

How Two Traditions of Privacy Defenses in Image Capture Technology Inform the Debate over Drones

DEREK LARSON & PATRICK S. ROBERTS*

CONTENTS

I.	TWO TRADITIONS OF PRIVACY CLAIMS.....	469
	A. Dignity-Based Privacy Arguments	469
	B. Technical Privacy Arguments.....	471
II.	PRIVACY CONCERNS AND IMAGE CAPTURE TECHNOLOGY	474
	A. Cameras.....	475
	B. Camera Phones.....	478
	C. Advanced Imaging (Thermal Imaging).....	482
	D. Drones	486
III.	DRONES AND THE NEED FOR AN INTEGRATED APPROACH	492

Abstract: Innovations in image capture technology create new versions of long-standing concerns about privacy, with the debate over unmanned aerial vehicles, known in the popular media as drones, as the latest example. The history of privacy claims in image capture technology weaves together arguments about technically-oriented harms and arguments about human dignity. Claims for defending privacy against intrusions from cameras, camera phones, and thermal imaging can be deployed in new forms in defenses of privacy against drones. This article ends with a caution about unintended consequences of regulating privacy, and of attempting to avoid regulation altogether.

Technological innovation has a fraught relationship with privacy, with the most pessimistic observers assuming that the sufficient

advance of the former inexorably leads to the destruction of the latter.¹ Even the most ardent believer in the power of privacy rights recognizes trade-offs between privacy and new technology: online shopping offers tremendous convenience at the cost of the shopper's personal data; the National Security Agency collects phone records to protect Americans' interests, creating an unprecedented store of information about citizens' activities. Furthermore, the increasingly sophisticated biometrics protecting sensitive data create their own stores of highly personal information.²

Drones, or unmanned aerial systems (UAS) as they are known in the industry, are at the leading edge of the privacy debate, with industry working with the American Civil Liberties Union or more specialized groups such as the Stop LAPD Spying Coalition to develop regulations intended to further technological development and make people's lives better, not worse.³ Privacy-oriented technology groups, such as the Electronic Privacy Information Center, have also taken the fight to government agencies, petitioning to initiate rulemaking "to address the threat to privacy and civil liberties that will result from the deployment of aerial drones within the United States."⁴ The Federal Aviation Administration (FAA) predicts there could be 15,000 civilian drones operating in U.S. airspace by 2020, though this will depend

* The authors would like to thank the editors and anonymous reviewer for comments, as well as Craig Woolsey and two Virginia Tech institutes, the Institute for Critical Technologies and Applied Science, and the Institute for Society, Culture, and Environment.

¹ Charles Nesson, *Threats to Privacy*, 68 SOC. RES. 105, 105 (2001).

² See generally Ann Cavoukian, Michelle Chibba & Alex Stoianov, *Advances in Biometric Encryption: Taking Privacy by Design from Academic Research to Deployment*, 29 REV. OF POL'Y RES. 37 (2012).

³ See generally Robert Heverly, *The State of Drones: State Authority to Regulate Drones*, 8 ALB. GOV'T L. REV. 29 (2015). A drone is an unmanned aerial vehicle with autonomous flight capabilities. A remote-piloted aircraft is not necessarily a drone. This is an important ethical and technological distinction, as manually remotely piloted aircraft are under human control, whereas fully autonomous drones may carry out their mission according to a predetermined algorithm.

⁴ Petition from the Electronic Privacy Information Center to Michael P Huerta, Acting Adm'r, U.S. Fed. Aviation Admin. (Feb. 24, 2012), <https://epic.org/privacy/drones/FAA-553e-Petition-03-08-12.pdf> [<https://perma.cc/4PBU-WYLU>].

both on whether government adopts UAS-friendly regulations and, ultimately, on a skeptical public's acceptance of the technology.⁵

Drone technology is poised to proliferate, and policy can influence technological innovation to only a limited extent. After Pandora's box is opened, it is too late. One of the few tools that policymakers have at their disposal in this regard is a robust, coherent, and precisely defined concept of privacy.⁶ The history of image capture technology shows that privacy norms can be used to shape how technology develops and what protections should accompany new technology. In fact, some scholars argue the privacy issues raised by the proliferation of drones may bring needed updates to how society approaches privacy and its legal protection with regards to other technologies.⁷

Drone technology is a contemporary phenomenon, but concern about the use and proliferation of image capture technology is not. This article situates the case of drones in the historical context of image capture technology in order to illuminate the tensions between technological development and privacy, and between different conceptions of privacy. There are two overlapping traditions and ways of arguing that provide resources for addressing claims about privacy rights in image capture technology, specifically cameras, camera phones, advanced imaging technologies, and drones. The first tradition views privacy in a more technical sense as the sum of thousands of specific precedents on particular legal issues, no different than many other mundane disputes. The second tradition makes claims for privacy as a broad-based right rooted in the lofty notion of human dignity. The first tradition relies on rules and regulations, while the second appeals more often to principled notions of what is good for human flourishing.⁸

Technical approaches to regulating privacy have proven useful because analogies can be made to earlier technologies. Scholars claim that existing torts provide tools for resolving many disputes over

⁵ FED. AVIATION ADMIN., AEROSPACE FORECAST FISCAL YEARS 2010-2030 (2010), https://www.faa.gov/data_research/aviation/aerospace_forecasts/2010-2030/media/2010%20Forecast%20Doc.pdf [<https://perma.cc/EGE4-24T9>].

⁶ See generally Daniel Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087 (2002).

⁷ M. Ryan Calo, *The Drone as Privacy Catalyst*, 64 STAN. L. REV. ONLINE 29, 29 (2011).

⁸ Terry L. Cooper, *Hierarchy, Virtue, and the Practice of Public Administration: A Perspective for Normative Ethics*, 47 PUB. ADMIN. REV. 320 (1987); Lewis C. Mainzer, *Vulgar Ethics for Public Administration*, 23 ADMIN. & SOC'Y 3 (1991).

privacy and drones, but that existing torts must be adapted to prevailing norms.⁹ The norms, however, are often articulated in terms of respect for human dignity, privacy, and personal property – claims to principles rather than just technical protections. At a deeper level, technical approaches depend on normative ideals.

The utility of dignity-based approaches has been limited when their arguments veer too far in the direction of first principles. Interest groups and legislators can appeal to an absolute right to privacy and control of one's surroundings, but the courts operate through addressing harms. Calo has argued that the lack of a mental model for privacy harm limits the appeal of privacy claims in the courts and public debates because there is no paradigmatic story about what constitutes a privacy violation when it comes to drones.¹⁰ Advocates for limits on the privacy harms that drones may cause lack their September 11 or Hurricane Katrina, even as drone technology ignites visceral fear.¹¹

This article shows how both dignity-based and technical approaches are woven throughout the history of image capture technology. Arguments about defending privacy against intrusions from cameras, camera phones, and thermal imaging can be deployed in defenses of privacy in the case of drones. The article ends with a caution about the unintended consequences of overregulating privacy or avoiding regulation altogether.

⁹ Benjamin Mathews, *Potential Tort Liability for Personal Use of Drone Aircraft*, 46 ST. MARY'S L.J. 573 (2015).

¹⁰ Calo, *supra* note 7.

¹¹ Drone technology may have some of the character of what psychologists call a "dread risk" since there is a perceived lack of control, the fear of catastrophic and fatal consequences, and inequitable risks and benefits. The public (as opposed to experts) tends to look past cost/benefit data and favor regulation of dread risks more than it does with other kinds of risks. See Baruch Fischhoff, Stephen Watson & Chris Hope, *Defining Risk*, 17 POL'Y SCI. 123, 129 (1984); Gerd Gigerenzer, *Dread Risk, September 11, and Fatal Traffic Accidents*, 15 PSYCHOL. SCI. 286, 286 (2004); Paul Slovic & Ellen Peters, *Risk Perception and Affect*, 15 CURRENT DIRECTIONS PSYCHOL. SCI. 322, 322-23 (2006).

