A Novel Approach to Modeling
Contextual Privacy Preference and Practice

Peter J. Radics

Dissertation submitted to the Faculty of the
Virginia Polytechnic Institute and State University
in partial fulfillment of the requirements for the degree of

Doctor of Philosophy
in
Computer Science and Applications

Nicholas F. Polys, Chair
Deborah G. Tatar
Dennis G. Kafura
Jeffrey M. Bradshaw
Chreston A. Miller

July 15, 2016
Blacksburg, Virginia

Keywords: Privacy, Framework, Behavior, Modeling

A Novel Approach to Modeling Contextual Privacy Preference and Practice

Peter J. Radics

(ABSTRACT)

We are living in a time of fundamental changes in the dynamic between privacy and surveillance. The ubiquity of information technology has changed the ways in which we interact, empowering us through new venues of communication and social intimacy. At the same time, it exposes us to the prying eyes of others, in the shape of governments, companies, or even fellow humans. This creates a challenging environment for the design of 'privacy-aware' applications, exacerbated by a disconnect between abstract knowledge of privacy and concrete information requirements of privacy design frameworks.

In this work, we present a novel approach for the modeling of contextual privacy preference and practice. The process guides a 'privacy analyst' through the steps of evaluating, choosing, and deploying appropriate data collection strategies; the verification and validation of the collected data; and the systematic transformation of the dense, unstructured data into a structured domain model. We introduce the Privacy Domain Modeling Language (PDML) to address the representational needs of privacy domain models. Making use of the structure of PDML, we explore the applicability of the information theoretic concept 'entropy' to determine the completeness of the resulting model. We evaluate the utility of the process through its application to the evaluation and re-design of a web application for the management of students' directory information and education records. Through this case study, we demonstrate the potential for automation of the process through the Privacy Analyst Work eNvironment (PAWN) and show the process's seamless integration with existing privacy design frameworks. Finally, we provide evidence for the value of using entropy for determining model completeness, and provide an outlook on future work.

Dedication

This dissertation is dedicated to the memory of my grandmother

Porkoláb Klára

(August 2, 1913 – September 17, 2015)

You once said "The only thing nobody can ever take away from you is your education." And truly, you demonstrated the truth of this statement throughout your life. Despite facing many hardships — including two world wars — your *joie de vivre* was nothing short of inspiring.

I am truly privileged to have known you!

You are sorely missed!

Acknowledgments

No work of true significance is ever achieved in isolation. Thus, I want to acknowledge the many incredible people that have helped me through this long — and sometimes arduous — journey.

My thanks goes to my advisor, Nicholas Polys, who has taken on this responsibility during a rough stretch of the journey. He provided me with the freedom to pursue the direction of research I envisioned while helping to focus its scope. His open door and willingness to bounce back and forth ideas were invaluable in addressing some of the challenges of the privacy domain.

This work would also not have been possible without the feedback and guidance of my committee. They, furthermore, helped me to focus on increasing the impact of this work through challenging me to consider how my suggested methodology would be used in real practice. Their continued interest and appreciation of the importance of the challenging topic provided me with motivation to see it through to the end. I would also like to thank Denis Gračanin, who was a major influence on the initial direction of this research.

Finally, none of this work would have been possible without the unwavering support of my friends and family. They were essential in keeping me sane throughout my tenure in graduate school, tolerating the many rants on both my research and graduate student life in general. Most importantly, they demonstrated incredible patience, humoring me when I replied to their questions as to when I was going to graduate with “when it’s done!” And now, that moment has finally come!

Contents

List of Figures

List of Tables

Chapter 1

Introduction

> *"To its profound distress, the American public has recently learned of a revolution in the techniques by which public and private authorities can conduct scientific surveillance over the individual."* – Alan F. Westin [Westin 1967, p. 3]

When reflecting upon this quote from Alan Westin's seminal work "Privacy and Freedom", one cannot help but draw parallels between the year 1967, in which the book was published, and today. The advances in technology that gave rise to the public concerns Westin addresses (like, e.g., wire taps or polygraphs) are by now well known and regulated. However, recent revelations on government surveillance programs (e.g., [Greenwald 2013a,b]) have brought discussions about surveillance and privacy back into public discourse. The technology industry has found itself on both sides of this discussion, whether as perceived perpetrator of institutionalized surveillance [Heath 2015] or as perceived champion of consumer privacy [Levine and Menn 2016].

However, there is widespread consensus about the implications of privacy for the design of technology [Shapiro 2010]. For example, it has been shown that privacy concerns are among the deciding factors for the acceptance of new technology [Caine et al. 2006b]. Not addressing these concerns correctly — or even ignoring them — has a stymieing effect on the adoption of certain types of technology [Chakraborty et al. 2011]. Furthermore, the unprecedented ubiquity of technology has made it increasingly harder for people to manage their own privacy [Chakraborty et al. 2011]. This is exacerbated by the fact that it is often hard to identify the potential of a certain technology being used for surveillance [Endler et al. 2011].

Now, more than ever, do designers of new technology need to consider the implications of privacy for their products and the effect of their products on the privacy of their customers [Shapiro 2010; Caine et al. 2006b].

1.1 Privacy and Technology

While privacy is not the main goal of users of information technology, failure to maintain it can cause more severe outcomes for the user than the breakdown of goal-related functionality [Karat et al. 2005]. The increasing amount of technology in our lives, be it in the form of social networks (e.g., [Lampinen et al. 2011; Squicciarini and Griffin 2012]), pervasive spaces (e.g., [Chakraborty et al. 2011]), location-based applications (e.g., [Kostakos et al. 2011; Poolsappasit and Ray 2008], assistive technology (e.g., [Gaßner and Conrad 2010; Park et al. 2010]), or smart homes and devices (e.g., [Arabo et al. 2012]), results in a growing burden on the user to specify privacy preferences [Chakraborty et al. 2011]. Thus, privacy concerns of technology users have become more and more present and pronounced.

Lessig [1999] attributes these rising concerns and the increased difficulty of protecting one's privacy to the growing imbalance between the *monitored* (the part of one's life that others may be able to perceive) and the *searchable* (the part of one's life that leaves a permanent record). Moreover, the embodied privacy-regulation techniques individuals apply in everyday life, which are inherently spatial in nature, often fail due to the difficulty of determining the presence of an entity in the environment, the persistence of information in the digital realm, and the overlapping of different environments [Palen and Dourish 2003]. Furthermore, the *contextual integrity* offered by physical environments is no longer guaranteed as digital information is usually stripped of its context [Nissenbaum 2004].

Pervasive (or ubiquitous) computing is an area of research that may yield many practical many benefits. It also faces important privacy challenges [Harrison et al. 2010]. For example, while the data captured through sensors within a user's environment can be beneficial for the detection of context, it also raises privacy issues [Schaub et al. 2012b]. These concerns are not limited to sensor environments, but are also pertinent to location-based applications [Poolsappasit and Ray 2008; Wernke et al. 2012; Wiese et al. 2011; Wu et al. 2011; Zhong and Hengartner 2009] and participatory sensing applications [Groat et al. 2012; Christin et al. 2012b]. Privacy issues may even pose a threat to the adoption of pervasive computing application [Groat et al. 2012; Chakraborty et al. 2011].

Challenges faced in the design of privacy-aware pervasive computing applications are twofold. First, the increasing amount of sensors and virtual entities in the environment result in a growing burden on the user to specify privacy preferences [Wiese et al. 2011; Schaub et al. 2012b; Chakraborty et al. 2011]. More importantly, the user may not even be aware of the presence of these entities [Endler et al. 2011]. Second, a further challenge lies in the design of techniques for privacy preservation. Thus, a lot of work within pervasive computing deals with the evaluation of the usefulness of concepts such as anonymity [Wu et al. 2011; Schaub et al. 2012b; Zhong and Hengartner 2009; Christin et al. 2012b] or obfuscation of data [Wernke et al. 2012; Schaub et al. 2012b], often in terms of abstract models of information flow or context (e.g., [De Cristofaro et al. 2011; Hore et al. 2009]).

However, the effectiveness of these approaches is debatable [Peddinti and Saxena 2011]. Kelley et al. [2011] further confirm that a simple opt-in/opt-out approach to the protection of privacy is not fine-grained enough. Toch et al. [2010] show that location sharing preferences are influenced by the diversity of a location and develop *location entropy* as a measure of that characteristic. Many pervasive computing applications, such as health monitoring systems [Banerjee and Gupta 2012] or location-based applications [Wernke et al. 2012; Wiese et al. 2011; Wu et al. 2011], are embedded in the context of complex social behavior. This gave rise to an increasing number of work investigating the social aspects of privacy in pervasive computing through behavioral analysis [Wiese et al. 2011; Biamino 2011; Choe et al. 2011]. These efforts are illustrative of the diverse privacy phenomena associated with the pervasive computing domain.

Wiese et al. [2011] examine the influence of the relationships between individuals on their location sharing behavior, showing that the identity of the recipient of the location information is the most important factor in the decision whether or not to share. Mancini et al. [2011] studied the effects of a location sharing application on close-knit groups and found that the technology had the potential of impacting the relationships of group members, as location-sharing preferences and feedback were insufficient in reflecting the complex dynamics of the groups.

Iachello et al. [2005] also studied location-sharing in close-knit groups. They observed that, given a location-based service that did not rely on real-time location sensing but rather on the disclosure of the location by the responder to a location-request, individuals utilized deception to protect their privacy. They further found that control over location disclosure was seen as a prerequisite for the utility of the messaging application. Furthermore, study participants displayed less inhibition to disclose their location to close friends or family than to individuals not falling into those categories. This relationship of closeness and information disclosure has also been observed by Judge et al. [2010] in their study of the 'family window', an application connecting families living far apart through a permanent video link. Their study also provided more evidence for the importance of controlling one's social interactions as well as others' knowledge of oneself. These findings were confirmed in a study of the influence of social relationships, location, and type of interaction on both the perception of an intrusion and the strategy employed to mitigate the situation [Radics and Gračanin 2011].

Similarly, concerns arise in assisted living environments and sensor-rich environments. With the integration of further technology into domestic environments, be it in the form of security cameras, environmental sensors, or wireless technology, the concerns about how to manage these systems in the resulting automated houses rises [Brush et al. 2011]. For example, Duncan et al. [2009] developed a system called 'Portal Monitor' that monitors the entrances of an elder's home, sending pictures of both the inside and outside of the home to a caregiver if activity near the door is detected. The system is meant to prevent wandering as well as provide additional security to the elder.

However, the video monitoring raises privacy concerns for both the elder and potential visitors. Caine et al. [2006a] compare the trade-offs involved with a visual monitoring system in terms of privacy, imaging technology (i.e., video image, blob tracker, point-light image), and functioning of the elderly. Faucounau et al. [2009] explore the requirements that a robotic agent would have to fulfill to support caregivers in providing care to an elder with cognitive impairments. Their study found that the main desired functions of the robot were cognitive stimulation of the elder, detection of emergency situations, as well as providing the elder with reminders.

Focusing on requirements of eHealth systems, Tan et al. [2010] posit that the main functions of such a system are assistance in the provision of cost-effective, patient-centered health care, as well as education of the chronically ill about their illness and assisting them in achieving long-term lifestyle changes. However, they also identify an increased reliance on health-related data that has to be exchanged between the patient and the caregiver. Little and Briggs [2009] raise the question whether ubiquitous computing systems, especially in the context of pervasive healthcare, will provide advantages or disadvantages to elderly people. They see a risk of transforming the physiological and psychological challenges elderly people face into social disability due to the rising complexity of technological systems today. The results of their study show that there are many trade-offs associated with ubiquitous computing services for the elderly. Major concerns for the elderly are not only trust and privacy, but rather surrounding penalizing non-adoption and social isolation.

Plaza et al. [2011] highlight how information and communication technology may not only be used for assistance in care or health-related tasks, but rather also for the development and maintenance of outside contact, preserving mental capacity, as well as providing the possibility of continued employment beyond retirement age through telework. They also noted that, under certain circumstances, benefits in safety and mobility might balance out privacy concerns. Caine et al. [2006a] found a trade-off in the monitoring of elderly family members through video technology in their homes, the influencing factors being the type of video data gathered and the level of functioning of the observed. Their findings suggest a trade-off between the level of functioning of the elderly family member and the choice of image technology, providing a connection between privacy and risk management [Slovic 1987].

