct ITS Research?	Do you Deploy ITS Technology?	Do you build ITS Technology?	Is the technology for use in a vehicle?	Is the technology for use in the infrastructure?	Does the technology interact between vehicles and the infrastructure?
Maint and Constr Vehicle and Equipment Tracking	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Maintenance and Construction Vehicle	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Road Weather Data Collection	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Weather Information Processing and Distribution	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Roadway Automated Treatment	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Maintenance and Construction Activity Coordination	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Environmental Probe Surveillance	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Infrastructure Monitoring	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

ITS America Membership VTI Privacy – Safety Project

7. Advanced Public Transportation Systems (APTS)

Please check whether your company uses, researches, develops, deploys, and/or operates any of the eight following transportation applications related to surface transportation (highway, rail, transit, commercial freight, passenger rail). Check NO to skip.

*** 5. Advanced Public Transportation Systems (APTS)**

Yes

No

ITS America Membership VTTI Privacy – Safety Project

8. Advanced Public Transportation Systems (APTS)

6. Advanced Public Transportation Systems (APTS). Check each box that applies to your technology.

	Do you operate ITS Technology?	Do you conduct ITS Research?	Do you Deploy ITS Technology?	Do you build ITS Technology?	Is the technology for use in a vehicle?	Is the technology for use in the infrastructure?	Does the technology interact between vehicles and the infrastructure?
Transit Vehicle Tracking	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Transit Fixed-Route Operations	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Demand Response	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Transit Operations	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Transit Fare Collection Management	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Transit Security	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Transit Fleet Management	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Multi-modal Coordination	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Transit Traveler Information	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Smart Card Data	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Transit Passenger Counting	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

ITS America Membership VTTI Privacy – Safety Project

9. Advanced Traveler Information Systems (ATIS)

Please check whether your company uses, researches, develops, deploys, and/or operates any of the eight following transportation applications related to surface transportation (highway, rail, transit, commercial freight, passenger rail). Check NO to skip.

* 7. Advanced Traveler Information Systems (ATIS)

Yes

No

ITS America Membership VTTI Privacy – Safety Project

10. Advanced Traveler Information Systems (ATIS)

8. Advanced Traveler Information Systems (ATIS). Check each box that applies to your technology.

	Do you operate ITS Technology?	Do you conduct ITS Research?	Do you Deploy ITS Technology?	Do you build ITS Technology?	Is the technology for use in a vehicle?	Is the technology for use in the infrastructure?	Does the technology interact between vehicles and the infrastructure?
Broadcast Traveler Information	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Interactive Traveler Information	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Autonomous Route Guidance	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Dynamic Route Guidance	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
ISP Based Trip Planning and Route Guidance	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Transportation Operations Data Sharing	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Yellow Pages and Reservation	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Dynamic Ridesharing	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
In Vehicle Signing	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VII Based Traveler Information	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

ITS America Membership VTTI Privacy – Safety Project

11. Commercial Vehicle Operations (CVO)

Please check whether your company uses, researches, develops, deploys, and/or operates any of the eight following transportation applications related to surface transportation (highway, rail, transit, commercial freight, passenger rail). Check NO to skip.

* 9. Commercial Vehicle Operations (CVO)

Yes

No

ITS America Membership VTTI Privacy – Safety Project

12. Commercial Vehicle Operations (CVO)

10. Commercial Vehicle Operations (CVO). Check each box that applies to your technology.

	Do you operate ITS Technology?	Do you conduct ITS Research?	Do you Deploy ITS Technology?	Do you build ITS Technology?	Is the technology for use in a vehicle?	Is the technology for use in the infrastructure?	Does the technology interact between vehicles and the infrastructure?
Fleet Administration	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Freight Administration	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
CV Administrative Processes	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
International Border Electronic Clearance	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Weigh-In-Motion	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Roadside CVO Safety	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
On-board CVO and Freight Safety and Security	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
CVO Fleet Maintenance	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
HAZMAT Management	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Roadside HAZMAT Security	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Detection and Mitigation	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
CV Driver Security Authentication	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Freight Assignment Tracking	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

ITS America Membership VTTI Privacy – Safety Project

13. Emergency Management (EM)

Please check whether your company uses, researches, develops, deploys, and/or operates any of the eight following transportation applications related to surface transportation (highway, rail, transit, commercial freight, passenger rail). Check NO to skip.

* 11. Emergency Management (EM)

Yes

No

ITS America Membership VTTI Privacy – Safety Project

14. Emergency Management (EM)

12. Emergency Management (EM). Check each box that applies to your technology.

	Do you operate ITS Technology?	Do you conduct ITS Research?	Do you Deploy ITS Technology?	Do you build ITS Technology?	Is the technology for use in a vehicle?	Is the technology for use in the infrastructure?	Does the technology interact between vehicles and the infrastructure?
Emergency Call-Taking and Dispatch	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Emergency Routing	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Mayday and Alarms Support	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Transportation Infrastructure Protection	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Wide-Area Alert	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Disaster Response and Recovery	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Evacuation and Reentry Management	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Disaster Traveler Information	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

ITS America Membership VTTI Privacy – Safety Project

15. Archived Data (AD)

Please check whether your company uses, researches, develops, deploys, and/or operates any of the eight following transportation applications related to surface transportation (highway, rail, transit, commercial freight, passenger rail). Check NO to skip.

* 13. Archived Data (AD)

Yes

No

ITS America Membership VTI Privacy – Safety Project

16. Archived Data (AD).

14. Archived Data (AD). Check each box that applies to your technology.

	Do you operate ITS Technology?	Do you conduct ITS Research?	Do you Deploy ITS Technology?	Do you build ITS Technology?	Is the technology for use in a vehicle?	Is the technology for use in the infrastructure?	Does the technology interact between vehicles and the infrastructure?
ITS Data Mart	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
ITS Data Warehouse	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
ITS Virtual Data Warehouse	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

ITS America Membership VTTI Privacy – Safety Project

17. Advanced Vehicle Safety Systems (AVSS)

Please check whether your company uses, researches, develops, deploys, and/or operates any of the eight following transportation applications related to surface transportation (highway, rail, transit, commercial freight, passenger rail). Check NO to skip.

*** 15. Advanced Vehicle Safety Systems (AVSS)**

Yes

No

ITS America Membership VTTI Privacy – Safety Project

18. Advanced Vehicle Safety Systems (AVSS)

16. Advanced Vehicle Safety Systems (AVSS). Check each box that applies to your technology.

	Do you operate ITS Technology?	Do you conduct ITS Research?	Do you Deploy ITS Technology?	Do you build ITS Technology?	Is the technology for use in a vehicle?	Is the technology for use in the infrastructure?	Does the technology interact between vehicles and the infrastructure?
Vehicle Safety Monitoring	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Driver Safety Monitoring	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Longitudinal Safety Warning	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Lateral Safety Warning	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Intersection Safety Warning	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Pre-Crash Restraint Deployment	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Driver Visibility Improvement	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Advanced Vehicle Longitudinal Control	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Advanced Vehicle Lateral Control	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Intersection Collision Avoidance	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Automated Highway System	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Cooperative Vehicle Safety Systems	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

ITS America Membership VTI Privacy – Safety Project

19. Type of Traveler Information

This section asks for data related to the type of personal information you collect and how you process and store that data. For all technologies identified in response to earlier questions, please check Yes or No whether your technology collects or will collect personal traveler information.