I. TWO TRADITIONS OF PRIVACY CLAIMS

A. Dignity-Based Privacy Arguments

Though it reflects a general claim about what is owed to fellow human beings, the dignity-centric conception of privacy grew out of specific grievances. American law's foundational work on privacy, Samuel Warren and Louis Brandeis' *The Right to Privacy*, was written partially in response to the emerging technology of its day: personal photography.¹² Warren and Brandeis had become alarmed by the threats to privacy posed by the combination of camera technology and yellow journalism.¹³ In response, the jurists examined existing legal precedent and found an underlying understanding that privacy is an inherent human right. Their argument identifies a common thread of privacy protection in the legal precedents established by slander and libel, intellectual property rights, violation of trust and contract, and trade secret law. Warren and Brandeis explained that in each of these areas there were obvious gaps that had been bridged by an understanding that people possess not just a desire for privacy, but a legal expectation of it.¹⁴

As an article and not a legal judgment, *The Right to Privacy* could not confer legal authority upon Warren and Brandeis' views. However, the ideas set forth in the essay would find traction in court cases across the country, slowly building its own legal precedent.¹⁵ After Brandeis assumed a seat on the Supreme Court in 1916, his judicial philosophy carried even greater weight. Though written in dissent, Brandeis' opinion in *Olmstead v. United States*¹⁶ was the foundation for much of the right to privacy doctrine that followed. The government argued in *Olmstead* that the Fourth Amendment only protected Americans from physical intrusions, meaning that the wiretap conducted without a warrant against Olmstead was legal.

¹² See generally Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

¹³ See generally Neil Richards & Daniel Solove, *Prosser's Privacy Law: A Mixed Legacy*, 98 CAL. L. REV. 1887 (2010).

¹⁴ Warren & Brandeis, *supra* note 12.

¹⁵ William Prosser, *Privacy*, 48 CAL. L. REV. 383, 386 (1960).

¹⁶ *Olmstead v. United States*, 277 U.S. 438 (1928) (Brandeis, J., dissenting).

While the majority found in favor of the government and the legality of the “warrantless wiretap,” Brandeis argued that the search was illegal. He wrote that since the adoption of the Bill of Rights, “Subtler and more far-reaching means of invading privacy have become available to the Government. Discovery and invention have made it possible for the Government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet.”¹⁷ Brandeis argued that technology would increase the government’s ability to intrude in the lives of citizens, and that the Constitution was surely able to protect its citizens from such seeming eventualities. “Can it be that the Constitution affords no protection against such invasions of individual security?”¹⁸

Though most famously espoused by Warren and Brandeis, dignity-based arguments about privacy became part of a rich tradition in the law. Edward Bloustein, a prominent legal scholar in the 1960’s and 1970’s, was an outspoken believer in Warren and Brandeis’ conception, equating violations of privacy to physical assaults on one’s person.¹⁹ Frequently sparring with those in favor of privacy in the tradition we describe as “technical,” he argued that the public’s concern in protecting privacy, both generally and in the case of emerging electronic monitoring, was through the “preservation of the individual’s dignity.”²⁰ Others would follow, emphasizing privacy’s fundamental moral dimensions, rooted in natural law and equal respect within a shared community.²¹ While some scholars argue that dignity-based privacy is a vague mishmash of legal theories, most scholars of the dignity-based tradition maintain the opposite viewpoint: that dignity-based privacy is a coherent-if difficult and multifaceted-concept rooted in the belief that individuals have a right to control their external exposure and limit others’ access to their

¹⁷ *Id.* at 473 (Brandeis, J., dissenting).

¹⁸ *Id.* at 474 (Brandeis, J., dissenting).

¹⁹ Edward Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. REV. 962, 1002 (1964).

²⁰ *Id.* at 1007.

²¹ Robert Post, *Rereading Warren and Brandeis: Privacy, Property, and Appropriation*, 41 CASE W. L. REV. 647, 651 (1964); see generally Lisa Nelson, *Privacy and Technology: Reconsidering a Crucial Public Policy Debate in the Post September 11 Era*, 64 PUB. ADMIN. REV. 259 (2004).

personal information.²² Loss of control over one's personal information results in a loss of the individuality necessary for the establishment of one's very personhood.²³

This conception of privacy is not a universally accepted notion. Many scholars note that such an understanding of privacy has an important cultural component that can impact societal expectations of what such a right entails.²⁴ If what dignity requires is not universal, the argument goes, then why rely on it as a foundation for privacy claims? Demonstrable harms rather than appeals to dignity make for a better case for protections, according to these critics. Furthermore, the lack of specificity contained in a broad dignity-based conception of privacy could lead to gaps in privacy protection or confusion when privacy intersects with other rights, such as freedom of expression. For these reasons, many practicing lawyers have framed their privacy claims in a more technical and specific manner, drawing on precedent and rulings about other technologies.

B. Technical Privacy Arguments

Much as Warren and Brandeis were the first to strongly and clearly articulate a right to privacy that incorporates a notion of human dignity, William Prosser was the most successful (if not first) advocate for a conception of privacy based less on philosophical and ethical grounds than on widely accepted legal concepts such as property rights and protection against slander. Prosser was the author of an influential article, titled simply *Privacy*, in which he examined the case law that had emerged since Warren and Brandeis' article was

²² See generally Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421 (1980); Hyman Gross, *The Concept of Privacy*, 42 N.Y.U. L. REV. 34 (1967); *Olmstead v. United States*, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting).

²³ Jonathan Kahn, *Privacy as a Legal Principle of Identity Maintenance*, 33 SETON HALL L. REV. 371, 378 (2003).

²⁴ See generally Tom Gerety, *Redefining Privacy*, 12 HARV. C.R.-C.L. L. REV. 233 (1977); Christopher Slogobin & Joseph Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at Understandings Recognized and Permitted by Society*, 42 DUKE L.J. 727 (1993); Shaun Spencer, *Reasonable Expectations and the Erosion of Privacy*, 39 SAN DIEGO L. REV. 843 (2002); Hank Jenkins-Smith & Kerry Herron, *Rock and a Hard Place: Public Willingness to Trade Civil Rights and Liberties for Greater Security*, 37 POL. & POL'Y 1095 (2009); John Gardner, *The Many Faces of the Reasonable Person*, 131 L. Q. REV. 563 (2015); Nelson, *supra* note 21.

published 70 years earlier. Whereas Warren and Brandeis and the scholars who followed them saw legal precedent a common thread based on respect for human dignity, Prosser saw a hodgepodge of legal concepts that fell into four baskets: intrusion upon one's seclusion, solitude, or personal business; public disclosure of private information; falsehood that leads to a negative public image; and use of a person's name or likeness for gain without approval.²⁵ Though the essay begins by paying homage to Warren and Brandeis, it can also be read as a refutation of the argument that privacy is rooted in natural rights.²⁶ Warren and Brandeis also referenced torts, but they argued that there is an underlying normative principle of privacy. In contrast, Prosser understood privacy rights as a collection of legal doctrines that are "tied together by the common name," but "otherwise have almost nothing in common".²⁷ This formed the basis of the technical conception of privacy.

Prosser's conception of privacy in the *Restatement of Torts, Second* influenced a generation of lawyers. His work became the source of legal authority for a technical conception of privacy, which his supporters have credited with organizing and legitimizing privacy as a legal concept, specifically negative-defined privacy, which defines privacy not in terms of what it is, but of what is not.²⁸ The technical approach, which is similar to what other authors have conceived of as "formal"²⁹ or "thin"³⁰ conceptions of legal understanding, offers an undeniable convenience: as objectionable actions take place, the injured parties can take civil action against their injurers. The actions or misdeeds in question can be linked to a specific type of legally validated injury and judged against similar case law, a process that seems to offer more concrete and actionable legal grounding than the

²⁵ Prosser, *supra* note 15, at 389.

²⁶ Bloustein, *supra* note 19, at 965.

²⁷ Prosser, *supra* note 15, at 389.

²⁸ Richards & Solove, *supra* note 13, at 1889.

²⁹ Paul Craig, *Formal and Substantive Conceptions of the Rule of Law: An Analytical Framework*, PUB. L. 467 (1997).

³⁰ Jesús Fernández-Villaverde, *Magna Carta, the Rule of Law, and the Limits of Government* (U. of Pa., Working Paper No. 15-035, 2015), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2676184 [<https://perma.cc/QD43-EX2A>].

more philosophical arguments of Warren and Brandeis' strict adherents. This same dynamic makes Prosser's negative conception popular among legislators and regulators. Rather than wrestle with questions of natural law or innate human rights, cases can be decided and laws or regulations can be put in place to remove the immediate threat to privacy caused by objectionable actions or practices.