Choe et al. [2011, 2012] studied the preferences of inhabitants towards the recording of activity in the home . Their most interesting finding suggests that, if people are aware of the monitoring, their behavior in the monitored space changes. According to Nguyen et al. [2011], individuals expressed most concern about the recording of activities that they had not given permission to, yet were also concerned about the amount of data collected, the user and use of the data, as well as potential misrepresentation due to errors in the data. This is reflected in the work of Judge et al. [2011] studying the 'family portal'. While they found that the potential for privacy issues was mitigated by the fact that participants were connected to family members they were close to, these issues were still encountered in the violation of solitude and confidentiality (i.e., observers witnessing something that they were not supposed to). The study provided more evidence for the importance of controlling one's social interactions as well as others' knowledge of oneself.

Furthermore, while the introduction of technologies can be seen as stepping stones towards truly smart homes, like the Virginia Tech lumenHaus [Gračanin et al. 2011] or the Georgia Tech Aware Home [Kientz et al. 2008], this does not go without consequences. Technology blurs the lines between work and the home, creating homogeneity between work places and the home, which has the potential of impeding the restorative character of the home [Aipperspach et al. 2009]. Unfortunately, findings from research performed in work environments cannot be easily transferred into domestic environments [Crabtree and Rodden 2004].

Further areas with strong implications for privacy include social networking applications (e.g., [Lampinen et al. 2011]) and wearable sensors (e.g., [Raij et al. 2011]). Social networking applications make it difficult for individuals to control what information is available about them, especially since they are not the only people contributing that information and social networking applications do not support the establishment or enactment of social contracts between the different parties involved [Lampinen et al. 2011]. Wearable sensors, for example, while having the potential to revolutionize healthcare by capturing important health-related data, also have the danger of potentially contributing to behavioral profiling [Raij et al. 2011].

In March 2012, the Federal Trade Commission [2012] released a new set of guidelines for businesses and policymakers regarding the protection of consumers' private information. The main point of the guidelines is the adoption of "Privacy by Design". This involves an increase in transparency, the limitation of data collection, as well as placing limits on data retention. Furthermore, the guidelines suggest providing users with choices regarding data contribution *within the context* they share the data. This is supposed to shift the burden of protecting privacy from the user to the business (and thus, ultimately, the application developer). Thus, designers have to provide architectural support for the control over access to personal data and minimize risk after that data leaves a users' direct control [Spiekermann and Cranor 2009]. Especially, since treating privacy protection as an add-on feature of a system rather than as a part of its fundamental design requirements causes technological challenges for design [Karat et al. 2005; Shapiro 2010]. They also have to integrate appropriate feedback and control mechanisms into their designs to make users aware of their current privacy state [Ayyavu and Jensen 2011].

However, despite this call for self-regulation, the widespread collection and sharing of data represents the status quo [Zang et al. 2015]. Collection by default is still the predominant approach, often without the option to opt-out [Heath 2015]. Furthermore, many applications still fall short of providing adequate controls for managing private information. Yet while there often is a clear monetary incentive for companies to collect or share information, this is not the only cause for the lack of privacy protection in modern applications. Rather, part of the issue lies in the fact that designing privacy-aware applications is *hard* (e.g., [Shapiro 2010]).

In fact, Karat et al. [2005] propose privacy as a critical area of research within Human-Computer Interaction to address the major challenges of designing for privacy. Thus, it is up to the privacy research community to provide designers with the mechanisms to achieve "privacy by design" [Shapiro 2010]. Yet, to truly understand these challenges, it is first necessary to understand the functions of privacy and its expressions in human behavior. Only this knowledge allows to clearly identify the nature of the challenges this complex social construct presents to designers and developers.

1.2 The Nature of Privacy

Privacy is a universal concept that can be found in cultures across the globe [Westin 1967]. However, at the same time, it is not an easy concept since the term has seen myriads of definitions and uses [Solove 2006]. This makes it necessary to provide designers and developers with both *knowledge* of why privacy is important and how it is expressed, as well as *guidance* in the use of that knowledge in the design of privacy-aware systems [Shapiro 2010]. Thus, we need to survey and explore the different motivations and behaviors that comprise the nature of privacy.

1.2.1 Motivations for Seeking Privacy

One of the most quoted accounts of privacy is the work of Westin [1967]. He distinguishes between four different states of privacy: *solitude* (freedom from observation), *intimacy* (being alone with a person or group of people), *anonymity* (being unrecognized while being with others), and *reserve* (limitation of disclosure of personal aspects). Westin argues that the fundamental motivations for privacy are to create opportunity for *personal autonomy*, *emotional release*, *self-evaluation*, as well as *limited and protected communication*. Privacy is required for *personal autonomy*, i.e., the development and maintenance of the self. Private *emotional release* is used to reduce the tension between the social self, carrying out the different roles a person plays in society, and the individual self. Emotional release is also necessary for relaxation from over-stimulation, to maintain intimate relationships, and for recuperating from emotional trauma. People need to carry out private *self-evaluation* to deal with the vast amounts of information they encounter every day. This includes contemplation on their own actions, both in terms of their morality as well as for creative purposes. Thus, self-evaluation helps to decide on when to make certain information public. Finally, *limited and protected communication* are required to prevent the damage that constant complete and truthful disclosure of information would do to the fabric of society. Furthermore, it allows the development and maintenance of close relationships and sets necessary psychological distance between the self and the other.

Pedersen [1979] builds on Westin's definition of privacy states by distinguishing between *solitude* (not being observable by others while not physically removed) and *isolation* (being physically removed from others) as well as *intimacy with family* and *intimacy with friends*. He also further differentiates Westin's functions of privacy to *contemplation*, *autonomy*, *concealment rejuvenation*, *confiding*, *creativity*, *recovery*, and *catharsis* [Pedersen 1997].

Autonomy and *concealment* are used for experimentation with new and potentially non-sanctioned behaviors. *Contemplation* is a related concept, as people use it to ponder aspects of their identity, yet is also used to recover from blows to self-esteem. Similarly, *rejuvenation* and *recovery* are used to recuperate from psychological damage to the self, *recovery* involving more contemplation. *Confiding*, *creativity*, and *catharsis* involve the free expression of one's self to others or in works of art. In further work, Pedersen [1999] discovered a connection between the different privacy states and the functions attributed to them.

Solove [2006] claims that privacy enables psychological maintenance as it protects an entity from external threats, like cognitive, affective, or information overload. It can, therefore, provide an environment for stress release, a prerequisite for so-called restorative environments [Kaplan and Kaplan 1989]. Newell [1994] provides a slightly different definition of privacy as *voluntary separation from the public*. She further affirms the necessity of privacy for *psychological maintenance* and *psychological development*, as it provides space and opportunity for experimentation without judgment. This intention to control how others perceive oneself links privacy to impression management.

Privacy as an Expression of Impression Management

Psychologists use the term Impression Management (or self-presentation) to describe behavior that begins when a human being gains self-awareness [Leary and Kowalski 1990]. Starting from that point in time, there is a difference between the image that people present to the outside world and the image that people have of themselves. Formally, it can be divided into two different processes: *impression motivation* and *impression construction*. On the one hand, impression motivation deals with the motivators of self-presentation. Here, people deal with the goal-relevance of impression, determine the value of desired goals, as well as evaluate the discrepancy between the desired and current image. The results of this process lead to impression construction. In impression construction, people not only decide on what image they want to present to a certain target, but rather also how they are going to convey that impression to their target. Furthermore, the intended impression might change depending on the target or the situation a person finds themselves in.

Social rules and norms complicate this behavior. Not only does a person want certain individuals or groups to perceive them in a certain way, but rather certain groups and individuals have expect a certain level of role conformance from individuals. This leads to interesting dynamics in terms of what behavior an individual feels comfortable with in lieu of who is around them, and what kind of behavior they hide from everyone or what behavior they feel comfortable with around certain people.

The pressure of social conformity might even lead to people acting in a way that conflicts with their personal view of themselves in order to prevent the stigma of being misclassified into a certain role. For example, adolescent males within groups of their peers might act in a boastful or misogynistic way contrary to their preference, just so they might not be categorized as a “wuss” or “homosexual” [Bosson et al. 2005]. Therefore, one can interpret curtailing certain behavior to certain instances or environments as a form of risk perception and management.

Risk Perception and Management

Slovic [1987] categorizes perception of risk along two axes: *dread risk* and *unknown risk*. *Dread risk* is felt in situations where people perceive they have little to no control over being in that situation or the outcome of the situation itself. On the other end of the spectrum, people perceive little risk if they assume to have a lot of control over a situation. The other axis, *unknown risk* characterizes risks based on the amount of knowledge that people have about a situation or activity. Thus, having no knowledge increases the amount of risk perceived, while having (or rather, assuming to have) a lot of knowledge reduces the amount of risk perceived.

Describing risk perception along these axes provides an explanation to many lapses of rationality in human behavior associated with dangerous situations. Thus, the risk of dying in a plane crash is oftentimes perceived as much higher than that of dying in a car accident, whereas, in fact, the likelihood of a fatal car accident is much higher than that of a plane crash. This bias can be explained through the potentially catastrophic outcome of a plane crash, the negligible amount of perceived control as the passenger of an airplane, as well as the salience of the outcomes of plane crashes through availability in the media. The latter is known as *availability bias* [Eysenck and Keane 2010].

Conversely, driving a car is a familiar everyday activity for most people, and people assume to have a high amount of skill in conducting a vehicle, establishing a feeling of being in control. Furthermore, the mechanics of a car are much more familiar than the workings of an airplane. These factors combined produce a biased response, resulting in an underestimation of risk of a car accident and an overestimation of the risk of a plane crash.

To make matters worse, our emotions (or affect) influence how we perceive and manage risks [Slovic and Peters 2006]. Positive emotions lead to behavior that attempts to recreate the situations that caused them, whereas negative affect leads to avoidance behavior. Furthermore, affect influences the rationality of decisions being made, as a good part of the emotional appraisal of a situation is subconscious [Eysenck and Keane 2010]. Thus, an ad-hoc affective reaction to a certain perceived risk oftentimes differs from the reaction that results from explicit contemplation of the risk. Moreover, the (automatic) affective reaction if generally faster than a deliberate reaction. This can lead to different outcomes in terms of behavior in cases where there is not time for deliberate contemplation [Slovic et al. 2005].

1.2.2 Privacy-Regulating Behavior

A person's desire for privacy is not always met. These “privacy incidents” can have many possible causes. For example, a person's preference might shift over time, creating a discrepancy between the desired and actual level of privacy within a situation [Altman 1975; O'Connor and Rosenblood 1996]. Alternatively, environmental factors might change a situation, creating a conflict between a person's desired and actual level of privacy [Newell 1994].

Due to the potentially detrimental effect of such privacy incidents, people weigh the costs (or risk) of staying in an environment without sufficient privacy against potential benefits [Newell 1994; Slovic 1987]. While Pedersen found differences in choice of privacy state between personality types [Pedersen 1982], genders [Pedersen 1987], and even place of living [Pedersen and Frances 1990], there are certain common forms of behavior. The simplest form of privacy regulating behavior is the change of activity [Busch 1999; Harrison and Tatar 2008] or location [Newell 1994]. Another common approach to regulating privacy is through the management of social affiliation.

Privacy Regulation through Management of Social Affiliation

One of the most often described forms of privacy-regulating behavior is the management of social affiliation (i.e., a person's availability to others for social interaction). In his seminal work *"Environment and Social Behavior"*, Altman [1975] describes human behavior as a dialectic process alternating between two poles: the desire for social interaction on the one hand and the desire for solitude on the other. Thus, an individual regulates a "boundary" between the self and the public. This Privacy Regulation Theory (PRT), furthermore, provides predictions of what happens once the desired state has been reached. Namely, PRT predicts that once a person achieves a desired state of privacy, that person is then more likely to seek out social interaction. Conversely, if a person desires social interaction while being alone, that person is more likely to seek out privacy after engaging in social interaction.