17. Personal Information

	Yes	No
Name	<input type="radio"/>	<input type="radio"/>
Address: Business or Home	<input type="radio"/>	<input type="radio"/>
Phone: Business, Home, or Mobile	<input type="radio"/>	<input type="radio"/>
Fax Number	<input type="radio"/>	<input type="radio"/>
E-mail Address	<input type="radio"/>	<input type="radio"/>
Social Security No.	<input type="radio"/>	<input type="radio"/>
Driver's License No./State	<input type="radio"/>	<input type="radio"/>
Signature	<input type="radio"/>	<input type="radio"/>
Medical Insurance	<input type="radio"/>	<input type="radio"/>
Medical Information	<input type="radio"/>	<input type="radio"/>
Driving Record	<input type="radio"/>	<input type="radio"/>
Shipping address	<input type="radio"/>	<input type="radio"/>

18. Vehicle Information

	Yes	No
License Plate/State	<input type="radio"/>	<input type="radio"/>
Make	<input type="radio"/>	<input type="radio"/>
Model	<input type="radio"/>	<input type="radio"/>
Color	<input type="radio"/>	<input type="radio"/>
Year	<input type="radio"/>	<input type="radio"/>
No. of Axles	<input type="radio"/>	<input type="radio"/>
No. of Tires	<input type="radio"/>	<input type="radio"/>
Vehicle Class	<input type="radio"/>	<input type="radio"/>
Complete Vehicle VIN	<input type="radio"/>	<input type="radio"/>
Partial Vehicle VIN	<input type="radio"/>	<input type="radio"/>
Registration Name	<input type="radio"/>	<input type="radio"/>
HAZMAT Code	<input type="radio"/>	<input type="radio"/>

19. Financial Information

	Yes	No
Credit Card No.	<input type="radio"/>	<input type="radio"/>
Debit Card	<input type="radio"/>	<input type="radio"/>
Bank Account No.	<input type="radio"/>	<input type="radio"/>
Household Income	<input type="radio"/>	<input type="radio"/>

ITS America Membership VTI Privacy – Safety Project

20. Security Information

	Yes	No
Customer Selected PIN number	<input type="radio"/>	<input type="radio"/>
Customer Selected password	<input type="radio"/>	<input type="radio"/>

21. Visual Images

	Yes	No
Video	<input type="radio"/>	<input type="radio"/>
Photograph	<input type="radio"/>	<input type="radio"/>
biometrics	<input type="radio"/>	<input type="radio"/>
other	<input type="radio"/>	<input type="radio"/>

22. Location

	Yes	No
Vehicle location	<input type="radio"/>	<input type="radio"/>
Vehicle movement (continuous or episodic)	<input type="radio"/>	<input type="radio"/>
Type of Freight in the vehicle	<input type="radio"/>	<input type="radio"/>

**23. What types of technology is used to collect data?
(Please check all appropriate boxes.)**

Wi-Fi

Wi-Max

Infrared

Bluetooth

DSRC

Other (please specify)

24. How and in what form is data collected (read only, read-write, smart)?

Read Only

Read-Write

Smart

25. Is data combined with other data, such as applications to subscribe to the technology, driving records, or credit records?

Yes

No

ITS America Membership VTTI Privacy – Safety Project

20. Data Handling

26. Is the data used for any purpose other than providing the transportation service, such as law enforcement, marketing, travel time estimates, vehicle counts for planning purposes?

- Yes
- No

27. Have third parties requested customer data?

- Yes
- No

28. Were the requests granted?

- Yes
- No

29. If yes, was the request from a:

- Public entity (Ex: Court order, Subpoena)
- Private entity (Ex: Credit Agency, Insurance Co.)

30. If yes, how are they using the data?

31. Does the data have value to:

	Yes	No
Law enforcement (investigate accidents/violation enforcement/criminal investigations)	<input type="checkbox"/>	<input type="checkbox"/>
Insurance companies	<input type="checkbox"/>	<input type="checkbox"/>
Mobile phone companies	<input type="checkbox"/>	<input type="checkbox"/>
Government planning organizations	<input type="checkbox"/>	<input type="checkbox"/>
Developers	<input type="checkbox"/>	<input type="checkbox"/>
Research organizations	<input type="checkbox"/>	<input type="checkbox"/>
Market researchers	<input type="checkbox"/>	<input type="checkbox"/>
Fleet operators	<input type="checkbox"/>	<input type="checkbox"/>
Private Investigators	<input type="checkbox"/>	<input type="checkbox"/>
Others	<input type="checkbox"/>	<input type="checkbox"/>

32. How is data processed?

ITS America Membership VTI Privacy – Safety Project

33. How is data stored? (Please Check All Appropriate)

- Centralized computer system
- Decentralized computer system
- Networked to other systems
- Aggregate form
- Stripped of personal identifiers

34. If aggregated, is the data combined with any other data?

- Yes
- No

35. Does your organization have a Chief Privacy Officer or equivalent?

- Yes
- No

36. Who within your organization has access to the data?

37. Do third-parties have access to the data?

- Yes
- No

38. Does your organization have a policy on giving or selling information?

- Yes
- No

39. How and to whom is data distributed?

40. What technical security mechanisms are in place to prevent tampering with data?

- Data encryption
- Access control through passwords
- Activity logs
- Check sums to detect alteration of data during transmission or storage
- Other (please specify)

ITS America Membership VTI Privacy – Safety Project

41. What non-technical security mechanisms are in place to prevent tampering with data?

- Written policies
- Personnel background checks
- Training programs
- Personnel surveillance
- Other (please specify)

42. For how long is data retained?

ITS America Membership VTI Privacy – Safety Project

21. Data Handling

43. For all transportation technologies that collect or will collect personal information, state whether your organization removes or will remove personal information from the data collected and/or whether your organization provides or will provide an opportunity for individuals to choose not to have personally identifiable information collected?

	Yes	No
Removes Personal Information	<input type="radio"/>	<input type="radio"/>
Gives Individuals A Choice	<input type="radio"/>	<input type="radio"/>

44. Please describe any other measures undertaken by your business to:

(1) safeguard collection, use, or distribution of personally identifiable information

(2) eliminate personally identifiable data collected in the course of operating transportation technologies.

45. For all transportation technologies identified in earlier responses, please indicate if your business discloses or will disclose to others:

	Yes	No
The type of data collected:	<input type="checkbox"/>	<input type="checkbox"/>
How the data is collected:	<input type="checkbox"/>	<input type="checkbox"/>
The purpose for collecting the data:	<input type="checkbox"/>	<input type="checkbox"/>
How is the data used:	<input type="checkbox"/>	<input type="checkbox"/>
How the data is processed:	<input type="checkbox"/>	<input type="checkbox"/>
Who has access to the data:	<input type="checkbox"/>	<input type="checkbox"/>
How the data is stored:	<input type="checkbox"/>	<input type="checkbox"/>
How the data is distributed:	<input type="checkbox"/>	<input type="checkbox"/>
How long the data is retained:	<input type="checkbox"/>	<input type="checkbox"/>

46. Does or will your business provide an opportunity for individuals or users of the transportation technologies identified in earlier questions to access and correct personal information?