Though the technical conception of privacy as defined by Prosser is newer than Warren and Brandeis' dignity-based conception, the tradition of examining privacy rights by how they fit into other legal traditions predates the latter model. As we will see later in this assessment, Warren and Brandeis' argument was originally seen by some jurists as unworkable because it failed to fit such violations into existing tort structures.³¹ Later scholars would examine the work of Warren and Brandeis or Bloustein and conclude that dignity simply did not offer enough specificity to serve as the foundation of privacy law.³² Both technical and dignity-based scholars came to define themselves in part by their reaction to the other tradition.

Though they became distinct schools of thought, the legal tools of both traditions overlap. Tort law is central to the Prosserian technical understanding of privacy, and Warren and Brandeis based their argument on existing, widely-accepted tort principles. Later champions of dignity-based privacy held torts as a central remedy to privacy violations.³³ In the Warren and Brandeis approach, torts are the vehicle for determining, in a context specific to the individual and the privacy violation, whether a specific incident violates the dignity-based conception of human rights.³⁴ This stands in contrast to the "technical" tradition, which sees torts not as a means of testing privacy violations but as the real force behind the legal concept of privacy.

It views dignity-based conceptions with skepticism, having the baggage of natural law, absolutism, and mysticism. In reality, arguments from these two traditions are mixed in the history of debates over image-capture technology.

³¹ Irwin Kramer, *The Birth of Privacy Law: A Century Since Warren and Brandeis*, 39 CATH. U. L. REV. 703, 716 (1989).

³² Gavison, *supra* note 22, at 438.

³³ See generally Edward Bloustein, *Privacy, Tort Law, and the Constitution: Is Warren and Brandeis' Tort Petty and Unconstitutional as Well?*, 46 Tex. L. Rev. 611 (1968).

³⁴ Warren & Brandeis, *supra* note 12, at 215; *id.* at 615.

Characteristics of Privacy	
Dignity-Based Privacy	Looks for meaning behind case law
	Flexible
	Not necessarily tied to specific legal provisions
	Violations tied to violation of personhood
Technically-Oriented Privacy	Specifically prohibits the most egregious behaviors
	Seeks to fit privacy inside other tort traditions
	Privacy as a legal right, not a moral one

II. PRIVACY CONCERNS AND IMAGE CAPTURE TECHNOLOGY

Both dignity-based and technically-oriented conceptions of privacy have virtues, but their differences become important as the competing conceptions are applied to new and emerging technology such as drones. Where data sources can be used to create a mosaic of personal information,³⁵ such considerations take on new urgency. To better explore the impact of these differing privacy traditions on the debate over UAS, we examine key junctures in the history of image capture technology and consider the strengths and weaknesses of each conception. The two traditions do not lead into a distinct Goldilocks-style third way between the porridge that is too hot and the porridge that is too cold. Rather, the history of image capture technology shows that arguments from both traditions can be employed for specific purposes – technical approaches to identify analogies for harms from earlier technology, and dignity-based approaches to appeal to the visceral reaction that many people have to defend human autonomy against drone spying.

³⁵ See generally Anne Washington, *Government Information Policy in the Era of Big Data*, 31 REV. OF POL'Y RES. 319 (2014).

A. Cameras

When daguerreotypes first emerged in the mid-19th century, the widespread proliferation of photography was limited by its costly, cumbersome, and temperamental nature. Early cameras required their subjects to remain still for the duration of a lengthy chemical process, limiting their utility. Even as camera technology improved, the cost limited it to the realm of professionals and the wealthy. This changed dramatically with the advent of the photographic process. Personal cameras democratized image capture, affording everyday citizens the ability to take pictures of the world around them. However, while this technology created new possibilities for many, for others it was the beginning of a frightening new affront to privacy. Beginning with the press' fascination with the lives of the wealthy and influential, this technology came to form the backdrop against which Warren and Brandeis' treatise was born. "Instantaneous photographs and newspaper enterprises have invaded the sacred precincts of private and domestic life," they proclaimed, "and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops."³⁶ The notion that people have an innate right to keep personal matters private reverberated among many who were concerned that technology such as the camera would continue to diminish any sense of privacy they once possessed.

Though the idea of a right to privacy gained some public acclaim, the legal precedent that emerged contradicted the assertions of Warren and Brandeis. In 1902, the New York Court of Appeals ruled in *Roberson v. Rochester Folding Box Co.*³⁷ that Roberson, who claimed to have suffered duress from the unauthorized use of her image by an advertising company for a flour company, was not entitled to collect damages based on a violation of her privacy. The Court viewed the idea that a person could have such control over his or her image as unworkable; it added that "the so-called 'right of privacy' has not as yet found an abiding place in our jurisprudence, and, as we view it, the doctrine cannot now be incorporated without doing violence to settled principles of law by which the profession and

³⁶ Warren & Brandeis, *supra* note 12, at 195.

³⁷ *Roberson v. Rochester Folding Box Co.*, 64 N.E. 442, 447 (1902).

the public have long been guided.”³⁸ Tremendous public outcry followed the ruling, prompting one of the judges on the appeals panel to issue an unprecedented public defense of the court’s ruling.³⁹ Spurred on by press scrutiny of the ruling, public pressure for a legislative fix mounted. The New York State Legislature eventually passed a law making it illegal to use a person’s likeness for profit or advertising without consent.⁴⁰

At the heart of *Roberson* was the question of one’s ownership over his or her own image, a concept central to the debate over photography and the right to privacy. While the Court’s ruling itself represented a step backward for the ideas espoused by Warren and Brandeis, the resulting legislative action demonstrated the power of their argument for a fundamental human right to privacy.⁴¹ Paradoxically, the resulting law⁴² followed the technical model that later became identified with Prosser, carefully detailing what constituted a violation of privacy and providing avenues for recourse if necessary. The New York law would be at the heart of numerous lawsuits, eventually being confirmed as constitutional, and similar statutes were eventually enacted in state legislatures across the country.⁴³ The right to control the use of one’s image with regards to its use for profitmaking is now generally referred to as the right to publicity and remains an issue addressed at the state rather than federal level.

While *Roberson* dealt with the issue of one’s image for the purpose of profit, other questions about limits of privacy arose over time. Over half a century later after the legal concept of a right to privacy had

³⁸ *Id.*

³⁹ Benjamin E. Bratman, *Brandeis and Warren’s The Right to Privacy and the Birth of the Right to Privacy*, 69 TENN. L. REV. 623, 641 (2002); Denis O’Brien, *Right of Privacy*, 2 COLUM. L. REV. 437, 438 (1902) (Much as Brandeis and Warren had laid out their conception of the right to privacy in a law journal, Judge Denis O’Brien similarly turned to one for his defense of the ruling and condemnation of the “erroneous, not to say extravagant, version of the reasons upon which the decision rests and of the consequences to follow from it.”).

⁴⁰ Bratman, *supra* note 39.

⁴¹ *See id.*

⁴² N.Y. CIV. RIGHTS LAW §§ 50-51 (1909).

⁴³ Prosser, *supra* note 15, at 385-86.

become widely accepted, *Daily Times Democrat v. Graham*⁴⁴ raised questions as to how far the right extended and how it interacted with other rights. In *Daily Times Democrat*, a woman and her son were visiting a fair when a gust of wind lifted her skirt up in public view. A photographer took a picture of the unfortunate event, and a local publication printed it.⁴⁵ Humiliated, the woman sued the newspaper, which claimed that not only did it have the right to print the picture under the first amendment, but the woman had no claim to privacy because the incident happened in a public setting.⁴⁶ The Alabama Supreme Court sided with Graham, finding it absurd to claim that a person “forfeits her right of privacy merely because she happened at the moment to be part of a public scene.”⁴⁷

Daily Times Democrat marked a significant step forward for the concept of an affirmative right to privacy in the tradition of Warren and Brandeis.⁴⁸ Whereas the courts had found in *Roberson* that no such right existed and had ruled, instead, in favor of “established principles of law,” *Daily Times Democrat* saw the right to privacy not only trump the freedom of the press, but expand to include public settings.⁴⁹ It is particularly on this second issue that privacy as a right based in human dignity proved to be decisive. The lawyers for the newspaper employed a narrow, technical argument in defending the publication of Graham’s picture. However, the Alabama Supreme Court ruled against such a limited protection of privacy, finding privacy to extend beyond one’s location to one’s dignity as a human being.