O'Connor and Rosenblood [1996] set out to verify the predictions made by Altman's theory. They challenged the assumption that privacy is best described as a dialectic process. The results of their study confirmed Altman's predictions in the cases participants were in a situation opposite to the one they desired. Thus, participants in their study were more likely to seek out social interaction if they were alone and desired company. They also tended to seek out solitude when engaged in social interaction while desiring to be alone.

However, contrary to Altman's predictions, participants preferences did not immediately change after achieving the state they desired. Thus, when desiring social interaction, participants were more likely to continue in that engagement for a certain amount of time rather than seeking out privacy. Similarly, people were not more likely to seek out social interaction right after they established solitude, but rather were more likely to stay by themselves for a certain period of time.

O'Connor and Rosenblood liken this behavior to the behavior associated with caloric intake, where no more food will be consumed after the consumption of satisfactory amount. Thus, their Social Affiliation Model (SAM) described affiliation regulation as a homeostatic process where an optimal range of social interaction or solitude is pursued and maintained until over or undersaturation is reached. It is noteworthy that both models provide a prediction of behavior for situations where an individual has the means to achieve privacy. However, it is important to note that neither model accounts for situations in which privacy is desired yet not achieved.

Palen and Dourish [2003] adapt the Privacy Regulation Theory [Altman 1975] and describe privacy as a dynamic boundary-regulation process along three boundaries: the *disclosure boundary*, the *identity boundary*, and the *temporal boundary*. The *disclosure boundary* deals with an individuals choices of what information to disclose to the public and what to keep private. It is not solely to retain certain information, but rather to strategically determine the trade-off involved in keeping the information private and to disclose it should the benefits outweigh the costs. Thus, it is closely linked to the *identity boundary*. The identity boundary is the boundary between the self and the other. More precisely, it involves decisions of what information to disclose to construct a certain impression of self to others and to oneself (see the discussion on impression management in Section 1.2.1). Finally, the *temporal boundary* highlights the influence of past experience on privacy behavior.

However, opportunities for affiliation-regulating behavior can be limited by context-based constraints [Haans et al. 2007]. This can be the case if a person does not have control over a situation [Newell 1994]. Thus, it is not surprising that people strive to exert control not only over situations, but also attempt to assert control over locations. This form of privacy regulation can be found in behaviors of territoriality [Westin 1967].

Privacy Regulation through Territorial Behavior

The ownership of a space, frequently expressed through its personalization [Benfield 2009], provides the benefits of regulating the access to the space, and thus directly allowing for the control of interaction within that space [Westin 1967]. In animals, territorial behavior is a basic mechanism supporting the management of social affiliation and also used to avoid crowding. In effect, animals assert dominance over a certain area and control access to it, attempting to fight off invaders and very reluctantly giving up the space they claimed for themselves. It is even expressed in the distance within which approaching further would trigger the fight-or-flight reflex.

In human beings, territoriality is more complex, while maintaining some of the characteristics of the behavior described above [Westin 1967]. In Western culture, territory has been institutionalized to a certain degree. Ownership of an area, as well as the right to use a certain space for a certain purpose, are the topic of legal agreements between individuals or individuals, the government and other institutions. However, on a social level, ownership of a space can also be asserted by the habitual use of a space, implicitly claiming that place for an individual or a group. There might even be hierarchical rights to the access or use of a particular place, depending on the group owning the place or the place itself.

Another difference between human and animal territoriality is the way places are claimed. For example, Benfield [2009] has observed the behavior of undergraduate students in colleges in respect to their assigned dormitory room. Students claimed ownership of the room (or parts of the room) through personalization (e.g., decoration or personal objects present in the space particular to an inhabitant). Analogous behavior can be found in domestic environments. Inhabitants appropriate physical space according to their needs [Attfield 1999; Harrison and Dourish 1996] and based on the physical dimensions of the home [Pennartz 1999]. They are making the space their own through the objects they introduce into it [Chevalier 1999], reconfiguring the place as their needs change [Harrison and Dourish 1996; Rodden and Benford 2003].

The ownership and control of the space of the home make it a nodal point opposite to public spaces [Short 1999]. Furthermore, different places within the confines of the home can serve different needs, like sanctuary, sustenance, or community [Busch 1999]. As sanctuary they provide opportunities for stress relief and enable psychological maintenance [Newell 1994]. As places of sustenance, they provide opportunities for physiological maintenance [Newell 1994]. Thus, homes are restorative environments [Kaplan and Kaplan 1989]. They play an important part in the creation of individual identity [Short 1999] by providing safe places for self-expression [Cieraad 1999].

Yet the privacy of the home is not without tensions. It also is influenced by the relationships of their inhabitants [Munro and Madigan 1999]. When multiple people live within a home, conflicts arise from the shared use of objects and spaces [Putnam 1999]. Requirements of individuality clash with requirements for togetherness, resulting in complex negotiations of the use of space [Munro and Madigan 1999]. While decisions about space use have become more democratic [Putnam 1999] the roles of parties involved might change over time [Munro and Madigan 1999]. Furthermore, the physical layout of domestic environments can influence how these tensions can be resolved [Munro and Madigan 1999]. This leads to constant (re-)negotiations about the use of shared space and the activities within, as well as the allocation of personal private space to all individuals, if possible [Munro and Madigan 1999].

Furthermore, domestic environments cannot be defined as being strictly the opposite of public spaces [Cieraad 1999] as they also serve public purposes. For example, they play an important part in the creation of social relations with visitors [Short 1999]. Thus, people decorate certain locations in a home specifically to project a particular image to visitors of the space [Chevalier 1999]. This follows the reasoning of Verbeek [2005] who claims that how an object reflects its owner's character is almost as important as meeting the owner's need. Thus, homes reflect the identity of their inhabitants through decorations as well as through the appropriation and adaptation of the spaces within its confines [Wakkary and Tanenbaum 2009]. Requirements of presenting an image of oneself towards the outside can conflict with those of identity creation [Munro and Madigan

1999] due to cultural connotations of the created space [Harrison and Tatar 2008]. Moreover, social relationships influence how a person attributes value to places [Buttimer and Seamon 1980]. As a result, both the physical and social structures within the home are subject to continuous change [Harrison and Dourish 1996; Rodden and Benford 2003].

Similarly, the appropriation of space changes as societies change as a room is not just a space with an amalgamation of objects [Putnam 1999]. Rather, every room in a house comes attached with understandings of appropriateness, expectations, and social norms [Attfield 1999]. Rooms are places rather than spaces [Harrison and Dourish 1996]. Yet, these understandings are neither free of conflicts, nor static. The norms and expectations of different groups of people may overlap [Nissenbaum 2004] or may even be expressed differently [Harrison and Dourish 1996]. Moreover, as societies change, so do the norms for spaces [Harrison and Dourish 1996].

Another tension lies in the appropriation of space itself. The more attached an individual becomes to a space, the more intrusion into that space is perceived as a threat and, as a result, results in its aggressive defense against intrusion [Altman 1975]. Benfield [2009] found an interaction between the amount of personalization of a space and the amount of attachment and sense of ownership of a student to his or her room. Correspondingly, reactions to an intrusion into a less-personalized space were not as pronounced as the reactions resulting from an intrusion into a more-personalized space. This has fascinating effects on how an intrusion into a space is interpreted based not only on the primary use of that space (e.g., a bedroom), but also based on what objects are present in that space.

Thus, the relationship between home and privacy is not a result of its spatiality alone. Rather, it arises through the activities of their inhabitants *within* its confines [Busch 1999]. Thus, its scope is not limited to place alone, but can rather encompass activities, information, decisions, thoughts, and communication [Nissenbaum 2004]. The need for privacy changes with context [Harrison and Dourish 1996] and through the change of attitudes towards it [Busch 1999]. It is apparent that every action within the confines of the home is situated within complex layers of social context [Nissenbaum 2004]. Harrison and Tatar [2008] coin this complex interplay between people, events, and loci (places) as a *semantic tangle*.

1.2.3 The Challenging Nature of Privacy

The previous sections have shown privacy to be a hugely complex area of human behavior. This behavior is subject to large variations based on personal, societal, and cultural differences [Hong et al. 2004]. Individuals have differing attitudes towards privacy, ranging from unconcerned to pragmatic to fundamentalist [Westin 1967]. Furthermore, preferences vary based on a multitude of factors, such as cultural background [Westin 1967], personality and attitude [Acquisti and Grossklags 2004], or age and gender [Radics and Gračanin 2011]. Also, a lot of privacy behavior is inherently context specific [Schaub et al. 2012a] which makes it hard to transfer findings from one context to another [Radics and Gračanin 2011]. Finally, much privacy behavior is still unobserved [Spiekermann and Cranor 2009] and there is still the need for unbiased methods for privacy research to capture behaviors yet unobserved [Patil et al. 2006].

Yet regulating privacy can require both psychological and physical effort [Haans et al. 2007]. Some of this effort stems from the intangibility of privacy as a concept: interests that might jeopardize privacy are far more easily articulated than privacy concerns [Solove 2006]. Individuals have to weigh the benefits of a privacy incident with the perceived costs of its prevention [Palen and Dourish 2003]. Often, this leads to individuals not acting on their privacy concerns [Spiekermann and Cranor 2009]. Yet even with privacy preferences previously specified, individuals tend to make adhoc decisions violating those preferences [Berendt et al. 2005]. As people are pursuing economic rationales or seeking immediate gratification [Spiekermann and Cranor 2009] inconsistencies can be exploited. This goes so far that individuals can be incentivized to deviate from their previously specified preferences when offered relatively small incentives [Christin et al. 2012a].

The introduction of technology complicates anticipating human behavior even further. The embodied privacy-regulation techniques individuals apply in everyday life, which are often inherently spatial in nature, break down due to the difficulty of determining the presence of an entity in the environment, the persistence of information in the digital realm, and the overlapping of different environments [Palen and Dourish 2003]. The *contextual integrity* offered by physical environments is no longer guaranteed as digital information is usually stripped of its context [Nissenbaum 2004].

These characteristics of privacy make it very challenging to pinpoint the implications of privacy for the design of new technology. Specifically we are faced with the following problem:

(P1) Every problem domain can potentially change the expression/perception of privacy.

To address this particular problem, we will need to answer the following question:

(Q1) How can we capture the expression/perception of privacy in a problem domain?

Due to this problem, many — if not all — current systems lack the ability to support nuances in behavior, present a lack of social flexibility, and an inability to support sufficient ambiguity [Ackerman 2000]. Ackerman uses the example of the Platform for Privacy Preferences (P3P) [Reagle and Cranor 1999] to present the 'wicked' problem of having to specify precisely the conditions under which sharing information is desirable. He notes that these decisions, when occurring in everyday life, are effortless and sometimes not even fully conscious. As a result, privacy controls within software systems are inadequate compared to the strategies of individuals in real life. And while individuals adapt their behavior to the properties and capabilities of technology (in a process called *co-evolution*) it does not absolve researchers and designers from the responsibility for the changes in behavior their ideas create [Ackerman 2000]. To address the challenging nature of of privacy for the development of privacy-aware applications, researchers have developed a number of privacy design frameworks.

1.3 Privacy Design Frameworks

Spiekermann and Cranor [2009] present a framework for privacy engineering that centers around the concept of information transfer and situate it within the Federal Trade Commission's Fair Information Practices (FIPS) [Federal Trade Commission 2000]. They outline two different levels of privacy protection: *privacy by policy* and *privacy by architecture*. Privacy by policy systems are systems that provide "notice and choice" as specified in the FIPS. These systems change their functionality based on user requirements. On the other hand, systems designed according to privacy by architecture limit the amount of information captured from users. In these systems the user is either anonymous or at least not linkable to the provided information with reasonable effort. Besides specifying the two different levels of privacy protection, Spiekermann and Cranor also provide guidelines for designing systems on the privacy by policy level.

Poolsappasit and Ray [2008] describe a privacy model geared towards the implementation of location-based services. The model is built around the concepts of requester identity, use of information, temporal constraints, and location. Entities in each of these categories are assigned numerical values between 0 and 1 depending on whether information should be shared or not. Values close to 0 signify a low incentive for sharing the location, values close to 1 a high incentive. The weighted sum of the entities describing a situation can then be used to determine whether the location is to be shared.