Yes
 No

ITS America Membership VTTI Privacy – Safety Project

47. For all transportation technologies please indicate whether your organization will provide an opportunity for individuals to opt out of the collection of traveler information?

Yes

No

48. Does your business have or are you developing any protocol, internal policies, or procedures for the collection, use, distribution, retention, or disposal of personally identifiable information collected in the course of operating and maintaining transportation technology systems?

Yes

No

49. If YES, please briefly describe the protocol, policies and/or procedures.

50. Please identify the number and job title of employees within your business who work on managing personally identifiable information.

51. Do you disclose any change in privacy policies?

Yes

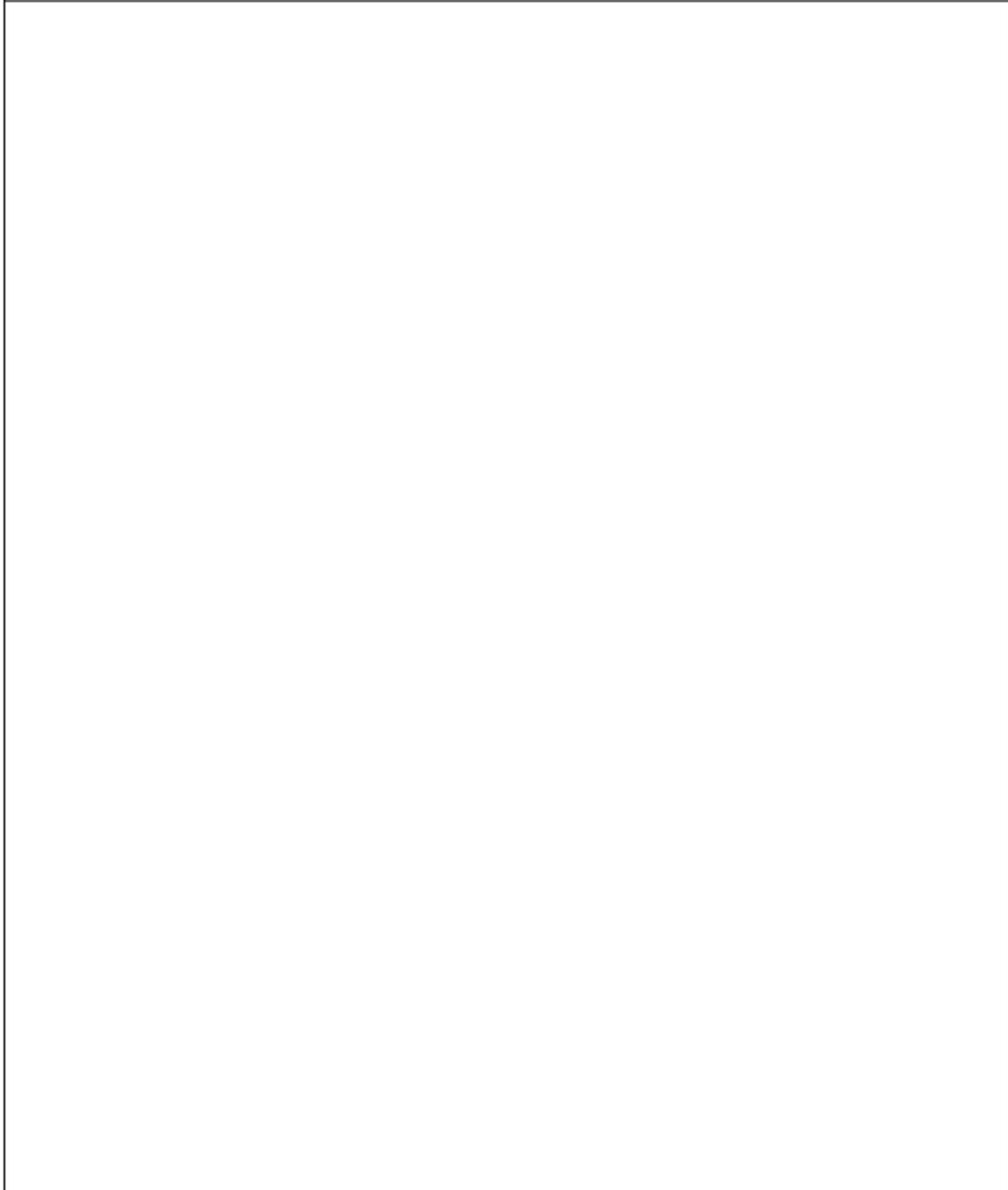
No

52. Could you describe the nature of technologies your company is involved with.

53. Could you describe any new or emerging technologies or application that might be relevant to privacy in the future.

ITS America Membership VTI Privacy – Safety Project

22. Thank You



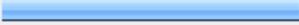
Part 3
Survey Response Summary

ITS America Membership VTTI Privacy – Safety Project

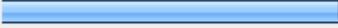
1. Advanced Traffic Management Systems (ATMS). This question requires an answer.			Response Percent	Response Count
Yes			81.3%	74
No			18.7%	17
			<i>answered question</i>	91
			<i>skipped question</i>	0

2. Advanced Traffic Management Systems (ATMS). Check each box that applies to your technology.						
	Do you operate ITS Technology?	Do you conduct ITS Research?	Do you Deploy ITS Technology?	Do you build ITS Technology?	Is the technology for use in a vehicle?	Is technology use in infrastructure?
Network Surveillance	41.9% (13)	51.6% (16)	67.7% (21)	35.5% (11)	19.4% (6)	80.6%
Traffic Probe Surveillance	23.5% (4)	70.6% (12)	58.8% (10)	35.3% (6)	47.1% (8)	64.7%
Surface Street Control	39.3% (11)	53.6% (15)	50.0% (14)	42.9% (12)	0.0% (0)	71.4%
Freeway Control	28.6% (8)	46.4% (13)	42.9% (12)	35.7% (10)	7.1% (2)	71.4%
HOV Lane Management	33.3% (8)	44.4% (8)	44.4% (8)	27.8% (5)	11.1% (2)	61.1%
Traffic Information Dissemination	43.2% (16)	51.4% (19)	51.4% (19)	32.4% (12)	21.6% (8)	67.6%
Regional Traffic Management	44.4% (12)	51.9% (14)	51.9% (14)	33.3% (9)	7.4% (2)	66.7%
Traffic Incident Management System	32.3% (10)	54.8% (17)	48.4% (15)	32.3% (10)	12.9% (4)	64.5%
Traffic Forecast and Demand Management	23.5% (4)	64.7% (11)	47.1% (8)	17.6% (3)	23.5% (4)	47.1%
Electronic Toll Collection	50.0% (6)	50.0% (6)	50.0% (6)	33.3% (4)	25.0% (3)	41.7%
Emissions Monitoring and Management	46.7% (7)	80.0% (12)	40.0% (6)	26.7% (4)	26.7% (4)	53.3%
Parking Facility Management	23.1% (3)	69.2% (9)	46.2% (6)	23.1% (3)	15.4% (2)	69.2%
Regional Parking Management	33.3% (2)	83.3% (5)	16.7% (1)	0.0% (0)	0.0% (0)	33.3%
Reversible Lane Management	25.0% (2)	50.0% (4)	62.5% (5)	37.5% (3)	12.5% (1)	75.0%
Speed Monitoring	26.9% (7)	53.8% (14)	50.0% (13)	46.2% (12)	11.5% (3)	73.1%