Questions regarding cameras and their impact on privacy did not end with *Daily Times Democrat*. As camera technology has continued to evolve, the concerns first laid out by Warren and Brandeis have

⁴⁴ See *Daily Times Democrat v. Graham*, 162 So. 2d 474 (1964).

⁴⁵ *Id.* at 476.

⁴⁶ *Id.* at 478.

⁴⁷ *Id.*

⁴⁸ Richard C. Turkington, *Legacy of the Warren and Brandeis Article: The Emerging Unencumbered Constitutional Right to Informational Privacy*, 10 N. ILL. U. L. REV. 479, 490 (1989-1990).

⁴⁹ Joseph Elford, *Trafficking in Stolen Information: A “Hierarchy of Rights” Approach to the Private Facts Tort*, 105 YALE L.J. 727, 754 (1995-1996).

gained new prominence. The rise of security cameras and closed circuit televisions drew concerns that privacy was doomed to disappear as an inevitable casualty of modernization.⁵⁰ Similar predictions were made with the introduction of digital cameras, which combine the potential privacy threat of cameras with the ability to quickly and easily share images online.⁵¹ However, another technology would truly test the limits of privacy protections because of its ubiquity and technological convergence: the camera phone.

B. Camera Phones

In 2002, camera phones became widely available in the United States.⁵² At the time of the camera phone's arrival, both cellular phones and cameras were widely used, but they existed as separate and distinct devices. This meant that, while cellular phones were often carried everyday by their users, cameras were not necessarily always at hand. Additionally, while dissemination of camera images had become easier with the introduction of digital cameras, such technology still required a user to connect the device to a computer in order to view and distribute the captured images. Camera phones offered their users the ability to take pictures on a device they already carried everywhere, making photography more convenient, and eventually the phones began to offer the ability to post pictures instantly to online platforms. By 2012, 85 percent of American adults owned a cell phone, and 82 percent of those owners used their phones to take pictures.⁵³ Scholars describe the tendency of technology to evolve to perform similar tasks as "convergence."⁵⁴ The idea has

⁵⁰ See Christopher S. Milligan, *Facial Recognition Technology, Video Surveillance, and Privacy*, 9 CAL. INTERDISC. L.J. 295 (1999-2000).

⁵¹ Jim B. Coleman, *Digital Photography and the Internet, Rethinking Privacy Law*, 13 J. INTEL. PROP. L. 205, 221 (2005-2006).

⁵² Anita Hamilton, *Cooler Inventions-Camera Phones*, TIME (Nov. 27, 2003), <http://content.time.com/time/magazine/article/0,9171,1006201,00.html> [<https://perma.cc/Z4BS-7GJC>].

⁵³ Maeve Duggan & Lee Rainie, *Cell Phone Activities 2012*, PEW RES. CTR. (Nov. 25, 2012), <http://www.pewinternet.org/2012/11/25/cell-phone-activities-2012/> [<https://perma.cc/DGE9-GR2F>].

⁵⁴ Amardeo C. Sarma & João Girão, *Identities in the Future Internet of Things*, 49 WIRELESS PERS. COMM. 353, 353-63 (2009).

evolved into the “internet of things,” a vision where technologies are connected and perform overlapping tasks. If convergence is inevitable, then the history of camera phones is relevant for new technologies that will combine capabilities in the future.

While the convenience of camera phones is hard to deny, the very capabilities that make them so helpful raise red flags with regards to personal privacy. These harken back to earlier concerns regarding cameras and the perceived degradation of the right to ownership over one’s image and identity. Adding to these fears is the multi-use nature of the devices, which increases the potential for a person to be recorded without their knowledge, particularly in public places.⁵⁵ That these devices are also linked to the internet, allowing would-be photographers and chroniclers the ability to instantly publish their photos, creates, for some, a distinctive threat in need of novel protections.⁵⁶ Building privacy protections for these devices on the muddled and often confusing case history of camera regulation creates even more difficulties.

As scholars have noted, no technology operates in a lawless space, building instead on regulations and controversies of previously existing technologies.⁵⁷ The shared legal lineage between cameras and camera phones is the source of two of the most fundamental questions at the heart of the tension between privacy and camera phone technology: is there an expectation of privacy in public, and where does personal privacy end and freedom of expression begin? These are not new questions—both were explicitly addressed in *Daily Times Democrat* and elsewhere—but the nature of the technology has caused these classic questions to evolve.⁵⁸ Modern day instances of *Daily Times Democrat* have occurred across the country⁵⁹, including at the

⁵⁵ Aimee J. Lum, *Don't Smile, Your Image Has Just Been Recorded on a Camera-Phone: The Need for Privacy in the Public Square*, 27 U. HAW. L. REV. 377, 377 (2004-2005).

⁵⁶ See Alan Kato Ku, *Talk is Cheap, But a Picture is Worth a Thousand Words*, 45 SANTA CLARA L. REV. 679 (2004-2005).

⁵⁷ See Ellen Stokes, *Nanotechnology and the Products of Inherited Regulation*, 39 J.L. & SOC'Y 93, 93-112 (2012).

⁵⁸ Lum, *supra* note 55.

⁵⁹ See Kristin M. Beasley, *Up-Skirt and Other Dirt: Why Cell Phone Cameras and Other Technologies Require a New Approach to Protecting Personal Privacy in Public Places*, 31 S. ILL. U. L.J. 69 (2006-2007).

Lincoln Memorial in Washington, DC in 2014. However, whereas the photographer in *Daily Times Democrat* took advantage of an unfortunate gust of wind, the man at the Lincoln Memorial took advantage of the innocuous appearance of his camera phone to take pictures up the clothes of women at the memorial. The District of Columbia District Court Judge threw out the voyeurism charges against the man, declaring that, though the man's actions were "repellant and disturbing," the women whom he had photographed had no expectation of privacy in such a public place.⁶⁰

Faced with a specific threat and mixed rulings from the judiciary, legislators have attempted to use technical limitations to either ban the practice of "upskirting" explicitly or include it under prohibitions as part of existing provisions of law. When faced with a ruling similar to the one described above, Massachusetts passed a law within two days that specifically banned the practice and provided a "reasonable expectation of privacy in not being so photographed."⁶¹ Chicago had similar concerns in mind when it enacted a broad policy that banned the possession of camera phones in certain facilities, including bathrooms.⁶² While city leaders admitted the policy was virtually impossible to enforce, they felt it important to send the message that such behavior would not be tolerated. Congress has also made efforts to stem such behavior, introducing in 2009 the Camera Phone Predator Alert Act, which would have required camera phones to make a "shutter sound" when a picture was taken.⁶³ Though the law did not pass, most manufacturers added the sound as a default setting, and a similar law is in place in Europe.⁶⁴

While laws and regulations specifically targeting the misuse of camera phones have been successful in some places in the United

⁶⁰ Alanna Vagianos, *Upskirt Photos Don't Violate A Woman's Privacy, Rules D.C. Judge*, HUFFINGTON POST (Oct. 10, 2014), http://www.huffingtonpost.com/2014/10/10/upskirt-photos-legal-dc_n_5966406.html [<https://perma.cc/Y9UL-G896>].

⁶¹ Mass. Gen. Laws Ann. ch. 272, §105 (West 2014).

⁶² Jo Napolitano, *Hold it Right There, and Drop that Camera*, N.Y. TIMES (Dec. 11, 2003), <http://www.nytimes.com/2003/12/11/technology/hold-it-right-there-and-drop-that-camera.html> [<https://perma.cc/FC2Q-LDSB>].

⁶³ Camera Phone Predator Alert Act, H.R. 414, 111th Cong. (last referred to S. Comm. on Commerce, Trade and Consumer Protection, Jan. 14, 2009).

⁶⁴ Napolitano, *supra* note 62.

States, policy makers in other areas have attempted to protect privacy through the use of existing legal provisions. In a number of cases, individuals have been prosecuted under wiretapping laws for recording others without their knowledge.⁶⁵ In California, paparazzi laws have been used to try and provide some level of protection for everyday people.⁶⁶ In cases in which the pictures have been posted online, authorities and plaintiffs have turned to anti-harassment laws for redress. While one could argue that, as Warren and Brandeis proposed, these cases illustrate a commonly understood universal right to privacy rooted in human dignity that undergirds these disparate policies, the lack of a unified approach seems to better support Prosser's "hodgepodge" characterization, at least as an empirical description if not normative aim.