Chakraborty et al. [2011] introduce a privacy model that models the tradeoff between quality of service (QoS) of sensor data provided with privacy concerns. The model establishes a trust graph to reflect the privacy requirements of the sensor data source towards different receivers, as well as the QoS requirements and desired data resolutions of the recipients to the source. Depending on the source's trust towards a receiver and that receivers QoS requirements, the source adjusts the accuracy, precision, currency, and completeness of data to be sent to the receiver. Chakraborty et al. provide an implementation in their SensorSafe framework.

Schaub et al. [2012a] introduce a *privacy context model* (PCM) centered around concepts of user, environment, and activity. Their approach suggests a focus on the changes in context relevant to the users' privacy, adapting the behavior of the intended application accordingly. To use PCM for analysis, the model is represented as a directed graph, the nodes being information sources, entities, or "disturbance endpoints" (i.e., privacy violations) and the edges being either observations or disturbances. Thus, any activity (an information source or disturbance endpoint connected to an entity by a path) added to this graph will manifest the privacy implications of that activity.

Colombo and Ferrari [2012] present a framework for the modeling of requirements for privacy-aware systems. Their Modeling and Analysis of Privacy-aware Systems (MAPaS) framework is based on a new Privacy-aware Modeling language (PaML) and is centered around the notion of "purpose". Thus, their modeling language allows to specify the intended purpose of information (i.e., what the information is supposed to be used for), as well as the role and access purpose (i.e., the reason for accessing the information) of a user. The implementation of the MAPaS framework, furthermore, allows for the analysis of the consistency of the specified model.

Beckers [2012] reviews four methods for privacy requirements engineering, including a method of his own. The other methods include the LINDDUN method [Deng et al. 2011], the PriS method [Kalloniatis et al. 2008], and Privacy Engineering Framework by Spiekermann and Cranor [2009] (described in more detail above). According to his review, all of the methods consider *personal information* as the goods to protect. Each of the methods allows the specification of privacy requirements in terms of abstract concepts like *anonymity, unlinkability, pseudonymity, unobservability, undetectability*.

Hong et al. [2004] propose a two-stage privacy risk model as an aid for designers in the creation of privacy-aware ubiquitous computing applications. Their privacy risk models are created through *privacy risk analysis* and *privacy risk management* steps. During the first stage (privacy risk analysis), designers conduct an application-specific analysis of potential privacy risks, identifying the stakeholders and their privacy concerns. In the second stage (privacy risk management), the designers prioritize the risks identified during the analysis and work towards identifying solutions. Hong et al. provide guiding questions for both steps of the process.

1.3.1 Challenges of Privacy by Design

The previous section has shown that there is no lack of frameworks designed to guide the process of building privacy-aware systems. Thus, the question arises why these frameworks have not been able to fully address the challenges of privacy-by-design. A closer examination shows that all of the frameworks have very specific prerequisites for them to be applicable.

The Privacy Engineering Framework [Spiekermann and Cranor 2009] requires knowledge of what data to gather, how to protect it, and what choices to provide to a system user. The data is only ranked based on different degrees of identifiability, from anonymous over pseudonymous to identifiable. Preferences of a user towards the sharing of certain types of data are not taken into consideration. Furthermore, users are given choice only about the use of their data for secondary purposes (i.e., purposes other than the primary purpose of the application). However, the decision what data is required for the primary purpose is left to the designer, regardless of potential concerns of the user. Privacy, therefore, factors into the development only *after* the functional requirements of the application have been determined, leading to the challenges described by Karat et al. [Karat et al. 2005]. In summary, a user would have to weigh the benefits of using an application designed with the Privacy Engineering Framework with the potential costs of future privacy incidents.

In their privacy framework for location-based services Poolsappasit and Ray [2008] posit that the willingness of a person to disclose location information relies on a combination of requester identity, use of information, temporal constraints, and locations. The main factor of a decision in their framework is based on the social distance of the requester to the person to be located. Thus, close relatives are more likely to receive location information than strangers. However, ‘closeness’ is not always a good indicator for the willingness to share information, as shown in [Radics and Gračanin 2011]. Similarly, on the time axis work hours are considered more publicly available than personal time, ignoring the potential tracking and monitoring of work behavior. Finally, quantifying usage and location are problematic, since these values may change with a user’s predisposition, as well as in relationship to the other parameters. Summarily, the quantification of values to identity, activity, time, and location is an attempt to disentangle what Harrison and Tatar call a *semantic tangle* [Harrison and Tatar 2008]. However, the meaning and value of these components are co-created, such that varying one component will affect the valuation of all remaining components.

The SensorSafe Framework [Chakraborty et al. 2011], dealing more generically with sensor data, model the trade-off between quality of service (QoS) and privacy. To that end, they combine privacy concerns about accuracy, precision, currency, and completeness into a single aggregate value. Furthermore, every source of data (i.e., the users) can specify their trust in receivers of data. Lastly, the framework aims to quantify the risk of information leakage by assigning a risk value as the product of probability of disclosure and value of the information. The resulting risk function can then be used as basis of a numerical optimization problem. However, this approach assumes knowledge about all the entities, data sources, and disturbance endpoints that make up the graph used for analysis. Furthermore, the burden of specifying and updating trust values falls to the user of the application. Finally, the aggregation of separate privacy concerns into a single value might conceal a user's high sensitivity towards one of the factors used in the calculation of that value.

Similarly, the MAPaS framework [Colombo and Ferrari 2012] provides a language for specifying and analysis of the consistency of requirements. They follow the approach of purpose-based access control (PBAC), putting the purpose for which data is used into the center of a privacy policy. They distinguish between *intended purposes*, making up the set of declaration of allowed and disallowed purposes and *access purposes* that specify the reasons for the access of data at a certain time. While intended purposes are assigned to data, access purposes are assigned to entities. Thus, the MAPaS framework allows to determine which data may be accessed by which entity. However, while the framework provides the vocabulary to define a model for data and entities within a system, it does not provide guidance for the determination of actual values in the resulting model.

Beckers' Privacy Requirements Engineering method [Beckers 2012], as well as the LINDDUN method [Deng et al. 2011], and the PriS method [Kalloniatis et al. 2008] have the benefit of providing a vocabulary with which requirements for the protection of personal information can be specified. These frameworks distinguish between *privacy goals* and *privacy requirements*. *Privacy goals* are abstract concepts such as *anonymity*, *unlinkability*, *undetectability*, or *unobservability*. *Privacy requirements*, on the other hand, are the actual expression of the privacy goals by a certain stakeholder of the system. The major difference between the frameworks lies in the set of privacy goals they address. However, regardless of these differences, all frameworks fail to provide the means to identify the information that needs to be safeguarded. Neither do they provide guidance in what mechanics to use for the protection of the information. Nor do these frameworks provide concrete strategies for the transformation of privacy goals into concrete privacy requirements. Furthermore, they do not provide any means to find alternatives to their privacy goals.

The Privacy Risk Model by Hong et al. [2004] is the closest to addressing this issue of eliciting privacy requirements. The questions provided for its privacy risk analysis task can help a designer in determining requirements. However, it does not provide the actual means to answer its own questions. Thus, designers could base requirements solely on their own experience, which, due to variations based on personal, societal, and cultural differences [Solove 2006; Westin 1967], is problematic at best. In summary, these observations reveal the following problem:

(P2) Privacy design frameworks rely on concrete, application-specific domain knowledge.

To address this particular problem, we will need to answer the following question:

(Q2) How can we elicit concrete, application-specific domain models?

This problem reveals a dichotomy between our knowledge of the nature of privacy and the prerequisites of the privacy design frameworks. Namely, the information in Section 1.2 is at a much too high level. Thus, while it is helpful knowing that privacy can be described in terms of a *boundary regulation process* [Palen and Dourish 2003], this does not provide a designer with information how that process can be supported. Similarly, understanding that reserve can be used for *impression management* [Leary and Kowalski 1990] shows that people use this strategy, yet does not provide details on when they are using it. Privacy behavior is too often described in abstract terms not specific to a particular environment. This is problematic for informing design decisions, since there is a large variation of behavior and preferences based on different personal dispositions towards privacy [Morton 2013], as well as different activities or locations [Radics and Gračanin 2011]. Since different applications support different activities and target audiences, this presents a *mismatch*. It is unclear how to use this knowledge to help elicit concrete, application-specific *requirements*. In other words, this kind of knowledge is *necessary* for a successful analysis of privacy requirements, as it provides a starting point for the analysis [Shapiro 2010]. However, it does not provide *sufficient* information on how to use this knowledge in the design of privacy-aware systems.

This gap between the abstract knowledge of privacy in terms of motivations, functions, and strategies, and the concrete, clear-cut, domain-specific requirements required by the design frameworks [Shapiro 2010] is an instance of what Ackerman [2000] coins as the *social-technical gap*. A social-technical gap is characterized by the dichotomy between requirements presented by social behavior and the inadequacy of technology to address these requirements. Ackerman [2000] suggests a systematic approach for bridging the social-technical gap in general, yet does not provide concrete details on the approach to use. Shapiro [2010] argues for methods that allow the effective translation of abstract concepts into concrete requirements. Yu et al. [2010] recommend the gathering of social requirements prior to the use of traditional methods. They, furthermore, advocate creating a requirements model specific to the intended system or application. In its essence, this suggests the need for the transformation of unstructured qualitative data into structured information.

However, nuances in privacy behavior based on the semantic tangle of activity, location, time, and identity prevent a high-level approach spanning different domains. Differences in the *social environments* of applications lead to different relationships between stakeholders and different success criteria for the application [Yu et al. 2010]. The *purpose* of an application has a similar impact [Radics and Gračanin 2011]. Thus, in order to bridge the gap between abstract knowledge and concrete requirements, it is necessary to provide support in the eliciting of application-specific privacy requirements [Shapiro 2010]. This leads to the main research hypothesis:

(H1) It is possible to leverage domain-knowledge and requirements gathering approaches to construct application-specific privacy domain models.

According to Yu et al. [Yu et al. 2010], social requirements need to consider the following: the purpose and setting of the proposed system; the stakeholders within the system as well as their intentions and relationships; the current strategies of the stakeholders for achieving their goals; and finally, why these strategies do or do not work. Previous work has shown that these elements need to be domain or even application-specific, as they change with differing environments [Radics and

Gračanin 2011]. Furthermore, the requirements need to capture the diverse laws and practices that regulate privacy for certain applications [Nissenbaum 2004]. Thus we define *application-specific privacy requirements models* (Privacy Model) as follows:

> **Definition *(Application-Specific Privacy Requirements Model)***
> An application-specific privacy requirements model captures the privacy requirements of a specific application. The model reflects the privacy requirements that stem from *purpose* and *setting* of the application. It captures how *stakeholders* and their *relationships* influence their privacy needs. The model furthermore captures *stakeholder's privacy preference and practice* with respect to the application domain. Finally, it models the constraints imposed by *laws*, other *rules and regulations*, *technical constraints*, and *functional requirements*.

However, the question arises how to construct such application-specific privacy requirements models. In particular, it is important to determine the source of the information captured in the model. While information on laws and technical constraints of a problem domain are readily available, the same cannot be said about information on social norms or user preferences and strategies. To elicit information on these aspects, data need to be collected and analyzed. This information needs to originate from the target population of the domain of inquiry. Thus, in order to address the question of how a privacy model can be created, we first have to address Q1.

1.4 Outline

The remainder of this work is structured as follows: We address considerations for the collection of privacy-related information in Chapter 2. Given the resulting data collection requirements, we examine the requirements of a privacy data analysis process and introduce the Privacy Requirements Engineering process (PREprocess) in Chapter 3 and the representational requirements of a privacy domain model in Chapter 4. Chapter 5 provides the methodology for the evaluation of our contributions, which is provided in Chapter 6. Finally, Chapter 7 provides a summary of the contributions of this work, identifies remaining challenges, and outlines future work.

Chapter 2

Considerations for Collecting Privacy Data

As we have shown in Section 1.2, the term ‘privacy’ represents an umbrella term for very complex social behavior. Part of this complexity lies in the fact that privacy preferences and the associated regulating behavior varies across cultures and can even differ from person to person [Westin 1967]. Furthermore, privacy behavior is very context-dependent and changes based on location, activity, and the people involved [Radics and Gračanin 2011; Busch 1999; Palen and Dourish 2003]. To make matters worse, much of privacy behavior falls into the category of *Situated Action* [Suchman 2007]. Thus, people inherently rely on the context in which they are situated to make decisions about privacy. Many of these decisions may not even be fully conscious [Endler et al. 2011].