Survey Response Summary

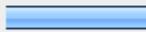
3. Maintenance and Construction Operations (MCO)			Response Percent	Response Count
Yes			39.7%	27
No			60.3%	41
			<i>answered question</i>	68
			<i>skipped question</i>	23

4. Maintenance and Construction Operations (MCO).						
	Do you operate ITS Technology?	Do you conduct ITS Research?	Do you Deploy ITS Technology?	Do you build ITS Technology?	Is the technology for use in a vehicle?	Is technology use in infrastructure?
Maint and Constr Vehicle and Equipment Tracking	61.5% (8)	69.2% (9)	69.2% (9)	15.4% (2)	61.5% (8)	46.2%
Maintenance and Construction Vehicle Maintenance	75.0% (6)	37.5% (3)	37.5% (3)	25.0% (2)	25.0% (2)	50.0%
Road Weather Data Collection	64.7% (11)	70.6% (12)	70.6% (12)	29.4% (5)	47.1% (8)	70.6%
Weather Information Processing and Distribution	66.7% (10)	73.3% (11)	66.7% (10)	20.0% (3)	33.3% (5)	66.7%
Roadway Automated Treatment	57.1% (4)	57.1% (4)	71.4% (5)	14.3% (1)	28.6% (2)	57.1%
Maintenance and Construction Activity Coordination	50.0% (7)	57.1% (8)	42.9% (6)	14.3% (2)	21.4% (3)	50.0%
Environmental Probe Surveillance	57.1% (4)	85.7% (6)	71.4% (5)	28.6% (2)	42.9% (3)	71.4%
Infrastructure Monitoring	50.0% (5)	80.0% (8)	60.0% (6)	30.0% (3)	40.0% (4)	60.0%

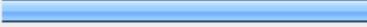
5. Advanced Public Transportation Systems (APTS)			Response Percent	Response Count
Yes			31.8%	21
No			68.2%	45
			<i>answered question</i>	66
			<i>skipped question</i>	25

6. Advanced Public Transportation Systems (APTS). Check each box that applies to your technology.						
	Do you operate ITS Technology?	Do you conduct ITS Research?	Do you Deploy ITS Technology?	Do you build ITS Technology?	Is the technology for use in a vehicle?	Is technology use in infrastructure?
Transit Vehicle Tracking	38.9% (7)	66.7% (12)	22.2% (4)	5.6% (1)	61.1% (11)	38.9%
Transit Fixed-Route Operations	63.6% (7)	45.5% (5)	27.3% (3)	9.1% (1)	45.5% (5)	27.3%
Demand Response Transit Operations	55.6% (5)	55.6% (5)	22.2% (2)	0.0% (0)	44.4% (4)	33.3%
Transit Fare Collection Management	66.7% (6)	44.4% (4)	44.4% (4)	33.3% (3)	55.6% (5)	22.2%
Transit Security	71.4% (5)	42.9% (3)	42.9% (3)	14.3% (1)	57.1% (4)	28.6%
Transit Fleet Management	41.7% (5)	66.7% (8)	25.0% (3)	8.3% (1)	50.0% (6)	50.0%
Multi-modal Coordination	50.0% (4)	50.0% (4)	25.0% (2)	25.0% (2)	25.0% (2)	25.0%
Transit Traveler Information	60.0% (9)	53.3% (8)	33.3% (5)	13.3% (2)	40.0% (6)	53.3%
Smart Card Data	60.0% (3)	40.0% (2)	40.0% (2)	20.0% (1)	60.0% (3)	60.0%
Transit Passenger Counting	60.0% (6)	40.0% (4)	40.0% (4)	10.0% (1)	60.0% (6)	40.0%

Survey Response Summary

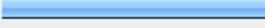
7. Advanced Traveler Information Systems (ATIS)			Response Percent	Response Count
Yes			71.2%	47
No			28.8%	19
			<i>answered question</i>	66
			<i>skipped question</i>	25

8. Advanced Traveler Information Systems (ATIS). Check each box that applies to your technology.						
	Do you operate ITS Technology?	Do you conduct ITS Research?	Do you Deploy ITS Technology?	Do you build ITS Technology?	Is the technology for use in a vehicle?	Is technology use in infrastructure?
Broadcast Traveler Information	66.7% (20)	56.7% (17)	56.7% (17)	20.0% (6)	33.3% (10)	56.7%
Interactive Traveler Information	73.1% (19)	50.0% (13)	50.0% (13)	38.5% (10)	42.3% (11)	57.7%
Autonomous Route Guidance	62.5% (5)	62.5% (5)	50.0% (4)	37.5% (3)	50.0% (4)	62.5%
Dynamic Route Guidance	33.3% (4)	91.7% (11)	41.7% (5)	25.0% (3)	41.7% (5)	50.0%
ISP Based Trip Planning and Route Guidance	46.2% (6)	61.5% (8)	38.5% (5)	15.4% (2)	15.4% (2)	46.2%
Transportation Operations Data Sharing	57.7% (15)	53.8% (14)	53.8% (14)	23.1% (6)	7.7% (2)	53.8%
Yellow Pages and Reservation	100.0% (4)	100.0% (4)	100.0% (4)	100.0% (4)	75.0% (3)	100.0%
Dynamic Ridesharing	0.0% (0)	100.0% (2)	0.0% (0)	0.0% (0)	0.0% (0)	0.0%
In Vehicle Signing	12.5% (1)	75.0% (6)	25.0% (2)	0.0% (0)	50.0% (4)	25.0%
VII Based Traveler Information	16.7% (2)	83.3% (10)	33.3% (4)	8.3% (1)	41.7% (5)	41.7%

9. Commercial Vehicle Operations (CVO)			Response Percent	Response Count
Yes			25.8%	17
No			74.2%	49
			<i>answered question</i>	66
			<i>skipped question</i>	25