Privacy advocates must also overcome the objections of advocates of other rights when rights claims are in conflict. The real battle for privacy protections may not be civil liberties groups versus industry, but privacy versus other rights. Champions of the right to freedom of expression and freedom of the press claim that the medley of legal concepts to defend freedoms of speech and expression is evidence of their supremacy over the nebulous concept of privacy.⁶⁷ Should people be allowed to wear and share images from body cameras in any setting, for example? If privacy advocates are split between multiple approaches, their arguments can appear muddy and lose out to free speech claims. Prosserians have argued for policies that target specific undesired activities, such as the aforementioned anti-upskirting law in Massachusetts, while dignity-based privacy advocates have called for broad-based policies. In support of their arguments, promoters of a dignity-based conception of privacy point to *Katz v. United States*, which linked privacy rights to a person's reasonable expectation of privacy, even in seemingly public places.⁶⁸ The 2012 ruling in *United*

⁶⁵ Seth F. Kreimer, *Pervasive Image Capture and the First Amendment: Memory, Discourse, and the Right to Record*, 159 U. PA. L. REV. 335, 338 (2010-2011).

⁶⁶ Ku, *supra* note 56, at 695.

⁶⁷ See Kreimer, *supra* note 65; Aaron H. Caplan, *Free Speech and Civil Harassment Orders*, 64 HASTINGS L.J. 781 (2012-2013); Travis Gunn, *Knowledge is Power: The Fundamental Right to Record Present Observations in Public*, 54 WM. & MARY L. REV. 1409 (2012-2013); Margot E. Kaminski, *Regulating Real-World Surveillance*, 90 WASH. L. REV. 1113 (2015).

⁶⁸ Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and The Right to Anonymity*, 72 MISS. L.J. 213, 268 (2002-2003).

States v. Jones that warrantless electronic tracking of vehicles, even if the vehicles are clearly visible and using public roads, constitutes a violation of privacy seemed to confirm this interpretation, though this point is in dispute.⁶⁹ Opinion polls show that the public prefers a broader, dignity-based conception of privacy, even as judicial rulings more often rely on the tort-based conception.⁷⁰

The courts have consistently, though not unanimously, used the technical model in assessing whether certain actions constitute a violation of specific statutes, rather than following the lead of the Alabama Supreme Court in taking a broader view of what privacy might entail. Similarly, while much of the rhetoric surrounding relief from camera phone intrusions has employed the logic of Warren and Brandeis, lawyers and lawmakers have sought legal protection and redress using technical conceptions involving narrowly crafted statutes and legal precedent.

C. Advanced Imaging (Thermal Imaging)

In a landmark case in 2001, the U.S. Supreme Court ruled that the Department of Interior had violated the rights of Danny Lee Kyllo when an investigator used a thermal imager to monitor the heat being released from Kyllo's house. Investigators had been watching the house because they believed Kyllo was growing marijuana in his home, an activity that creates large quantities of heat, which needs to be vented. The thermal imager provided investigators with enough evidence to obtain a warrant, and law enforcement officials confirmed their suspicions. However, in a 5-4 decision that crossed ideological lines, the U.S. Supreme Court ruled that this high tech investigative method was inherently intrusive when conducted without a warrant and constituted an illegal search and seizure of Kyllo's property.⁷¹

⁶⁹ See Christopher Slobogin, *Making The Most of United States v. Jones in a Surveillance Society: A Statutory Implementation of Mosaic Theory*, 8 DUKE J. CONST. L. & PUB. POL'Y 1 (2012) (notes that the majority opinion, authored by Justice Antonin Scalia, actually found in favor of a 4th Amendment violation based on the physical violation of private property rights involved in the placing and maintenance of the electronic tracker. However, Slobogin also notes the concurring opinions by Justices Alito (with Ginsberg, Beyer, and Kagan) and Sotomayor all invoked the concept of a reasonable expectation of privacy).

⁷⁰ Christopher Slobogin & Joseph Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permitted by Society"*, 42 DUKE L.J. 727 (1992-1993).

⁷¹ *Kyllo v. United States*, 533 U.S. 27, 40 (2001).

Privacy advocates lauded the Court's attempt to bring privacy protections into the information age.

While the decision in *Kyllo* was groundbreaking in terms of applying technological limits to police investigations, it is neither the beginning nor the end of the story. In fact, the ruling in the case itself is complicated, raising questions of its own. Beyond the outcome of the ruling, the actual precedent and constitutional tests set forth in *Kyllo* were shaped by subsequent rulings in privacy and technology policy.

The precedent set in *Olmstead* would stand until 1965, when the Supreme Court declared in *Katz v. United States*⁷² that a fourth amendment violation did not necessitate a physical intrusion. In *Katz*, the Federal Bureau of Investigation (FBI) had placed a listening device outside of a telephone booth that Katz used to run his bookmaking business. The Court found that even though Katz was using a public facility, he had an expectation of privacy inside the telephone booth, making the government's recording an unconstitutional search. "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."⁷³ This set up a two-pronged test for determining whether a violation of privacy has occurred: does the person have a reasonable expectation to privacy, and does society accept that expectation as reasonable? The standard established by *Katz* bore a stronger resemblance to dignity-based privacy protection than previous rulings, and it was derided by some as circular, subjective, and unpredictable.⁷⁴ Still, it set the first limitation on law enforcement's use of technology to gather evidence against and prosecute potential criminals.

Katz would not be the last word on the issue of privacy and law enforcement powers. In 1983, the Supreme Court heard *United States v. Place*,⁷⁵ a case in which a traveler, Raymond Place, drew the attention of law enforcement, who detained his luggage and subjected

⁷² *Katz v. United States*, 389 U.S. 347, 353 (1967).

⁷³ *Id.* at 351.

⁷⁴ Richard H. Seamon, *Kyllo v. United States and the Partial Ascendance of Justice Scalia's Fourth Amendment*, 79 WASH. U. L. Q. 1013, 1022 (2001).

⁷⁵ *United States v. Place*, 462 U.S. 696, 707 (1983).

it to a canine sniff test. The canine unit indicated the presence of narcotics, and a later search of the luggage revealed cocaine. The Supreme Court found that as the luggage had not been opened, the dog was only detecting what had seeped into public space. Additionally, because the canine unit's training specifically for detecting narcotics, the search did not represent an unwarranted invasion of privacy.⁷⁶ Similarly, in *California v. Greenwood*,⁷⁷ the Laguna Beach Police Department brought drug charges against Billy Greenwood after searching his garbage. While lower courts had ruled in favor of Greenwood, the Supreme Court found that, since Greenwood had deposited his garbage on the curb for the express purpose of a third party removing it, he had no expectation of privacy and, therefore, was not the victim of a fourth amendment violation (Herdrich 1988, 995).

*California v. Ciraolo*⁷⁸ is particularly relevant for the emerging issue of domestic government drone surveillance. Dante Ciraolo's backyard marijuana farm had attracted the attention of local law enforcement. The police could not see over Ciraolo's tall fence, so they rented a private plane to fly at an altitude of 1,000 feet and look into the yard from above. The officers identified large marijuana plants and photographed them with a standard 35mm camera.⁷⁹ While lower courts disagreed among themselves as to the legality of the police's tactics, the Supreme Court found in favor of law enforcement. In his majority opinion, Chief Justice Burger argued that the police were flying at a height navigated by the public and that "any member of the public flying in this airspace who cared to glance down could have seen everything that the officers observed."⁸⁰ The court ruled *Ciraolo's* expectation of privacy was not reasonable, and the police tactic legitimate.⁸¹ Legal scholars expect that this case will be an important

⁷⁶ Richard E. Myers, *Detector Dogs and Probable Cause*, 14 GEO. MASON L. REV. 1, 6 (2006-2007).

⁷⁷ *California v. Greenwood*, 486 U.S. 35 (1988).

⁷⁸ *California v. Ciraolo*, 476 U.S. 207 (1986).

⁷⁹ Rosemarie Falcone, *California v. Ciraolo: The Demise of Private Property*, 47 LA. L. REV. 1354, 1365 (1986).

⁸⁰ *Ciraolo*, 476 U.S. 207.