This poses a significant challenge for the design of privacy-aware systems. As we have seen in Section 1.3.1, privacy-by-design approaches requires concrete domain knowledge to provide guidance for the designer. Yet how can we gain such concrete knowledge, if the very people we build our system for do not have a full grasp of what influences their behavior? How can we get a detailed, complete, and unbiased picture of all relevant actors, artifacts, and interactions for our desired application?

The short answer is: we cannot. As Suchman [2007] remarks, no enumeration of elements constituting a particular context can ever be complete. No approach of gathering data about the application domain will yield completely unbiased information [Hammersley 2008]. Thus, we do not only need "... to understand how things are done under current conditions, why they work or do not work, from whose perspective, and according to what criteria. [Yu et al. 2010, p.4]". Rather, we also need to understand *how* to collect data, *whom* to ask or observe, and how both these choices affect the *validity* of the information we gather.

Therefore, in the remainder of this chapter, we will first examine the fundamental considerations that should go into choosing the approach for data collection. This exploration will allow us to consequently come to an understanding of what factors influence the quality and validity of a data gathering approach, what choices we have in the selection of participants, as well as what actual data gathering methodology to use.

2.1 Fundamentals of Data Acquisition

Data acquisition and analysis are fundamental parts of the scientific method and provide the basis of systematically creating or extending knowledge about the world [Heppner et al. 2008]. Thus, the choice and justification of both data acquisition and analysis methodology requires thorough consideration and documentation. And while both data collection and analysis are intricately linked, they need to be considered separately [Flick 2014]. The development of a plan for the structure of an investigation is referred to as *research design* [Heppner et al. 2008].

One of the major factors in the choice of research design is the field of inquiry and, more specifically, the particular research question that motivates the inquiry [Heppner et al. 2008]. Since we are mainly interested in understanding privacy preferences and behavior in a particular domain, our inquiry focuses on humans and their environments. Research involving humans as either participants or the focus of inquiry have a long history in the social sciences. Thus, it is not further surprising that the topic of research design and methodology has found extensive consideration in those fields (e.g., [Flick 2014; Eysenck and Keane 2010; Hammersley 2008; Heppner et al. 2008]). In terms of data collection approaches, this has created a vast number of available methods with different advantages and disadvantages. Thus, the value of any given approach needs to be evaluated in context of the following question: what approach adds the most value or diversity to the existing corpus of knowledge? [Heppner et al. 2008]. The easiest ways to distinguish between data collection approaches is through the categorization of the questions they are designed to answer.

On the one hand, *quantitative* approaches attempt to measure constructs in the domain of inquiry for hypothesis testing [Heppner et al. 2008]. The data collected is meant to paint a broad picture of the relationship among constructs. Quantitative processes also follow a certain structure [Gubrium and Holstein 2014]. The initial step involves conceptualization and hypothesis building: the researcher defines concepts, formulates arguments about empirical relationships between concepts, and hypothesizes how they are represented in the population. This is followed by data collection and the consequent comparison of 'findings' with the hypothesis. [Gubrium and Holstein 2014].

On the other hand, *qualitative* approaches focus on exploration of phenomena within context, especially in terms of individuals' meaning-making of situations [Heppner et al. 2008]. Thus, qualitative approaches produce significantly different data than quantitative approaches. Furthermore, they differ in the structure of inquiry. While researchers do rely on their preconceptions when conducting qualitative research, those preconceptions represent *working* conceptualizations, *working* definitions, and *working* hypotheses. In other words, they evolve in lockstep with exploring the data collected [Gubrium and Holstein 2014]. This also oftentimes requires data collection and analysis to be done in parallel, as questions arising through analysis might drive further research [Flick 2014]. Thus, contrary to a common preconception, qualitative methodologies should not be seen as a precursor to quantitative research, but rather accepted as alternative, synergistic approaches with unique outcomes [Heppner et al. 2008].

An alternative classification can be made based on whether an approach *produces data* or is simply meant to *collect and examine existing data* [Flick 2014]. In this classification, *interviews*, *focus groups*, *surveys*, *ethnography*, and the like fall into the category of data-producing methods. Here, the data is created either by the researcher, or their creation is at least prompted by a request of the researcher. Existing data can be represented by artifacts like *laws*, *diaries*, *home videos*, or similar objects that have been created without prompting or interaction with the investigator. An alternative view of this classification is the separation of methods into *experiencing*, *enquiring*, and *examining* [Heppner et al. 2008]. This further distinguishes the data-producing approaches into those where the investigator or participant document their experiences (e.g., ethnography) and the approaches where data is produced as a response to a query of the investigator.

Combining the two strata, we can distinguish approaches into those *focusing on subjective experience* (e.g., interviews, diaries), approaches that *focus on describing social situations* (e.g., observation, recording), and those that *focus on implicit or unconscious aspects of social phenomena* [Flick 2014]. Regardless of the classification of approaches, however, an analyst's choice of research design should be influenced by existing knowledge of the domain, the research designs used in the generation of that knowledge, the resources available to the analyst, the advantages and disadvantages of the approaches, an the interaction between all these factors [Heppner et al. 2008].

Ideally, all assumptions and choices regarding the eventual research design should be documented by the analyst. This *bracketing* should convey the analyst's 'lens' to their audience , as well as make the analyst aware of the assumptions that go into the research design, research question, and the (working) hypotheses. [Roulston 2014; Heppner et al. 2008]. However, an analyst also needs to accept the fact that planning and careful deployment of methodology does not guarantee good data [Gubrium and Holstein 2014]. In fact, the 'Bubble Hypothesis' states that all experiments are somehow flawed [Heppner et al. 2008]. This should not be taken as discouragement, but rather as an incentive to possibly use multiple methods that counterbalance their respective disadvantages. Furthermore, this only reinforces the importance of transparency regarding the selection of the research design [Flick 2014].

Before we delve into an analysis of different data collection methods and their applicability to produce privacy-related information, we will first provide a discussion of the criteria commonly used to assess the quality and validity of both the approaches used in data collection and the data they produce.

2.2 Criteria for the Assessment of Quality and Validity of Data

Every argument, whatever the context, lives and dies through the data that supports it. However, the presence of data in and of itself does not signify evidence for or against a claim. Rather, scientists have to show not only that data is present and in support of their claims, but also why those data are applicable for the use in the argument. In other words, scientists have to provide support for why their data (and their argument) are *valid*. Yet what criteria or qualities can be used to determine whether or not data is suitable for a certain argument? Or, conversely, what are the threats to the validity of an argument?

According to Hammersley [2008], questions of validity within social research have been focusing a lot on distinctions between qualitative and quantitative approaches. The main question, in this regard, is whether criteria traditionally applied to quantitative methods can be transferred directly to qualitative methods. Namely, three aspects of research methodology are commonly examined in the evaluation of validity: "...measurement, generalization, and the control of variables." [Hammersley 2008, p. 43]. These criteria have most notably been formulated as a single framework by Campbell [1957]. In the framework, he distinguishes between *internal* and *external validity*. Internal validity represents a combination of measurement validity and causal validity (achieved through the control of variables), whereas external validity is used synonymously for generalizability [Hammersley 2008].

As we have stated before, *measurement* of phenomena represent the central focus of quantitative approaches [Heppner et al. 2008]. Measurement validity relies on both the *reliability* of the measurement process and the *validity* of the measures they produce [Hammersley 2008]. Reliability, in this context, refers to whether or not the data collection method will produce the same results on separate occasions. The validity of a measurement process is concerned with the *findings* of the process and can be broken down based on two separate criteria. First, findings are said to have *convergent validity* if different ways of measurement produce the same findings. Second, if measures of a phenomenon are consistent with actual behavior observed at a later point in time, the findings have *predictive validity*. As such, reliability is a prerequisite to the validity of a process, as inconsistency in the results of a process would lead to inconsistency in the validity of those results.

A related aspect used to evaluate research methodology is the *generalizability* of the findings from the sample selected to the general population [Hammersley 2008]. As investigating the presence of a phenomenon within the entire population is unfeasible, determining generalizability is usually achieved through a combination of statistical sampling and statistical significance tests. Statistical sampling is meant to remove bias from the sampling process[1], whereas statistical significance tests are used to provide a measure for the likelihood of the validity of inferences made.

The last aspect that is commonly evaluated when examining the validity of research methodology is the *control of variables* [Hammersley 2008]. This criterion refers to the degree to which the *independent variables* have been managed in the attempt to determine whether a causal relationship exists between those variables and the *dependent variable*. Therefore, the appropriate control of variables is a requirement for such *causal validity* [Hammersley 2008]. Variables can be controlled through the choice of experimental design [Heppner et al. 2008]. A commonly used strategy is the random allocation of participants to treatment and control groups to avoid any potential bias or noise in the data. An alternative strategy is the statistical control through multivariate analysis [Hammersley 2008]. Moreover, statistical tests are often used to assess outcomes in either case.

It is important to note that these three constructs are not wholly independent. Thus, while experimental control may increases the ability to infer causal relationships (i.e., increased internal validity), this higher amount of control can lead to low generalizability of the findings (i.e., lower external validity) [Heppner et al. 2008]. In contrast, conducting a study in the actual setting of a phenomenon of interest (i.e., a field study) may highly increase the generalizability of the findings, yet at the cost of control over the environment found in a laboratory. Figure 2.1 explores this relationship by contrasting research designs with different combinations of setting and level of experimental control.

As we can see, a *descriptive laboratory study* (i.e., a study which does not use randomization or strong experimental control) scores low in terms of both external and internal validity. However,

[1] We will examine the importance of sampling in Section 2.3 in more detail.

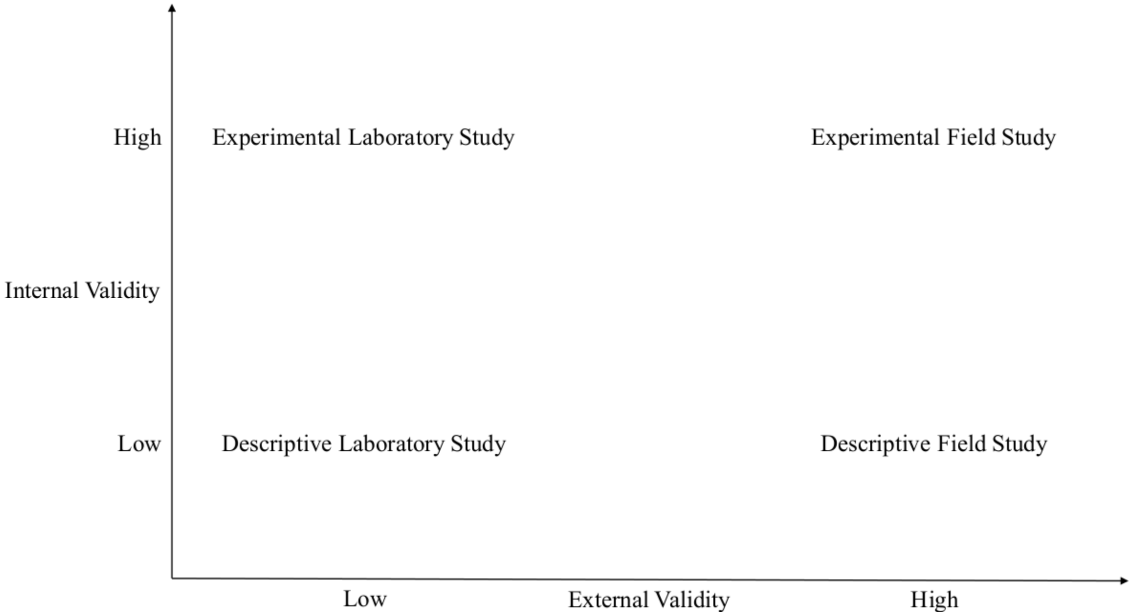


Figure 2.1: Relationship between Validity and Experimental Design (adapted from [Heppner et al. 2008]).

despite its obvious shortcomings, such studies have the advantage of allowing some control over variables, combined with easy data collection and a possible reduction of effect of data collection on participants. Furthermore, they might be the only option, as studying a phenomenon in a real-world scenario may be unfeasible [Heppner et al. 2008].