10. Commercial Vehicle Operations (CVO). Check each box that applies to your technology.						
	Do you operate ITS Technology?	Do you conduct ITS Research?	Do you Deploy ITS Technology?	Do you build ITS Technology?	Is the technology for use in a vehicle?	Is technology used in infrastructure?
Fleet Administration	25.0% (1)	75.0% (3)	50.0% (2)	50.0% (2)	100.0% (4)	75.0%
Freight Administration	0.0% (0)	75.0% (3)	25.0% (1)	25.0% (1)	50.0% (2)	50.0%
CV Administrative Processes	50.0% (2)	50.0% (2)	50.0% (2)	50.0% (2)	25.0% (1)	25.0%
International Border Electronic Clearance	0.0% (0)	50.0% (1)	50.0% (1)	50.0% (1)	50.0% (1)	100.0%
Weigh-In-Motion	37.5% (3)	37.5% (3)	50.0% (4)	25.0% (2)	25.0% (2)	75.0%
Roadside CVO Safety	28.6% (2)	85.7% (6)	28.6% (2)	14.3% (1)	42.9% (3)	57.1%
On-board CVO and Freight Safety and Security	25.0% (1)	75.0% (3)	0.0% (0)	0.0% (0)	50.0% (2)	50.0%
CVO Fleet Maintenance	0.0% (0)	100.0% (2)	0.0% (0)	0.0% (0)	50.0% (1)	50.0%
HAZMAT Management	25.0% (1)	75.0% (3)	0.0% (0)	0.0% (0)	50.0% (2)	75.0%
Roadside HAZMAT Security Detection and Mitigation	0.0% (0)	100.0% (1)	0.0% (0)	0.0% (0)	100.0% (1)	100.0%
CV Driver Security Authentication	50.0% (1)	50.0% (1)	50.0% (1)	0.0% (0)	50.0% (1)	50.0%
Freight Assignment Tracking	0.0% (0)	100.0% (3)	0.0% (0)	0.0% (0)	66.7% (2)	66.7%

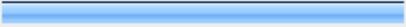
Survey Response Summary

11. Emergency Management (EM)			Response Percent	Response Count
Yes			53.8%	35
No			46.2%	30
			<i>answered question</i>	65
			<i>skipped question</i>	26

12. Emergency Management (EM). Check each box that applies to your technology.						
	Do you operate ITS Technology?	Do you conduct ITS Research?	Do you Deploy ITS Technology?	Do you build ITS Technology?	Is the technology for use in a vehicle?	Is technology use in infrastructure?
Emergency Call-Taking and Dispatch	57.1% (12)	38.1% (8)	47.6% (10)	14.3% (3)	33.3% (7)	38.1%
Emergency Routing	43.8% (7)	50.0% (8)	56.3% (9)	12.5% (2)	18.8% (3)	31.3%
Mayday and Alarms Support	80.0% (4)	60.0% (3)	60.0% (3)	20.0% (1)	60.0% (3)	40.0%
Transportation Infrastructure Protection	71.4% (5)	42.9% (3)	28.6% (2)	14.3% (1)	28.6% (2)	42.9%
Wide-Area Alert	64.3% (9)	50.0% (7)	35.7% (5)	14.3% (2)	28.6% (4)	57.1%
Disaster Response and Recovery	63.6% (7)	36.4% (4)	45.5% (5)	9.1% (1)	18.2% (2)	45.5%
Evacuation and Reentry Management	75.0% (9)	33.3% (4)	50.0% (6)	25.0% (3)	8.3% (1)	33.3%
Disaster Traveler Information	50.0% (11)	45.5% (10)	45.5% (10)	18.2% (4)	27.3% (6)	45.5%

13. Archived Data (AD)			Response Percent	Response Count
Yes			42.2%	27
No			57.8%	37
			<i>answered question</i>	64
			<i>skipped question</i>	27

14. Archived Data (AD). Check each box that applies to your technology.						
	Do you operate ITS Technology?	Do you conduct ITS Research?	Do you Deploy ITS Technology?	Do you build ITS Technology?	Is the technology for use in a vehicle?	Is technology use in infrastructure?
ITS Data Mart	80.0% (8)	30.0% (3)	50.0% (5)	30.0% (3)	30.0% (3)	50.0%
ITS Data Warehouse	60.0% (12)	55.0% (11)	45.0% (9)	20.0% (4)	10.0% (2)	55.0%
ITS Virtual Data Warehouse	60.0% (6)	40.0% (4)	60.0% (6)	40.0% (4)	20.0% (2)	40.0%
<i>answered question</i>						
<i>skipped question</i>						

15. Advanced Vehicle Safety Systems (AVSS)			Response Percent	Response Count
Yes			18.8%	12
No			81.3%	52
			<i>answered question</i>	64
			<i>skipped question</i>	27

16. Advanced Vehicle Safety Systems (AVSS). Check each box that applies to your technology.						
	Do you operate ITS Technology?	Do you conduct ITS Research?	Do you Deploy ITS Technology?	Do you build ITS Technology?	Is the technology for use in a vehicle?	Is technology use in infrastructure?
Vehicle Safety Monitoring	10.0% (1)	80.0% (8)	0.0% (0)	0.0% (0)	0.0% (0)	0.0%
Driver Safety Monitoring	12.5% (1)	75.0% (6)	0.0% (0)	0.0% (0)	12.5% (1)	0.0%
Longitudinal Safety Warning	0.0% (0)	66.7% (4)	0.0% (0)	0.0% (0)	33.3% (2)	0.0%
Lateral Safety Warning	0.0% (0)	66.7% (4)	0.0% (0)	0.0% (0)	33.3% (2)	0.0%
Intersection Safety Warning	0.0% (0)	85.7% (6)	0.0% (0)	0.0% (0)	0.0% (0)	0.0%
Pre-Crash Restraint Deployment	0.0% (0)	80.0% (4)	0.0% (0)	0.0% (0)	20.0% (1)	0.0%
Driver Visibility Improvement	0.0% (0)	100.0% (4)	0.0% (0)	0.0% (0)	0.0% (0)	0.0%
Advanced Vehicle Longitudinal Control	0.0% (0)	60.0% (3)	0.0% (0)	0.0% (0)	40.0% (2)	0.0%
Advanced Vehicle Lateral Control	0.0% (0)	100.0% (5)	0.0% (0)	0.0% (0)	0.0% (0)	0.0%
Intersection Collision Avoidance	0.0% (0)	85.7% (6)	0.0% (0)	0.0% (0)	0.0% (0)	0.0%
Automated Highway System	0.0% (0)	100.0% (6)	0.0% (0)	0.0% (0)	0.0% (0)	0.0%
Cooperative Vehicle Safety Systems	0.0% (0)	77.8% (7)	0.0% (0)	0.0% (0)	22.2% (2)	0.0%

Survey Response Summary

17. Personal Information			
	Yes	No	Response Count
Name	18.4% (9)	81.6% (40)	49
Address: Business or Home	10.6% (5)	89.4% (42)	47
Phone: Business, Home, or Mobile	20.4% (10)	79.6% (39)	49
Fax Number	6.1% (3)	93.9% (46)	49
E-mail Address	18.4% (9)	81.6% (40)	49
Social Security No.	0.0% (0)	100.0% (46)	46
Driver's License No./State	2.2% (1)	97.8% (45)	46
Signature	2.1% (1)	97.9% (47)	48
Medical Insurance	0.0% (0)	100.0% (48)	48
Medical Information	4.2% (2)	95.8% (46)	48
Driving Record	0.0% (0)	100.0% (48)	48
Shipping address	4.3% (2)	95.7% (45)	47
	<i>answered question</i>		50
	<i>skipped question</i>		41