⁸¹ Falcone, *supra* note 79, at 1377.

precedent in arguments for the legality of domestic drone surveillance.⁸²

By 2001's *Kyllo* ruling, however, the Court expanded the boundaries of the individual's expectation of privacy further. As previously mentioned, the case revolved around the warrantless use of a thermal imager to examine the heat being produced and vented from various areas of his house to determine if Danny Lee Kyllo was growing marijuana.⁸³ The government argued that, like the case of narcotics particles in *Place*, the heat was being vented into public, thereby making the information no longer private. Additionally, the Court had previously ruled that police could use equipment to augment their senses, and that thermal imaging equipment was simply an extension of this principle. In *Kyllo*, the Court rejected both arguments. Writing for the majority, Justice Antonin Scalia argued that unlike the case of a drug sniffing dog that will only indicate the presence of narcotics, the thermal imaging equipment was not nearly as narrowly focused. Instead of indicating a marijuana growing operation, the technology could reveal any number of activities – even when a person liked to take baths.⁸⁴ The technology granted investigators new senses rather than simply enhanced existing ones the way binoculars might. The potential expansiveness of the technology led to the Court's tightening of the conditions under which the technology could be used.

For many, the ruling in *Kyllo* was a triumph for privacy and protection of individual rights in the face of increasingly sophisticated government and law enforcement technology. However, there was also trepidation. While the case had shown that the Court was concerned with the effect of technological advancement on privacy, Scalia's opinion also sought to ensure law enforcement was not at a technological disadvantage. The opinion referenced police use of advanced technology that is not in "general public use," an important caveat designed to make sure that police are not forced to pursue

⁸² Philip J. Hiltner, *The Drones are Coming: Use of Unmanned Aerial Vehicles for Police Surveillance and its Fourth Amendment Implications*, 3 WAKE FOREST J.L. & POL'Y 397 (2013); Chris Schlag, *New Privacy Battle: How the Expanding Use of Drones Continues to Erode Our Concept of Privacy and Privacy Rights*, 13 PITT. J. TECH. L. & POL'Y 1 (2012); Timothy T. Takahashi, *Drones and privacy*, 14 COLUM. SCI. & TECH. L. REV. 72, 72-114 (2012).

⁸³ Seamon, *supra* note 74, at 1016.

⁸⁴ *Kyllo v. United States*, 533 U.S. 27, 38 (2001).

criminals with increasingly outdated tools. While attempting to add flexibility to the ruling, the majority introduced practical legal questions as well as normative ones.⁸⁵

While the practical issues raised in the *Kyllo* dissent are troubling from a legal process standpoint, the primary normative concern about what privacy should require is of even greater concern. Even though Justice John Paul Stephens disagreed with the finding in *Kyllo*, one of the criticisms in his dissent alludes to the problem left in the decision's wake. Even if one were to ignore the lack of clarity in the "general public use" provision, "this criterion is somewhat perverse because it seems likely that the threat to privacy will grow, rather than recede, as the use of intrusive equipment becomes more readily available."⁸⁶ While ensconced in a legal argument, the concept Stephens refers to is not the legal one shaped by *Katz* and *Place* and others. Instead it is like the Scalia-penned majority opinion, the more ethereal concept of privacy as we currently understand it. Much as Warren and Brandeis did in *The Right to Privacy*, Stephens is not referring to an existing legal concept of privacy, but a normative one, drawing on a conception of human dignity that is universal, or at least that applies to all citizens.

D. Drones

Drones entered the public lexicon through news about military and intelligence activities overseas. While talk of UAS technology still conjures up images of armed Predator drones, in reality most unmanned aircraft used domestically employ smaller, cheaper multiple-rotor technology. These systems have varying degrees of autonomy. They lack the range and power of military drones, but retain the ability to carry cameras and advanced imaging technology.

Many of the contemporary concerns over UAS are new formulations of lingering debates over how far government can go in using image capture technology. Echoes of *Kyllo* and *Ciraolo* can be heard in questions about the purposes for which government can use cameras in the sky,⁸⁷ though their unique capabilities such as size,

⁸⁵ Tracey Maclin, *Katz, Kyllo, and Technology: Virtual Fourth Amendment Protection in the Twenty-First Century*, 72 MISS. L.J. 51, 57 (2002).

⁸⁶ *Id.* at 105.

⁸⁷ See Matthew R. Koerner, *Drones and the Fourth Amendment: Redefining Expectations of Privacy*, 64 DUKE L.J. 1129; Taly Matiteyahu, *Drone Regulations and Fourth*

mobility, and flight times seem to raise the stakes.⁸⁸ With these features, they can capture images and information in ways and from vantages not previously considered by lawmakers or the courts.

The public and politicians have reacted strongly against perceived excesses, though the legal rationales remain murky. For example, a bipartisan group in Congress promised to reign in the FBI's use of UAS to conduct even limited domestic surveillance.⁸⁹ At the local level, news that the Los Angeles Police Department (LAPD) had obtained drones led to protests and the creation of the Stop LAPD Spying Coalition, an amalgamation of privacy and civil rights organizations in Los Angeles, California.⁹⁰ As a result of the public outcry, the LAPD grounded the systems until it received federal guidelines about where, when, and how to use them.⁹¹ The LAPD's drones originally belonged to the Seattle Police Department, which purchased them using grant money from the Department of Homeland Security but sold them following public protests.⁹² Despite assurances by officials in all these cases that UAS's would be used only under highly controlled circumstances, concerns over both potential misuse and eventual operation led to organized protests that grounded the aircraft.

While the ability of government to infringe upon privacy rights is at the forefront of questions regarding drone use, concerns regarding UAS use by private parties also exist. Many have expressed concerns regarding Amazon's efforts to use autonomous drones for low-weight package deliveries, with critics arguing that allowing the use of such

Amendment Rights: The Interaction of State Drone Statutes and the Reasonable Expectation of Privacy, 48 COLUM. J.L. & SOC. PROBS. 265 (2025).

⁸⁸ Ryan M. Calo, *The Drone as a Privacy Catalyst*, 64 STAN. L. REV. ONLINE 29, 30 (2011).

⁸⁹ Carol Cratty, *FBI Uses Drones for Surveillance in U.S.*, CNN (June 20, 2013), <http://www.cnn.com/2013/06/19/politics/fbi-drones> [<https://perma.cc/A9R9-ZXEC>].

⁹⁰ Joseph Serna, *Anti-Spying Coalition Launches Campaign Against LAPD Drones*, L.A. TIMES (Aug. 21, 2014), <http://www.latimes.com/local/lanow/la-me-ln-anti-drone-campaign-lapd-city-hall-20140821-story.html> [<https://perma.cc/MSG5-9UJJ>].

⁹¹ *Id.*

⁹² Christine Clarridge, *Seattle Grounds Police Drone Program*, SEATTLE TIMES (Feb. 8, 2013), <http://www.seattletimes.com/seattle-news/seattle-grounds-police-drone-program/> [<https://perma.cc/MSG5-9UJJ>].

technologies could lead to mass surveillance.⁹³ Phones arguably offer the potential for mass surveillance already, but drones inspire a particularly visceral reaction among the public. Since Amazon's announcement, other technology giants such as Google have announced their own drone programs. Fears over corporate use of drones only intensified when, in April 2015, the FAA announced that it was granting Amazon's request to test its UAS technology in the open skies. Permission had been granted in March for a different Amazon UAS technology, but the approval process had taken so long that the technology was obsolete.⁹⁴ Privacy advocates have taken notice of the potential for increasing surveillance by the private sector, with the Electronic Privacy Information Center (EPIC) filing suit against the FAA in April 2015 for its failure to include privacy provisions in its proposed rulemaking regarding commercial drone use.⁹⁵ Other criticisms focus not so much on the camera or aviation technology but on the degree to which algorithms that assess and employ the data are hidden from view.⁹⁶ The increasingly emotional debate between advocates of technology and the skeptical public is similar to other conflicts with new technology, such as genetically modified food.⁹⁷

The federal agency that has found itself at the center of the U.S. drone debate is the Federal Aviation Administration. The FAA, which regulates use of the nation's airways, was charged in the FAA Modernization and Reform Act of 2012 (P.L. 112-95) to not only create regulations governing the use of commercial drones in the United States, but also to increase the use of UAS technology and

⁹³ David Horsey, *Jeff Bezos' Amazon Drone Fleet Raises Premature Privacy Fears*, L.A. TIMES (Dec. 5, 2013), <http://articles.latimes.com/2013/dec/05/nation/la-na-tt-amazon-drone-fleet-fears-20131204> [<https://perma.cc/Y6FP-E9L9>].