Descriptive field studies (i.e., studies without experimental control in a realistic environment) provide results that are highly generalizable. They have the further advantage that they may have little to no impact on the participants' behavior (e.g., in case of the retrospective study of routinely collected data) [Heppner et al. 2008]. This comes at the cost of not being able to establish causality.

On the opposite end of the spectrum, *experimental laboratory studies* allow for such inferences, while the generalizability of their results represent a key point of contest [Heppner et al. 2008]. Lastly, *experimental field studies* employ both randomization and experimental while being conducted in the field. Thus, they seemingly have high validity on both axes. However, their external validity is at best only moderately high, since the control of variables make the environment non life-like [Heppner et al. 2008].

In general, we can see that validity represents a continuum on both axes. Rather, *threats* to validity can be seen as such, as “Validity is singular not multiple…” [Hammersley 2008, p. 44]. A study cannot be both valid and invalid at the same time. In other words, the different *types* of validity just highlight different areas of potential errors. These potential errors, then, have to be evaluated in the context of the type of knowledge the study is meant to produce. Namely, the knowledge can be *descriptive*, *explanatory*, and *theoretical*, each with different requirements and threats to validity [Hammersley 2008]. Furthermore, all types of knowledge are interrelated, as descriptive claims are the basis of both explanations and theoretical claims. Additionally, explanations depend upon theoretical knowledge (whether implicit or explicit) [Hammersley 2008].

The validity of descriptions relies on two factors. First, a description can be considered valid only if the features of the phenomena under observation are described accurately. Furthermore, the phenomena need to manifest the features to the degree indicated in the description [Hammersley 2008]. The validity of both explanations and theoretical conclusions rely in large parts on the validity of the descriptions they are based on. In the case of explanations, moreover, the theoretical principles linking them to their descriptions need to be valid. In addition, the choice and application of that theoretical principle has to be correct. [Hammersley 2008] Conversely, theoretical conclusions have to explicitly define the circumstances in which they are applicable. Furthermore, such conclusions need to demonstrate that other theoretical conclusions, in fact, do not apply to those circumstances [Hammersley 2008].

Threats to validity vary strongly based on sources of evidence [Heppner et al. 2008; Hammersley 2008]. For example, accounts of informants can introduce biases (in addition to researchers’ own biases). These biases may be reduced through the use of direct observation, as only the researchers’ biases are present. Yet, at the same time, such biases may also provide additional insight into certain phenomena [Hammersley 2008]. Sources of evidence also vary in terms of the *reactivity* they may introduce. The term ‘reactivity’ describes those variables that affect the phenomenon under investigation [Heppner et al. 2008]. As an example, a participant’s awareness of being observed may result in the altering of their behavior. Thus, it is obvious that existing documents or artifacts collected after the fact (e.g., home videos) have low probability of reactivity, whereas laboratory experiments are much more likely to suffer from this effect [Hammersley 2008].

Thus, it also becomes apparent that assessing validity is crucial irrespective of approach (whether qualitative or quantitative). Moreover, the different approaches of assessing validity do not provide measures of validity, but rather provide evidence for the *judgment* of validity. [Hammersley 2008]. Such judgment inherently requires background knowledge on the topic under investigation, the available data sources, as well as the different methods of investigation. Especially, since any knowledge claim is only valid within its particular framework of assumptions [Hammersley 2008]. This, once again, reinforces the importance of the *bracketing* of both assumptions and methodology employed [Roulston 2014; Heppner et al. 2008]. Furthermore, it is important to understand that the scientific method is designed to *reduce* the threats to validity, yet cannot completely *eliminate* them [Hammersley 2008]. Therefore, the knowledge, training, and skill of a researcher have more impact on the outcome of an investigation than methodology per se [Heppner et al. 2008]. This does not only include a good formulation of a research question or the right choice of methodology, but also the identification and sampling of the target population for the research.

2.3 Identification and Sampling of a Target Population

Determining the constituents of the target population as well as choosing who to involve in the research or design are a central concern both within social science research (e.g., [Rapley 2014; Heppner et al. 2008]) and Software Engineering (e.g., [McDonald 2015; Hartson and Pyla 2012]). These two processes, while intricately connected, required different amount of consideration depending on the type and stage of (research or design) project endeavored. Thus, analysts and researchers involved in the design of new products or spearheading a new direction of research need to put more consideration into identifying the members of the target population than those who work on improving existing designs or continuing existing research endeavors [Hartson and Pyla 2012]. Whereas, for example, a new product requires analysts to brainstorm potential users and research competing products and their users, this step can be skipped (or at least abbreviated) given an existing product, as the current users of the product constitute an obvious choice for the target population of ‘user research’ [McDonald 2015].

Before discussing what considerations need to be made in the process of defining the *target population*, identifying an available *participant pool*, and finally selecting a *sample* from that participant pool, it is necessary to clarify what is meant with each of these terms. Technically, the term ‘population’ refers to observations of people, not to the people themselves [Heppner et al. 2008]. In practice, this results in populations being defined in terms of the characteristics of people. We can further distinguish between *hypothetical* populations (i.e., potentially infinite set of theoretically possible values of the chosen characteristics) and *real* populations (i.e., set of the actual observations of the chosen characteristics) [Heppner et al. 2008]. Given the selection of the desired characteristics that define the target population, the researcher then has to identify people who fit said characteristics and are accessible. This group of people is referred to as the participant pool [Rapley 2014]. Note that it might be necessary to test whether a person is part of the population or not [Heppner et al. 2008]. Finally, the group of the actual participants selected from the participant pool based on a certain sampling strategy represents the sample.

Each of the three steps — defining the target population, identifying the participant pool, and selecting the sample — has the potential of introducing *bias* [Heppner et al. 2008]. Thus, background knowledge and prior research are invaluable to limiting bias introduced by the researcher [Rapley 2014]. However, as the sample is restricted to voluntary participants, it is impossible to completely avoid bias. Thus conscious choice and documentation of the sampling strategy is important.

2.3.1 Sampling Strategies

In general, sampling strategies can be divided into three different approaches: *total population sampling*, *probabilistic sampling*, and *purposive sampling* [Rapley 2014]. As the name suggests, total population sampling means the use of the entire participant pool as the sample. In other words, every possible participant is selected. Obviously, this sampling strategy is rarely available, as participation is voluntary and both access to the participant pool and resources might be limited [Heppner et al. 2008].

Probabilistic or *random sampling* is the strategy of choice for quantitative research [Rapley 2014]. It is used to avoid bias in the selection of participants. However, there are caveats attached to the use of random sampling. First, random sampling relies on comparatively large samples, since large numbers are required to limit sampling errors [Rapley 2014]. This is exacerbated should the target population be highly diverse or should the phenomenon of interest exhibit high variance among the population. Thus, sample size has to be increased to counteract these irregularities. Furthermore, probabilistic sampling does not guarantee that the selected sample is representative of the population as a whole [Heppner et al. 2008]. Nor can it be assumed that the phenomenon of interest is randomly distributed within the population [Rapley 2014]. Limited access to the desired participant pool might further limit the applicability of random sampling. Thus, there are different approaches for selecting a random sample from the participant pool (shown in Table 2.1).

Table 2.1: Probabilistic Sampling Strategies

Name	**Description**
Simple random sampling	Selection of participants entirely at random.
Sequential sampling	Selection of every nth participant.
Stratified random sampling	Random selection of participants from partitions of the participant pool formed through application of relevant criteria.
Multi-stage sampling	Selection of participants in multiple stages for the subdivision of large clusters.

Another boon of probabilistic sampling is the fact that it allows to establish a direct relationship between the size of a sample and the statistical power of the findings [Heppner et al. 2008]. In other words, we can establish how many participants we need to achieve a specific likelihood (or alpha value) of rejecting the null hypothesis should the alternative be true as well as detecting an effect should it be present. Both power and sample size are further tied to the statistical test used, its directionality (i.e., whether deviation is detected in only one or both directions), and the estimate of the strength of the phenomenon in the sample (effect size). Determining these values, however, requires knowledge of the phenomenon under investigation as well as the characteristics of the target population [Rapley 2014].

Unlike quantitative research, qualitative research often is interested in particular — even biased — perspectives [Rapley 2014]. This is but one possible case in which random sampling is not desirable, but rather particular choices need to be made in selecting participants. These approaches are referred to as *purposive sampling* or *purposeful sampling* approaches. Both Coyne [1997] and Patton [1990] provide very thorough discussions of different rationales for the use of purposive sampling. Table 2.2 highlights Patton's categorization of different purposive rationales.

Table 2.2: Purposive Sampling Strategies according to [Patton 1990].

Name	**Description**
Atypical case sampling	Selection of atypical or extreme cases from the participant pool (also: extreme or deviant sampling).
Typical case sampling	Selection of typical or common cases from the participants.
Intensity sampling	Selection of a sample that promises extensive amounts or rich, high-quality data.
Heterogeneous sampling	Selection of participants that are as different as possible (also: maximum diversity or maximum variation sampling).
Homogeneous sampling	Selection of participants based on similarity to each other.
Criterion sampling	Selection of participants based on predetermined criterion.
Stratified purposeful sampling	Selection of participants based on multiple selection criteria.
Purposeful random sampling	Purposeful selection of small random sample.
Quota sampling	Selection of participants to fulfill quota of selection criteria.
Theoretical sampling	Selection of participants based on likelihood of presence of a theoretical construct (also: operational construct sampling).
Snowball sampling	Sequential selection of participants based on previous samples (also: chain sampling).
Confirming/disconfirming sampling	Selection of participants with the purpose of confirming or disconfirming existence of phenomenon.
Critical case sampling	Selection of participants that that will immediately prove or disprove existence of phenomenon.
Political sampling	Selection of participants to fulfill obligations or external requirements.
Opportunistic sampling	Undirected selection of participants based on events during research (also: emergent sampling).
Convenience sampling	Selection of participants based on convenience and availability (also: maximum availability sampling).

Among these strategies, many are very relevant to researching privacy phenomena. Thus, heterogeneous sampling can be useful to get a good overview of behavior within the target population without requiring large sample sizes. Homogeneous sampling, in contrast, can be used to elicit in-depth information about a subsection of the population. Finally, theoretical sampling plays an important role in the validation of newly formed concepts. Furthermore, it can be used both data-driven (i.e., in an iterative fashion, building on data collected) and model driven (i.e., for the confirmation of hypotheses based on prior data) [Rapley 2014]. In contrast, both opportunistic and convenience sampling should be used as last resorts, since they provide little to no justification for claims made from the data collected.

One of the downsides of purposive samples, however, are their relative subjectivity and the resulting introduction of bias [Heppner et al. 2008]. Thus, identifying the characteristics of the population and the selected sample are of utmost importance. One possible way of increasing the external validity of claims made based on purposive samples is the use of *factorial design* [Heppner et al. 2008]. Factorial design refers to the grouping of participants based on a 'status variable', which allows detection of interaction between that variable and the phenomenon under investigation. However, it is impossible to account for all potentially influencing variables, thus requiring a prioritization among status variables. Furthermore, the measurement of an influencing variable might not be straight-forward or even possible [Heppner et al. 2008]. Moreover, the power of factorial design relies in part on having equal numbers of participants in each 'cell' of the design. This has the potential of introducing bias, if groups are not equally present in the target population [Heppner et al. 2008].

Thus, once again, documentation of choices and population characteristics are of utmost importance to provide evidence for the validity of the collected data based on the sample selected [Heppner et al. 2008]. It is, furthermore, clear that no perfect choice exists. However, "It is enough to make good, analytically driven, thoughtful, decisions." [Rapley 2014, p. 55]. These decisions require the researcher or analyst to acquire knowledge about the target population and the phenomena of interest. This results in an iterative relationship between sampling, data collection, and analysis in order to generate the knowledge desired [Rapley 2014].

The software design process adds additional considerations to the selection of participants in the development of an application that are not generally present in purely academic research. This is a result of the acquisition of knowledge itself not being the main motivation of the data collection.