Survey Response Summary

18. Vehicle Information			
	Yes	No	Response Count
License Plate/State	30.4% (14)	69.6% (32)	46
Make	23.4% (11)	76.6% (36)	47
Model	23.4% (11)	76.6% (36)	47
Color	23.9% (11)	76.1% (35)	46
Year	17.4% (8)	82.6% (38)	46
No. of Axles	32.6% (15)	67.4% (31)	46
No. of Tires	20.0% (9)	80.0% (36)	45
Vehicle Class	41.3% (19)	58.7% (27)	46
Complete Vehicle VIN	10.9% (5)	89.1% (41)	46
Partial Vehicle VIN	6.7% (3)	93.3% (42)	45
Registration Name	2.3% (1)	97.7% (43)	44
HAZMAT Code	15.6% (7)	84.4% (38)	45
		<i>answered question</i>	50
		<i>skipped question</i>	41

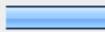
19. Financial Information			
	Yes	No	Response Count
Credit Card No.	10.6% (5)	89.4% (42)	47
Debit Card	6.5% (3)	93.5% (43)	46
Bank Account No.	4.3% (2)	95.7% (45)	47
Household Income	0.0% (0)	100.0% (46)	46
		<i>answered question</i>	47
		<i>skipped question</i>	44

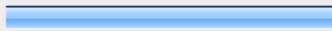
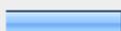
Survey Response Summary

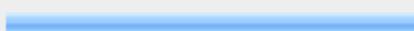
20. Security Information			
	Yes	No	Response Count
Customer Selected PIN number	14.9% (7)	85.1% (40)	47
Customer Selected password	16.7% (8)	83.3% (40)	48
	<i>answered question</i>		48
	<i>skipped question</i>		43

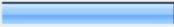
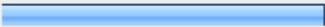
21. Visual Images			
	Yes	No	Response Count
Video	47.1% (24)	52.9% (27)	51
Photograph	40.8% (20)	59.2% (29)	49
biometrics	6.3% (3)	93.8% (45)	48
other	8.9% (4)	91.1% (41)	45
	<i>answered question</i>		51
	<i>skipped question</i>		40

22. Location			
	Yes	No	Response Count
Vehicle location	55.1% (27)	44.9% (22)	49
Vehicle movement (continuous or episodic)	44.7% (21)	55.3% (26)	47
Type of Freight in the vehicle	11.4% (5)	88.6% (39)	44
	<i>answered question</i>		49
	<i>skipped question</i>		42

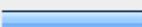
23. What types of technology is used to collect data? (Please check all appropriate boxes.)			Response Percent	Response Count
Wi-Fi		72.0%	18	
Wi-Max		20.0%	5	
Infrared		12.0%	3	
Bluetooth		16.0%	4	
DSRC		40.0%	10	
Other (please specify)				24
			answered question	25
			skipped question	66

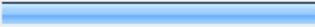
24. How and in what form is data collected (read only, read-write, smart)?			Response Percent	Response Count
Read Only		66.7%	26	
Read-Write		30.8%	12	
Smart		23.1%	9	
			answered question	39
			skipped question	52

25. Is data combined with other data, such as applications to subscribe to the technology, driving records, or credit records?			Response Percent	Response Count
Yes		18.2%	8	
No		84.1%	37	
			answered question	44
			skipped question	47

26. Is the data used for any purpose other than providing the transportation service, such as law enforcement, marketing, travel time estimates, vehicle counts for planning purposes?			
		Response Percent	Response Count
Yes		34.9%	15
No		65.1%	28
<i>answered question</i>			43
<i>skipped question</i>			48

27. Have third parties requested customer data?			
		Response Percent	Response Count
Yes		41.5%	17
No		58.5%	24
<i>answered question</i>			41
<i>skipped question</i>			50

28. Were the requests granted?			
		Response Percent	Response Count
Yes		28.1%	9
No		71.9%	23
<i>answered question</i>			32
<i>skipped question</i>			59

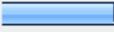
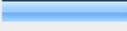
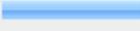
29. If yes, was the request from a:		
		Response Percent
		Response Count
Public entity (Ex: Court order, Subpoena)		63.6%
Private entity (Ex: Credit Agency, Insurance Co.)		54.5%
	<i>answered question</i>	11
	<i>skipped question</i>	80

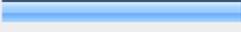
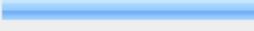
30. If yes, how are they using the data?		
		Response Count
		6
	<i>answered question</i>	6
	<i>skipped question</i>	85

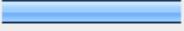
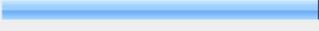
Survey Response Summary

31. Does the data have value to:			
	Yes	No	Response Count
Law enforcement (investigate accidents/violation enforcement/criminal investigations)	67.6% (25)	32.4% (12)	37
Insurance companies	50.0% (17)	50.0% (17)	34
Mobile phone companies	21.2% (7)	78.8% (26)	33
Government planning organizations	86.1% (31)	13.9% (5)	36
Developers	48.5% (16)	51.5% (17)	33
Research organizations	70.6% (24)	29.4% (10)	34
Market researchers	55.9% (19)	44.1% (15)	34
Fleet operators	45.5% (15)	54.5% (18)	33
Private Investigators	39.4% (13)	60.6% (20)	33
Others	37.5% (9)	62.5% (15)	24
	<i>answered question</i>		39
	<i>skipped question</i>		52

32. How is data processed?		
		Response Count
		18
	<i>answered question</i>	18
	<i>skipped question</i>	73

33. How is data stored? (Please Check All Appropriate)			Response Percent	Response Count
Centralized computer system			75.0%	27
Decentralized computer system			22.2%	8
Networked to other systems			25.0%	9
Aggregate form			27.8%	10
Stripped of personal identifiers			25.0%	9
			<i>answered question</i>	36
			<i>skipped question</i>	55

34. If aggregated, is the data combined with any other data?			Response Percent	Response Count
Yes			48.4%	15
No			51.6%	16
			<i>answered question</i>	31
			<i>skipped question</i>	60

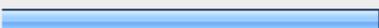
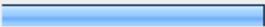
35. Does your organization have a Chief Privacy Officer or equivalent?			Response Percent	Response Count
Yes			35.9%	14
No			64.1%	25
			<i>answered question</i>	39
			<i>skipped question</i>	52

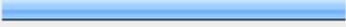
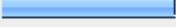
36. Who within your organization has access to the data?		
		Response Count
		28
		<i>answered question</i>
		28
		<i>skipped question</i>
		63

37. Do third-parties have access to the data?			
		Response Percent	Response Count
Yes		27.5%	11
No		72.5%	29
		<i>answered question</i>	40
		<i>skipped question</i>	51

38. Does your organization have a policy on giving or selling information?			
		Response Percent	Response Count
Yes		64.1%	25
No		35.9%	14
		<i>answered question</i>	39
		<i>skipped question</i>	52