⁹⁴ Bart Jansen, *FAA Approves Amazon Drone Research Again*, USA TODAY (Apr. 9, 2015), <http://www.usatoday.com/story/money/2015/04/09/faa-amazon-drone-approval-prime-air/25534485/> [<https://perma.cc/JBS5-EVRQ>].

⁹⁵ Keith Laing, *Privacy Group Sues Feds Over Drone Rules*, THE HILL (Apr. 2, 2015), <http://thehill.com/policy/transportation/237728-privacy-group-suing-feds-over-drone-rules> [<https://perma.cc/43U3-XYDM>].

⁹⁶ FRANK PASQUALE, *THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION* (2015).

⁹⁷ MARK A. POLLACK & GREGORY C. SHAFFER, *WHEN COOPERATION FAILS: THE INTERNATIONAL LAW AND POLITICS OF GENETICALLY MODIFIED FOODS* (2009).

ensure the protection of privacy. The agency long protested being given more responsibility to regulate privacy, claiming that it lacks sufficient expertise and capacity.⁹⁸ In February 2015, the responsibility for the privacy-related portion of the rulemaking was removed by a presidential memorandum and transferred to the Department of Commerce's National Telecommunications and Information Administration (NTIA).⁹⁹

Beyond shifting the responsibility for privacy regulations from the FAA to the NTIA, the memorandum provided insight into the approach the president would take to protect privacy. Naming both privacy and civil liberty protection as essential to federal regulation of drone use, the document cites the importance of the Privacy Act as a foundation. The Privacy Act regulates how the government collects, stores, and disseminates personal information, also allowing individuals access to and the ability to amend their personal data. Unfortunately, the Act has not been as successful in accomplishing these goals as many of its supporters would hope.¹⁰⁰ The Presidential Memorandum also forbids agencies' sharing of information collected by drones except when required by law or when it fulfills the program's authorized purpose. This technocratic approach is meant to allow agencies to operate within familiar guidelines while extending some level of privacy protection to individuals. Privacy advocates supported the memorandum's approach as a first step, but said that "much more needs to be done to protect our privacy."¹⁰¹

Congress has also been involved in the debate over what privacy protections should extend to domestic drone operations. At a hearing

⁹⁸ UAS INTEGRATION OFFICE, FED. AVIATION ADMIN., FAA UNMANNED AIRCRAFT SYSTEMS (UAS): CYBER SECURITY INITIATIVES 11, 12 (2015), https://beta.csrc.nist.gov/CSRC/media/Presentations/FAA-Unmanned-Aircraft-Systems-Update/images-media/2015-feb_george-ispab.pdf [<https://perma.cc/PT6N-3T5W>].

⁹⁹ *Presidential Memorandum: Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems*, WHITE HOUSE (Feb. 15, 2015), <https://obamawhitehouse.archives.gov/the-press-office/2015/02/15/presidential-memorandum-promoting-economic-competitiveness-while-safegua> [<https://perma.cc/B2ZV-S5PJ>].

¹⁰⁰ See Gloria Cox, *Implementation of the Routine Use Clause of the Privacy Act*, 10 REV. POL. RES. 42 (1991).

¹⁰¹ Neema Singh Guliani, *Unchecked Government Drones? Not Over My Backyard*, THE HILL (Mar. 24, 2015), <http://thehill.com/blogs/congress-blog/civil-rights/236701-unchecked-government-drones-not-over-my-backyard> [<https://perma.cc/26JV-R99G>].

regarding the aforementioned FBI activities, Senator Diane Feinstein (D-CA), the then-Chairwoman of the Senate Select Committee on Intelligence, declared, “I think the greatest threat to the privacy of Americans is the drone and the use of the drone, and the very few regulations that are on it today and the booming industry of commercial drones.”¹⁰² One measure of congressional attention is how many bills are introduced on a subject. In the 113th Congress (2013-2014), 32 bills were introduced to regulate drone use by authorities and private parties.¹⁰³ Ranging from bans on armed drones to requirements that officials obtain warrants before utilizing UAS technology, the introduced legislation reflects the broad-based concerns many harbor toward drone technology. At the same time, however, many legislators recognize the commercial and law enforcement potential for the technology, and have attempted to tailor their efforts to accommodate growth and development of the sector.¹⁰⁴

Some scholars argue that national legislation is necessary to protect privacy and prevent confusion, but in the absence of clear guidance, states have been unwilling to wait.¹⁰⁵ Other scholars contend that states, as the primary venue for privacy law, are the natural place to tackle drone-related privacy concerns.¹⁰⁶ As in the case of camera phones, states have used a combination of existing privacy statutes and new laws to tackle privacy issues. In 2014, 36 states introduced legislation to restrict drone use, many focused on limiting government use, however only 15 states had passed such legislation (including legislation enacted in 2013) by the end of 2014.¹⁰⁷ While state legislatures continue to debate potential drone-

¹⁰² Cratty, *supra* note 89.

¹⁰³ CONGRESS.GOV, <https://www.congress.gov/> [<https://perma.cc/6XXY-K8G5>].

¹⁰⁴ Keith Laing, *Move Would Ground Domestic Drones over Privacy Concerns*, THE HILL (Nov. 4, 2013), <http://thehill.com/policy/transportation/189208-sen-markey-files-bill-to-protect-privacy-in-commercial> [<https://perma.cc/7WLK-XWZQ>].

¹⁰⁵ See Ben Jenkins, *Watching the Watchmen: Drone Privacy and the Need for Oversight*, 102 KY. L.J. 161 (2013-2014).

¹⁰⁶ See Wells C. Bennett, *Civilian Drones, Privacy, and the Federal-State Balance*, in THE ROBOTS ARE COMING: THE PROJECT ON CIVILIAN ROBOTICS 2 (2014); Margot E. Kaminski, *Regulating Real-World Surveillance*, 90 WASH. L. REV. 1113, 1118 (2015).

¹⁰⁷ 2014 State Unmanned Aircraft Systems (UAS) Legislation, NAT'L CONF. OF ST. LEGISLATURES (July 2, 2015), <http://www.ncsl.org/research/transportation/2014-state-unmanned-aircraft-systems-uas-legislation.aspx> [<https://perma.cc/LH4Z-2TX6>].

related measures, existing statutes such as anti-wiretapping and “peeping tom” laws have been used to protect against private actors, while search and seizure laws have constrained law enforcement UAS use.¹⁰⁸ Cities have also sought to tackle the drone issue with a variety of approaches. Some have simply passed resolutions calling for state or federal regulations,¹⁰⁹ while others have considered specific restrictions on private or law enforcement use.¹¹⁰ Courts are testing whether existing laws, such as those covering trespassing and unlawful surveillance, provide adequate protection of privacy rights.¹¹¹

States That Introduced Drone-Related Legislation in 2014		
Alabama	Louisiana*	Rhode Island
Alaska*	Maryland	South Carolina
Arizona	Massachusetts	Tennessee*
California	Michigan	Utah*
Connecticut	Minnesota	Vermont
Georgia	Missouri	Virginia
Hawaii	Nebraska	Washington
Illinois*	New Hampshire	West Virginia
Indiana*	New York	Wisconsin*
Iowa*	New Jersey	Wyoming
Kansas	North Carolina*	Oklahoma
Kentucky	Ohio*	Pennsylvania

*Legislation Passed in 2014

States Enacting Legislation	Year
Alaska	2014
Florida	2013
Idaho	2013
Illinois	2013, 2014
Indiana	2013
Iowa	2013
Louisiana	2014
Montana	2013
North Carolina	2013, 2014
Oregon	2013
Tennessee	2013, 2014
Texas	2013
Utah	2014
Virginia	2013
Wisconsin	2014

¹⁰⁸ Bennett, *supra* note 106, at 4.

¹⁰⁹ Jason Koebler, *City in Virginia Becomes First to Pass Anti-Drone Legislation*, U.S. NEWS & WORLD REPORTS (Feb. 5, 2013), <http://www.usnews.com/news/articles/2013/02/05/city-in-virginia-becomes-first-to-pass-anti-drone-legislation-> [https://perma.cc/38VL-NK6P].