2.3.2 Stakeholders in Software Design

The differences between participant selection in a research endeavor and software development start with different terminology. While in research design, we are talking about research *participants*, software engineers are concerned about *stakeholders*. Thus, what we have referred to as participant identification and selection is generally referred to as *stakeholder analysis* (e.g., [McDonald 2015; Bjørner 2006]). However, the term 'stakeholder' also includes more than just the eventual users of the application under design. Especially in a corporate or industrial setting, stakeholders can include anyone from management to purchasing, with different influence, values, and needs [Hartson and Pyla 2012]. This is reflected in the following broad definition:

> "[Stakeholders refer to] A group or individual with a relationship to the change, the need, or the solution." [McDonald 2015, p. 16]

The need, in this case, refers to any problems or opportunities of a person within the target domain, whereas a solution addresses such a need. The change, then, is what is necessary to transform said needs into solutions. The above definition may even include members of the analyst's or designer's own team or organization, as the may have influence on the development of the desired application. Thus, it is necessary not only to identify the users (or target population), but rather also the social structures surrounding those users. Due to finite resources, this makes it necessary to *manage* various stakeholders [McDonald 2015]). One possible approach to this is through the use of a *stakeholder map* (see Figure 2.2).

A stakeholder map allows an explicit discussion about the importance and influence of various stakeholders or stakeholder groups for the design project. It further allows to manage the design team to prioritize resources based on the quadrants of the map. For example, stakeholders from within the 'manage closely' quadrant should represent the top priority, and may even represent

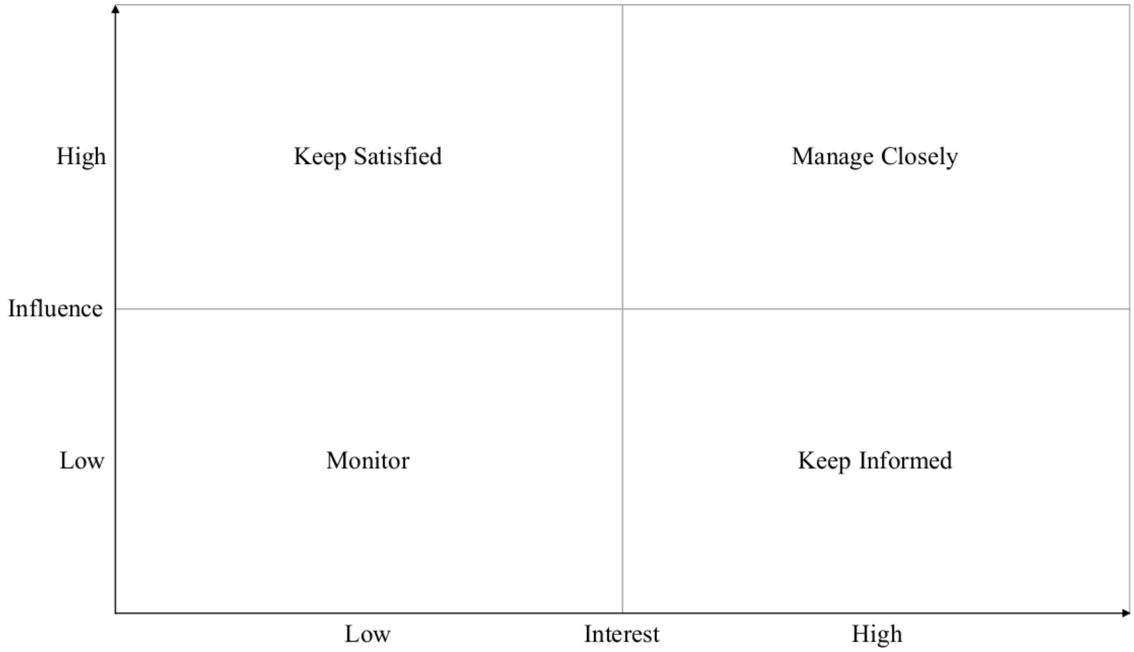


Figure 2.2: Stakeholder Map (reproduced from [McDonald 2015]).

invaluable additions to the design team [McDonald 2015]. On the other end of the spectrum, stakeholders in the 'monitor' quadrant play little to no role within the design process, unless their influence or interest changes. A similar technique is the use of a *commitment scale* to compare the actual involvement of stakeholders within the project with the involvement that is required for the success of the project [McDonald 2015]). Thus, the stakeholder groups can be ranked ranging from 'hostile' to 'enthusiastically supportive'. The commitment scale, furthermore, allows similar planning of engagement of stakeholder groups as the stakeholder map, since discrepancies in desired and actual involvement identify regions in need of improvement.

There are many reasons to examine all stakeholders and not just the intended users of the system. Different stakeholders might provide additional and significantly different perspectives from those of the actual users and thus should be considered when selecting samples. Furthermore, and more importantly, certain stakeholder groups may have the potential to influence the viability of certain sampling and data collection methodologies. For example, management might restrict access to key users that would contribute invaluable information to the design process, should data collection detract from the work of those key users [Hartson and Pyla 2012]. Thus, it is important to choose wisely which data collection method to use, both in terms of required time and effort (both for participants and analysts) and in terms of the data they produce. In our case, it is furthermore vital to gauge the utility of different data collection methods for the capturing privacy data.

2.4 Data Collection Methodologies

As we have mentioned before, data collection methodologies can be categorized by the focus of their inquiry into methods of *experiencing*, *enquiring*, and *examining* [Heppner et al. 2008]. However, these categories do not have clear-cut borders, since many methods use aspects of more than one category. We have further seen, that we can distinguish between experimental (quantitative) methods and descriptive (qualitative) methods. Thus, the choice of data collection method ultimately relies on the research question (i.e., the information that is sought). Different data collection methods provide different perspectives and generate different data [Heppner et al. 2008]. More precisely, they fall on different locations within the continuum from emic to etic data [Stewart et al. 2009]. *Emic data* can be seen as data arising 'naturally' from the phenomenon itself, without influence or structuring by the investigator. On the other end of the spectrum, *etic data* arises from the structure imposed through the investigator and the data collection method.

Traditionally, interviews, focus groups, and observations (and their resulting transcripts) have been used in social science research [Flick 2014]. More recently. the collection of video or audio data, along with other, sometimes *virtual* data have become more common. These approaches have also been adopted by the human-computer interaction (HCI) community (e.g., [Hartson and Pyla 2012; Dourish 2006; Rosson and Carroll 2002]). Due to the large amount of choices and the important implications of the choice of data collection methodology, we will therefore provide an overview of some of the most common methods.

2.4.1 Interviews

Interviews are among the most commonly used data collection methodologies and represents a for of *inquiry* [Flick 2014]. They can be seen as a form of self-report of the interviewee [Heppner et al. 2008]. However, they also have a collaborative aspect, as interviewer and interviewee jointly explore the phenomena of interest [Wang and Yan 2012]. In other words, interviewer and interviewee co-create the information through their interaction [Heppner et al. 2008]. Interviews can be categorized into *structured*, *unstructured* and *semi-structured* interviews [Heppner et al. 2008].

In *structured interviews*, the interviewer determines both the questions and their order before the interview. An important aspect of these types of interviews is the fact that the interviewer does not ask follow-up questions. In this regard, the interviewer takes a neutral stance, serving only as impartial recorder of the answers of the interviewee, not providing valuation or any kind of feedback to the interviewee [Heppner et al. 2008]. This usually goes hand-in-hand with the use of a-priori protocols for the classification of answers. The advantage seen through adopting the highly structured format is a minimization of variation within the answers. Furthermore, the lack of feedback by the interviewer avoids the introduction of potential bias. At the same point in time, it can be argued that — due to their inflexibility — they shape the data according to the hypotheses of the investigator, thus producing inherently biased responses [Heppner et al. 2008]. The pre-determined questions also do not adapt for differences in language use between investigator and participant. Lastly, the neutral stance creates distance between interviewer and interviewee, limiting the chance for eliciting affective responses. [Heppner et al. 2008].

On the opposite end of the spectrum, *unstructured interviews* explicitly allow — even encourage — follow-up questions. This can go to the extent that the interview is shaped more like a conversation about a topic, with little to no questions being determined a-priori [Heppner et al. 2008]. However, while this structure allows the interviewer to adapt to different participants, the approach is not without dangers. For example, it requires considerable skill to avoid shaping responses by cueing based on the interviewer's hypotheses of the phenomena of interest. Furthermore, the characteristics of the interviewer or interviewers are likely to influence the responses of participants. These characteristics include things like personality, gender, or position of the interviewer; the power-relationship between interviewer and interviewee; or the personal dynamic between multiple interviewers [Wang and Yan 2012]. Thus, it is important that the interviewee drives the narrative in these types of interviews, capturing their voice and point of view [Heppner et al. 2008]. This, in turn, leads to wide variations between the data contributed by different participants.

Finally, *semi-structured interviews* strike a middle ground between structured and unstructured interviews. In semi-structured interviews, the investigator does create pre-defined questions to allow for increased consistency within the answers, potentially even providing an order in which the interviewer should ask the questions [Heppner et al. 2008]. However, the interview is shaped more like an unstructured interview, encouraging follow-up questions and deviation from any order for the sake of more salience within the collected data. Thus, semi-structured interviews attempt to provide a compromise between the consistency achieved by structured interviews and the salience of unstructured interviews.

Regardless of the type of interview, the structure of this data collection method stays the same. Heppner et al. [2008] describe this process in six steps. First, the researcher has to gain access to the participant pool. In other words, researchers need to engage potential participants and negotiate their participation in the interview process. This step goes hand-in-hand with the familiarization of the researcher with the context, culture, and language of the target population. Without such preparations, the interviewer might ask questions in a way that run afoul of participants' cultural values. Furthermore, without understanding the idiosyncrasies of the language used by participants, the interviewer might simply not be able to understand the participants, or even misunderstand them. Gaining access to the population and initial interaction with the target population (as well as later interactions) are heavily influenced by the self-presentation of the researcher. As we mentioned before, participants may react and answer questions differently based on the characteristics of the interviewer. Thus, the researcher has to make a conscious decision about what image to present.

The previous three steps are a requirement to be able to identify the *key informants* within the participant pool. Identifying these individuals serves two purposes. First, they are needed to provide information on which researchers can base their sampling decisions. Second, they themselves often represent invaluable sources of information as interviewees. Throughout these steps, it is important for researchers to build rapport with the people they encounter, regardless of whether they represent key informants or potential interviewees. Gaining an interviewee's trust will improve the chance of an honest and descriptive response — especially when considering sensitive topics like privacy. However, interviewers have to make certain that building such relationships do not cloud their judgment regarding the phenomena of interest by taking on the point of view of the interviewees. Finally, an important decision concerns the means and environment of data collection. Different media, for example, can influence the strength of rapport. For example, face-to-face interviews allow for stronger inter-personal relationships than phone interviews. Furthermore, the means of capturing the interview influences the quality of data. Commonly, audio recordings are used, with video recordings becoming more common. Neither of these approaches, however, obviate the need for taking field notes, capturing immediate thoughts and reactions of the interviewer.

One of the main advantages of interviews is their flexibility [Heppner et al. 2008]. Thus, they can be used for both quantitative and qualitative research. This flexibility stems from the ability to tailor questions asked to the information needs of the researcher. A *how* question will yield different results than a *what* or *why* question [Gubrium and Holstein 2014]. Heppner et al. [2008] further differentiate questions based on their purpose. *Background questions* prompt the participant to provide information about themselves and their context. *Behavioral questions* serve as a prompt for information about certain activities or interaction of participant. Interviewees can further be asked about their *opinions or beliefs*, as well as their *feelings* about certain phenomena or cues. Moreover, *knowledge questions* can be used to query interviewees for information about their practice (whether work or private) or information on the qualities of phenomena. *Sensory prompts* can reveal details about the sensory experience of participants, whereas *experiential questions* can serve as a source of information on past or present experiences of the participants.

Other advantages of using interviews are their interactivity [Heppner et al. 2008]. Especially in unstructured or semi-structured interviews, the interviewer can react and adapt to the responses of the interviewee. This allows to collect very detailed accounts of the interviewee's experience.

Furthermore, this human-human interaction allows the interviewer to contribute observations of the interviewee to the corpus of data [Heppner et al. 2008]. Lastly, interviews have the advantage of often eliciting a relatively high response rate.