39. How and to whom is data distributed?		
		Response Count
		25
		<i>answered question</i>
		25
		<i>skipped question</i>
		66

40. What technical security mechanisms are in place to prevent tampering with data?			
		Response Percent	Response Count
Data encryption		55.9%	19
Access control through passwords		76.5%	26
Activity logs		52.9%	18
Check sums to detect alteration of data during transmission or storage		29.4%	10
Other (please specify)		14.7%	5
		<i>answered question</i>	34
		<i>skipped question</i>	57

41. What non-technical security mechanisms are in place to prevent tampering with data?			
		Response Percent	Response Count
Written policies		80.8%	21
Personnel background checks		38.5%	10
Training programs		69.2%	18
Personnel surveillance		34.6%	9
Other (please specify)		15.4%	4
		<i>answered question</i>	26
		<i>skipped question</i>	65

42. For how long is data retained?		
		Response Count
		23
	<i>answered question</i>	23
	<i>skipped question</i>	68

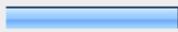
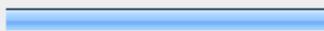
43. For all transportation technologies that collect or will collect personal information, state whether your organization removes or will remove personal information from the data collected and/or whether your organization provides or will provide an opportunity for individuals to choose not to have personally identifiable information collected?			
	Yes	No	Response Count
Removes Personal Information	89.5% (17)	10.5% (2)	19
Gives Individuals A Choice	47.4% (9)	52.6% (10)	19
		<i>answered question</i>	20
		<i>skipped question</i>	71

44. Please describe any other measures undertaken by your business to: (1) safeguard collection, use, or distribution of personally identifiable information (2) eliminate personally identifiable data collected in the course of operating transportation technologies.		
		Response Count
		10
	<i>answered question</i>	10
	<i>skipped question</i>	81

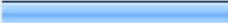
45. For all transportation technologies identified in earlier responses, please indicate if your business discloses or will disclose to others:

	Yes	No	Response Count
The type of data collected:	78.6% (22)	21.4% (6)	28
How the data is collected:	82.1% (23)	17.9% (5)	28
The purpose for collecting the data:	82.1% (23)	17.9% (5)	28
How is the data used:	75.0% (21)	25.0% (7)	28
How the data is processed:	60.7% (17)	39.3% (11)	28
Who has access to the data:	67.9% (19)	35.7% (10)	28
How the data is stored:	67.9% (19)	32.1% (9)	28
How the data is distributed:	71.4% (20)	32.1% (9)	28
How long the data is retained:	69.2% (18)	30.8% (8)	26
	<i>answered question</i>		28
	<i>skipped question</i>		63

46. Does or will your business provide an opportunity for individuals or users of the transportation technologies identified in earlier questions to access and correct personal information?

		Response Percent	Response Count
Yes		34.6%	9
No		65.4%	17
	<i>answered question</i>		26
	<i>skipped question</i>		65

47. For all transportation technologies please indicate whether your organization will provide an opportunity for individuals to opt out of the collection of traveler information?

		Response Percent	Response Count
Yes		54.2%	13
No		45.8%	11
<i>answered question</i>			24
<i>skipped question</i>			67

48. Does your business have or are you developing any protocol, internal policies, or procedures for the collection, use, distribution, retention, or disposal of personally identifiable information collected in the course of operating and maintaining transportation technology systems?

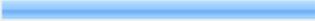
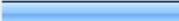
		Response Percent	Response Count
Yes		37.5%	9
No		62.5%	15
<i>answered question</i>			24
<i>skipped question</i>			67

49. If YES, please briefly describe the protocol, policies and/or procedures.

	Response Count
	8
<i>answered question</i>	8
<i>skipped question</i>	83

Survey Response Summary

50. Please identify the number and job title of employees within your business who work on managing personally identifiable information.		
		Response Count
		17
		<i>answered question</i>
		17
		<i>skipped question</i>
		74

51. Do you disclose any change in privacy policies?			
		Response Percent	Response Count
Yes		63.6%	14
No		36.4%	8
		<i>answered question</i>	22
		<i>skipped question</i>	69

52. Could you describe the nature of technologies your company is involved with.		
		Response Count
		20
		<i>answered question</i>
		20
		<i>skipped question</i>
		71

53. Could you describe any new or emerging technologies or application that might be relevant to privacy in the future.		
		Response Count
		14
		<i>answered question</i>
		14
		<i>skipped question</i>
		77

PART 4
Open-Ended Responses to Survey Questions

This appendix contains additional observations from the survey data as well as the responses given to the open-ended questions.

Question 1: The largest number of responses was from organizations that were involved with ATMS.

Question 2: Responses to this question suggested that ITSA members who participated in this survey operate in a wide variety of functions or IT areas, with the majority working in infrastructure applications.

Question 4: Responses seem to indicate the organizations in the category of MCO organizations are concerned with both vehicle and infrastructure technologies.

Question 6: The responses here suggest that the majority of the respondents to this category are involved with traffic toll and fare collection and enforcement.

Question 8: The data here suggests respondents are involved with at least one of the 511 systems: highway advisory radio, highway news, or congestion information.

Question 10: The majority who responded here seem to be in vehicle tracking technologies

Question 11: Around 1/3 of the ITSA members who responded are involved in EM in some form.

Question 16: The responses here suggest that an overwhelming number of ITSA members who responded to this survey are research oriented or have a research component as part of their organizations.

Question 17: Despite the high degree of privacy concerns, the majority of the respondents indicated that they do not collect personal data. It might be significant that 41 of the 91 respondents skipped or chose not to answer this question.

Question 18: While a small number of respondents report that they collect personal data (over 19), a slightly larger number acknowledge they do collect vehicle information.

Question 19: The collection of financial information seems to be in the same range as the collections of personal information.

Question 21: The responses to this question suggest that while ITSA members might not be collecting personal and vehicle data, many more collect it passively by utilizing video and photo technologies from which personal data can be derived.

Question 23: Respondents preferred wireless technologies for data collection and tracking. This seems to be in line with Question 20 which indicates a preference for the use of passive technologies.

Question 25: Responses to this question tend to indicate that there is some amount of data creep since 8 respondents do combine the data they collect with other data.

Questions 26-29: Questions regarding the external use of data, other than providing the service, show some inconsistency. Fifteen respondents report the data is used for other purposes, 17 respondents reported 3rd party requests, but only 9 honored those requests. However, in question 29, the respondents reported that a total of 13 requests were honored split between public and private entities.

Question 31: A high % percentage of respondents reported that the data had value to a range of public and private purposes.

Questions 33 -34: Most data is stored on a centralized computer system and 15 respondents combine stored data.

Question 37-39: See open-ended question below for insight.

Question 43: Virtually all entities that collect personal information will remove that information or permit individuals to have a choice whether it is collected or not.

Question 46: Entities that collect personal information do not find a need to correct the data.

Question 47-48: There appears to still be a need to develop policies to deal with personal information on an industry by industry basis.

Open-Ended Survey Responses

Question 23: What types of technology are used to collect data? (Please check all appropriate boxes.) Duplicate answers were eliminated, and some were edited for clarity.