¹¹⁰ Jason Koebler, *New York City's Drone Ban Would Be the Strictest in the Country*, MOTHERBOARD (Dec. 16, 2014), <http://motherboard.vice.com/read/new-york-citys-drone-ban-would-be-the-strictest-in-the-country> [https://perma.cc/KUU2-X4E4].

¹¹¹ Robert A. Heverly, *The State of Drones: State Authority to Regulate Drones*, 8 ALB. GOV'T L. REV. 29, 48-58 (2015); James Barron, *Drones Outpacing Rules as Popularity Soars in New York*, N.Y. TIMES (Aug. 3, 2014), http://www.nytimes.com/2014/08/04/nyregion/drones-outpacing-rules-as-popularity-soars-in-new-york.html?_r=0 [https://perma.cc/9DDH-Y3FW].

III. DRONES AND THE NEED FOR AN INTEGRATED APPROACH

The history of image capture technology shows the utility of technical approaches to the law. Violations of privacy using one technology can offer analogies to privacy violations in another. Cameras are ubiquitous now, but the early struggle over how to set limits on their use helped frame subsequent debates over camera phones and thermal imaging, and today they offer analogies to defending privacy against drone technology. History shows that some jurists will permit specific restrictions on technology to reduce demonstrable harm even when they are unwilling to interpret a broader dignity-based understanding of privacy. In some sense, we are all “Prosserian” in the American legal system—positivist jurisprudence is the most common contemporary legal framework.¹¹²

Beyond the courts, history shows that legislators and regulators look first to narrow technical policies to protect privacy. The implication is that any attempt to protect privacy without incorporating the Prosserian tradition is likely to be impotent. Generalized defenses of privacy alone are an insufficient foundation for laws meant to restrict government from conducting certain activities, or for a court to find that one person has legally injured another.

At the same time, the Warren and Brandeis tradition of dignity-based privacy has proven to be a valuable resource often enough that it should be part of a robust defense of privacy.

Research shows that the public’s understanding of what privacy entails is closer to the broad notion of a dignity-based human right to privacy than it is to the technical conception.¹¹³ The dignity-based conception of privacy ensures some democratic accountability, since it satisfies the intuition of a large portion of the public while not being strong enough on its own to stop technological development. While technical defenses of privacy are more limited and bound by what is reasonable, dignity-based conceptions of privacy assume claims about

¹¹² See Joseph Raz, *Legal Positivism and the Sources of Law*, in ARGUING ABOUT LAW 117 (Aileen Kavanagh & John Oberdiek eds., 2009).

¹¹³ See Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 MISS. L. REV. 213 (2002); Christopher Slobogin & Joseph E. Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at Understandings Recognized and Permitted by Society*, 42 DUKE L.J. 727 (1993).

self-ownership —later referred to as the right to publicity. Dignity-based conceptions of privacy show greater potential for prevailing over competing rights, as in the examples from camera technology, and for contributing to the “visceral jolt” that Calo hopes attention to drones will bring to 21st century privacy law.¹¹⁴

The broader, dignity-based privacy tradition also offers substantial resources to support one of law’s roles as a source for claims about first principles of right and justice.¹¹⁵ These principles need not be confined to philosophy and textbooks. For example, a judge in 2015 dismissed all charges against a man who shot down a drone that he claimed was invading his privacy.¹¹⁶ The man shot down the drone to defend himself, and the judge found that the operator had no cause for bringing charges against someone defending his own property. Despite the trend toward positivism in law, drones provoke visceral reactions in deed and speech. Dignity-based claims remain powerful in part because technical approaches to law in these cases are unsettled. As Froomkin and Colangelo write, “Intrusion on seclusion is a recognized, if somewhat exotic, tort, but its rarity in the courts means that the scope of permissible self-help against privacy-invading chattels—like the camera planted by the landlord in the tenant’s bedroom—is poorly charted legal territory. When a privacy intrusion also involves a trespass, the trespass rule likely defines the scope of permissible self-help. But some robot-enhanced privacy intrusions will not involve trespass, and these are the hardest cases.”¹¹⁷

Current law on the books may not adequately protect against the potential threats to privacy posed by rapidly advancing technology, leaving individuals without recourse in response to obvious moral wrongs. Taking a wider view of privacy can bridge the gaps left by narrowly crafted policies, much as Warren and Brandeis espoused over a century ago. The increasing ubiquity of image capture technology suggests that gaps will emerge at a greater rate as technology progresses. For example, several cases and related

¹¹⁴ Calo, *supra* note 88.

¹¹⁵ See Lon L. Fuller, *Reason and Fiat in Case Law*, 59 HARV. L. REV. 376 (1946).

¹¹⁶ *Judge Dismisses Charges for Man Who Shot Down Drone*, WDRB.COM (Oct. 26, 2015), <http://www.wdrb.com/story/30354128/judge-dismisses-charges-for-man-who-shot-down-drone> [<https://perma.cc/U374-L4A2>].

¹¹⁷ Michael Froomkin & Zak Colangelo, *Self-Defense Against Overflying Drones*, 48 CONN. L. REV. 1, 4 (2015).

scholarly interpretations claim that privacy harms can only occur when a person is present to commit the harm— a robot or drone, therefore, could not commit a privacy harm, the logic goes.¹¹⁸ A dignity-based argument about privacy and some technical analogies to other cases may help extend privacy protection in these cases. For example, drones have an operator just as a camera does; the principal difference is that the operator sits at a greater distance.

Drawing on both of these conceptions of privacy will give privacy advocates the benefit of the respective virtues of each tradition. Dignity-based privacy is broad enough to adapt to new and unforeseen technological developments or novel uses. Furthermore, policy that draws upon dignity-based ideas of privacy are likely to elicit greater support from a public that understands privacy in terms of broad principles rather than legal technicalities. At the same time, using technical measures will allow policy makers to target those behaviors found to be most repellant and will be specific enough to reduce uncertainty about whether or not the behaviors are permitted. For instance, the Department of Homeland Security Privacy Office is charged with maintaining a balance between privacy and the department's goals. The office is statutorily required under the Homeland Security Act of 2002 to enforce privacy-related policies, such as the Freedom of Information Act and Privacy Act, and ensure they are embedded into the activities of the organization. While the policies the DHS Privacy Office is charged with implementing are technical, the office claims a more normative mantle. In describing its mission relating to cybersecurity, the office proclaims privacy to be "more than just compliance with privacy laws," invoking the values of public trust, transparency, and confidence in the government as guiding principles.¹¹⁹ Other government agencies may want to follow the same path by tying together the technical provisions they implement under a normative claim about the substantive goods that a defense of privacy serves.

Synthesizing the approaches will not be easy in practice, however, as the advantages of each approach do not necessarily negate the weaknesses of the other, and could, in fact, exacerbate them. For instance, the imprecision of dignity-based approaches would be all the

¹¹⁸ See, e.g., *Illinois v. Caballes*, 543 U.S. 405 (2005).

¹¹⁹ *Cybersecurity and Privacy*, DEP'T OF HOMELAND SEC., <https://www.dhs.gov/cybersecurity-and-privacy> [<https://perma.cc/24F5-KMVA>].

more glaring if inelegantly wedged into technical legal provisions. Similarly, the addition of Prosserian language to a dignity-based policy could limit its utility by establishing some protections or violations as more important than others. As such, any attempt to incorporate both understandings of privacy must be done with the appreciation of not only the beneficial possibilities, but also the potential pitfalls of such efforts.

Forum	Privacy Conception	Potential Shortcoming
Statute	Technical	Inflexible
Regulation	Technical	
Judicial Rulings	Technical	
	Dignity-Based	Insufficiently Specific
Public Debate	Dignity-Based	

History and contemporary events demonstrate that as technology advances, there will inevitably be concerns regarding how these advances will impact personal privacy. Already, voices in the drone debate are shifting their attention from the multicopters of today to the insect-sized miniature drones of tomorrow. There may always be a tension between technological innovation and privacy concerns, particularly big data technologies that make even the most seemingly arbitrary pieces of personal information potentially valuable. Satisfying both the desire for innovation and the protection of privacy requires judges and lawmakers to identify the line between public and private information in context. Both Warren and Brandeis' conception of dignity-based privacy and Prosser's tort-based conception are resources for these debates, as each tradition offers its own advantages. Philosophers and the public may understand privacy as rooted in a broad conception of human dignity, but the law will offer the most certainty when privacy is buttressed by technical claims and protections.