1. Wireless road sensors that provide anonymous vehicle re-id?
2. Cellular data, 3G
3. On-board DAS with cellular download
4. Radar, radio, and cell phone modems
5. Cellular/Radio
6. All the above (if available)
7. Video camera, electronic toll collection system is currently out to bid implemented
8. Wired Ethernet
9. Roadway Sensors
10. Microwave Radar
11. Private networks, agency land-line infrastructure
12. Web site, user entry, leased telephone lines
13. Radar

14. CDMA, GPRS, Sp.Sp. Frequency Hopping
15. Laser, video and camera
16. Radar; GPRS
17. FCC-assigned mobile and microwave radio frequencies

Question 30: If yes, how are they using the data?

1. Traffic companies want to put data on web sites
2. Planning
3. Evidence in court cases
4. University Research
5. Information only
6. Facilities planning; where to locate branch locations based on traffic considerations

Question 32: How is data processed?

1. OCR for toll amount debit or enforcement
2. Through a server in the TMC
3. Archived through central software
4. By hand
5. Multiple records are integrated for certain parameters
6. On site
7. Collected from field devices and processed/stored centrally
8. Credit card transactions to purchase passes are processed by bank
9. On-board computer
10. Proprietary Software Platform
11. Various software including customer supplied software
12. On a central server where it is collated and tallied.
13. Speed data is collected once a minute. No personal information of any kind.

Question 36: Who within your organization has access to the data?

1. Engineers
2. Operations
3. Administrators
4. Project Manager and Project Operations Staff
5. We give specific permission to have access to the data
6. Executive level
7. We do not collect personal data; all traffic detection and incident information is placed on website & ftp site (updated at least every minute) ?
8. Anyone with business need.
9. Access is limited to a need to know and customers
10. Only authorized users
11. Sales and technical staff
12. Risk Management, Transit Operations, Safety
13. Need to know basis
14. System Administrators for all data. CSR's for specific authorized data.
15. Researchers

16. No one.
17. Project Managers and Contractors
18. System Operators
19. Traffic Engineering IT staff
20. Only the department manager and developers.
21. Customers
22. Everyone

Question 39: How and to whom is data distributed?

1. Goes to director, then to FTP site to be downloaded
2. Public request
3. Regional Archive Data Server
4. Annual Reports
5. Client base data (toll authorities)
6. With sponsor approval (DOE, DOT, etc.)
7. Turnpike Commission, Traffic Operations Center, Law Enforcement
8. Customer only
9. Anybody who wishes to have it via our website and/or ftp site
10. Public Information by law - distributed on request. Personal confidential data would be omitted if it were collected.
11. Customers/Web
12. We only distribute data through our end customer.
13. Need to know
14. Only for USDOT project funding data collection
15. Traffic data is provided to Information Service Providers and researchers
16. Customer determines
17. Authorized state & weather service contractors and employees
18. Public data request
19. Government Agencies; traffic information providers; changeable message signs; TV/radio

Question 40: What technical security mechanisms are in place to prevent tampering with data?

Other (please specify)

1. The data is all anonymous
2. No personal data is available outside the DMZ
3. Lifecycle security needs assessed and appropriate controls designed. Wherever possible we do not collect confidential information, e.g., credit cards are processed - but we do not store the data.
4. Optional VPN or other levels of security used to access data sources
5. Read only

Question 41: What non non-technical security mechanisms are in place to prevent tampering with data? Other (please specify)

1. We give them a test trial with our data
2. Data is accessed by one individual only. No one else has access.

3. Responsibility of our customer within the State Agency
4. Read only

Question 42: For how long is data retained?

1. 1 year
2. Depends
3. Don't know
4. Not sure
5. Varies per agency policy
6. Customer choice
7. Up to five (5) years
8. Most of this data is retained indefinitely for analysis purposes.
9. Forever
10. Varies with customer requirements and contract
11. As long as needed
12. Unknown
13. Length of project
14. Varies - traffic speed data is discarded every 24 hours
15. ATMS data is the only thing that is retained
16. Backed up onto CD on a yearly basis
17. Customer determined
18. It varies based upon data type & customer.
19. Up to the customer
20. 10 years
21. 2 years

Question 44: Please describe any other measures undertaken by your business to: (1) safeguard collection, use, or distribution of personally identifiable information, (2) eliminate personally identifiable data collected in the course of operating transportation technologies.

1. We cannot have PII information on our computers. There is software available to check computers
2. Design to avoid collecting it.
3. No personal data collected at this time.
4. Video data does not have personally identifiable information
5. We have privacy policies and regularly assess our compliance with these policies.
6. Up to customer

Question 48: Does your business have or are you developing any protocol, internal policies, or procedures for the collection, use, distribution, retention, or disposal of personally identifiable information collected in the course of operating and maintaining transportation technology systems?

Question 49: If YES, please briefly describe the protocol, policies and/or procedures.

1. Regional Protocols in place

2. The only personal item we acquire is a person's telephone number and we scrub the final four digits before releasing
3. If you have to do it, authorized access, encryption in storage and transmission, redaction required.
4. Under development
5. See privacy policy at traffic.511.org
6. Freedom of Information act

Question 50: Please identify the number and job title of employees within your business who work on managing personally identifiable information.

1. Our communications equipment systems enable the collection of data by the agency.
2. 1-IT Manager
3. 3 PIO
4. Numerous Managers/Directors
5. 2-3 Senior Planners
6. Customers use the data they collect
7. All IT staff

Question 52: Could you describe the nature of technologies your company is involved with.

1. Tolling & toll processing, enforcement
2. Government traffic data
3. Secure managed fiber network
4. Collection of performance measures for technologies
5. Wireless Broadband Communications at the 4.9GHz frequency for Transit, Utilities and Public Safety use.
6. Wireless video surveillance of roadways for traffic management, incident management and response.
7. Detection, CCTV, 511, Internet display of incidents
8. Information Management
9. Traffic control, traffic management systems, vehicle detection system, and vehicle data collection systems
10. Digital video on transit, electronic fare payment, automated passenger counters, web based trip planner
11. ITS, GPS/AVL
12. DSRC, safety applications
13. Transit ITS technologies
14. Microwave Radar Systems
15. Personalized traveler information
16. Telematics/Telediagnosics
17. Photographic speed enforcement
18. We measure traffic speed and disseminate current traffic conditions to the public
19. Intelligent railroad systems

Question 53: Could you describe any new or emerging technologies or application that might be relevant to privacy in the future.

1. VII e-payment, Probe

Open-Ended Responses

2. The wireless network may enable the collection of sensor data from vehicles along the roadway that may include personal data about the driver or the vehicle.
3. Vehicle tracking in order to assess travel times; subscription services for information
4. We have introduced a security product that can secure access to both data sources and field equipment via a hardware device signature that is unique to each physical device. This can be used to prevent unauthorized access to data or field device.
5. DSRC
6. VII/IntelliDrive
7. Complete solution speed enforcement
8. CCTV
9. Cell phone tracking, toll tag tracking, cell phone carrier signal tracking all create personal privacy issues