One of the major disadvantages of interviews, however, is their high time requirement [Heppner et al. 2008]. As we have seen in the description of the interview process, a good interview requires a lot of preparation. Furthermore, depending on the amount of questions asked and the format of the interview, the time cost for interviewees can be a deterring factor for participation. In this regard, the less structured an interview, the more time it takes to both collect and to organize the data.[Heppner et al. 2008]. This raises additional challenges in terms of data management [Roulston 2014]. In addition, interviews often raise additional question, requiring follow-up interviews [Heppner et al. 2008]. The medium used for interviewing can influences these factors. For example, phone interview tend to be shorter and generate less information. The latter can also be counted as a disadvantage. Furthermore, they lead to a loss of some inter-personal channels and tend to result in a lower response rate [Heppner et al. 2008].

However, the probably most important disadvantage of interviews in regards to eliciting privacy data is the fact that — due to the direct interaction between interviewer and interviewee — discussion of sensitive topics tends to be difficult [Heppner et al. 2008]. Thus, a lot of time and effort has to be put into studying the culture of the target population. Moreover, the choice of interviewer and their presentation towards the interviewee will heavily influence responses. Establishing trust between interviewer and interviewee, thus, is a crucial factor. These factors, furthermore, reveal that, in order to elicit high-quality data, the interviewer has to be well trained and skilled [Heppner et al. 2008]. Without training, the chances of incorrect use of procedure can severely devalue the data collected [Roulston 2014].

That being said, the depth of information created in combination with their versatility make interviews perhaps the most commonly used data collection method [Flick 2014]. Furthermore, they are often used in combination with other data collection methods (e.g., in combination with *ethnography* in *contextual inquiry* [Hartson and Pyla 2012]). Lastly, they can also be used to elicit information from groups. Group interviews are usually referred to as *focus groups*, and require somewhat different considerations than single-participant interviews.

2.4.2 Focus Groups

Stewart et al. [2009] describe focus groups as group discussions with focus on a particular topic. As such, they have a long history of use within market research and can be used to diagnose particular problems within a product [Heppner et al. 2008]. In terms of 'pure' research, focus groups are useful for the exploration of a phenomenon of interest, and are thus mostly used early-on in the investigation of a phenomenon [Stewart et al. 2009]. Similar to interviews, they produce a rich body of data in the participants' own words through the interaction of interviewer and participants. This similarity is due to the almost identical structure of the procedure Focus groups require additional consideration regarding the research question driving the inquiry [Stewart et al. 2009]. Furthermore, since they involve a group of people, the sampling of participants becomes more challenging.

The first consideration regarding the chosen sample are based on the type and amount of data desired. These characteristics influence the choice of the number of participants per group, the number of groups, as well as the types of questions asked [Stewart et al. 2009]. Furthermore, while focus group members in marketing research were traditionally strangers, purposive sampling is much more desirable [Heppner et al. 2008]. Whereas heterogeneous sampling may be conducive to the broad coverage of the phenomenon of interest, care should be put to maintain somewhat homogeneous groups. Including members from vastly different socioeconomic circumstances or cultures within the same group can give rise to problems and devalue the data collected [Stewart et al. 2009]. Thus, it may be appropriate to sample participants based on existing groups within the target population [Heppner et al. 2008].

A lot of care must also be put into anticipating (and potentially managing) the group dynamics present in the selected groups [Stewart et al. 2009]. While the interactions between group members represent one of the major selling points of the focus group format, the interviewer (or moderator) needs to make sure that minority opinions are not suppressed by the majority [Heppner et al. 2008]. However, the interventions by the moderator may also influence the type and quality of the responses [Stewart et al. 2009]. Thus, the moderator has to be aware of the purpose of the research, especially regarding the type and specificity of information sought, as well as the reasons for collecting it. Furthermore, it is important to note that the number of question per time allotted influences quality of the responses [Stewart et al. 2009].

Whereas more care is required in the selection of participants, one of the advantages of focus groups is the fact that the viewpoints of multiple participants are captured at the same time, thus making them more economic than interviews [Stewart et al. 2009]. Furthermore, focus groups stand out from other data collection methods through the fact that they capture the collaborative building of meaning by participants. The social context of interacting within a group is also considered to lead to honest and rich responses [Heppner et al. 2008]. Focus groups tend to be very flexible in terms of topics, individuals, and settings, although there may be variation based on the chosen topics [Stewart et al. 2009]. As they are often conducted in specialized environments, they also allow for collaboration of multiple researchers in observing and managing the group [Stewart et al. 2009].

The social construction of meaning, however, can also limit the generalizability of results, as interviewees may feel social pressure to conform to the majority opinion [Stewart et al. 2009]. Furthermore, the dominance of one or more members of the group can lead to the lack of participation by more reserved members. Unless video recordings are used, the non-verbal communication between group members is lost [Stewart et al. 2009]. The use of video recordings, however, adds to the already large amounts of data, resulting in longer time requirements for analysis [Heppner et al. 2008]. Finally, focus groups require highly skilled moderators trained in group dynamics in addition to the skills required by an interviewer [Stewart et al. 2009].

In terms of utility for capturing privacy data, focus groups have similar limitations to interviews in terms of broaching sensitive topic. However, in focus groups, being able to elicit valid responses not only depend on the self-presentation of the moderator and the rapport between one person, but multiple people. Furthermore, group dynamics might contribute to the strength of potential taboos of talking about certain topics. Yet, at the same time, the presence of a group and the social construction of meaning might make conscious aspects of behavior that may not surface with a single interviewee, as they may be subconscious. Moreover, for the concept of *community privacy* [Kafura et al. 2011], it is vital to survey the viewpoint of the community or groups within a community. Thus, the lack of anonymity and the presence of multiple people within a focus group represent both an advantage and disadvantage. When looking for a data collection methodology with high levels of anonymity, surveys may be suited best.

2.4.3 Surveys

Surveys, just like interviews and focus groups, are counted among the data collection methods used for self report as well as inquiry [Heppner et al. 2008]. As the name suggests, surveys have the goal of analyzing the nature or frequency of a phenomenon within a target population. They are commonly used in both qualitative and quantitative studies, however it is noteworthy that, contrary to experimental approaches, surveys are not well suited to manipulate an individual variable [Heppner et al. 2008]. Most commonly, surveys employ self-report questionnaires as data collection instruments, yet are not bound to a specific medium. Thus, like interviews, surveys can be conducted over the phone. Furthermore, they can be distributed through mail or the internet, where the latter gains more and more popularity [Heppner et al. 2008]. Thus, surveys are often used in early stages of researching a phenomenon of interest, as they can be useful to identify characteristics of target populations.

As a method of inquiry, surveys share a lot of procedural steps with interviews and focus groups [Heppner et al. 2008]. Thus, just like it was the case with interviews and focus groups, formulating the research question represents the initial step of survey design. This step is followed by determining the target population and participant pool, as well as initial decisions about the sample to be taken. Given the target population and research question, survey researchers have the option of either selecting an existing survey 'inventory', or developing their own [Heppner et al. 2008]. Once questions have been selected, the investigators have to decide which medium to use for data collection. Irrespective of medium, the lack of previous interaction with members of the participant pool can result in relatively low response rates, particularly with mail surveys. Internet surveys appear as a convenient solution to this issue. However, this method potentially biases the sample to people with Internet access [Heppner et al. 2008].

The main advantages of survey-based research are that surveys are relatively easy to administer and have the potential to reach otherwise inaccessible population groups [Heppner et al. 2008]. Furthermore, they allow for the collection of data from a larger data than is the case with interviews and focus groups, as they do not require as much time and resources from the researcher. Similarly, compared to the other forms of inquiry, survey research requires significantly less training [Heppner et al. 2008]. Researchers can reduce time requirements even more by selecting questions from existing (and potentially tested or verified) inventories. Since they do not require face-to-face interaction, surveys also afford participants with confidentiality or even anonymity, given that the questions asked do not reveal their identity to the researchers.

However, the lack of interaction between researcher and participants are also one of the drawbacks of using surveys. Similar to the issues stemming from a neutral stance in structured interviews, the lack of interaction with a researcher may lead to a lack of trust on the side of the participants [Heppner et al. 2008]. This may negatively influence the veracity or quality of answers provided, especially regarding sensitive topics. On the opposite end of the spectrum, the lack of interaction with the researcher also may distort participants' responses, as they may try to 'help' the researcher, try to guess the research question, or try to make themselves 'look good' [Heppner et al. 2008]. Furthermore, the lack of rapport between researchers and potential participants is reflected in the challenge of recruiting respondents. This makes it hard to determine whether the resulting sample of the participant pool is representative of the population as a whole [Heppner et al. 2008]. Finally, while survey research may not require as much training as interview or focus group research, much care has to be put into all decision made. This is especially true in the design of questions, as the researcher does not receive any feedback about misunderstandings and has no option to correct or clarify should there be any issues.

Regardless of these drawbacks, surveys have their place in the toolbox of a privacy researcher. As mentioned before, surveys have the unique ability of providing the participant with anonymity, which may alleviate concerns about discussing topics of a sensitive nature. Furthermore, given the relatively ease of distribution and their potential to reach a lot of people, surveys are useful to capture aspects of phenomena across large populations. However, at the same time, the lack of interaction with participants limits their usefulness for delving deep into the characteristics and motivations of privacy phenomena. This is partially offset by an increased likelihood of encountering evidence of contextual factors that may influence privacy behavior that many participants are not consciously aware of within the responses (e.g., [Radics and Gračanin 2011]). However, like interviews and focus groups, surveys only allow to ask questions about the past or hypothetical future situations. Yet privacy behavior is highly contextual, which limits the value and validity of these types of information. Observations represent a potential alternative for this issue.

2.4.4 Observations

Behavioral observations are performed by trained observers who record their observations of the overt behavior of the study participants [Heppner et al. 2008]. Thus they are collections of the first-hand experiences of the phenomenon of interest by the observers, as opposed to retrospective accounts given by participants. There are a wide variety of approaches to observation with varying levels of observer involvement [Heppner et al. 2008]. On the non-interventional side of the spectrum, the *complete observer* is undetected by and unknown to participants, providing a ‘fly on the wall’ insight into the phenomena of interest. However, complete observation is ethically challenging and hence employed very rarely. A more common approach sees the *observer-as-participant*, where participants are aware of the observer in their midst, but there is no interaction between participants and observers. Interaction between observer and participants occurs when the *participant-as-observer* approach is used, where either the observer takes an active role as a participant, or a participant is chosen to fill the role of observer. Finally, in some cases the observer is a *complete participant*, meaning they were part of the group under observation before the study started. Early observational studies were strictly non-interventional, whereas *ethnographical* approaches (i.e., participant-as-observer) are most common today [Heppner et al. 2008]. Observational studies allow the observer to thoroughly conceptualize the phenomenon through extended, deep exposure. Furthermore, observation allows the observer to engage with a phenomenon both on an intellectual and emotional level, providing a more complete image of the phenomenon of interest [Heppner et al. 2008].

Procedurally, thus, an observation study starts with the selection of the phenomenon to observe within an identified target population [Heppner et al. 2008]. This requires extensive background knowledge of the target population to allow the choice of the right participant pool and sample. Observational studies almost exclusively employ purposive sampling. Depending on the phenomenon of interest, researchers may look for typical or atypical cases, highly salient cases, homogeneous or heterogeneous groups, or even critical cases. Before observers can enter the field, they need extensive training. First, they need operational background knowledge to be able to detect the phenomenon of interest as well as distinguish between important and unimportant behavior [Heppner et al. 2008]. Furthermore, observers need to be trained to capture detailed observations without premature analysis and from the perspective of the participants.

Given a well defined focus, a desired participant pool and sampling strategy, as well as highly trained observer, access to the target population needs to be gained. Depending on the chosen population and phenomenon, a different degree of involvement may need to be chosen [Heppner et al. 2008]. Moreover, the time, duration, and frequency of observations needs to be decided. Provided all these preparations have been completed and the observer or observers have gained access to the participants in the field, data collection can commence. One of the most important aspects of this part of the process is the creation of field notes containing the descriptions of time, environment, activity, and actors, along with the phenomenon of interest. The level of detail of these captured notes raises or lowers the value of the data. Furthermore, care needs to be taken to separate the thoughts, intuitions, and analyses of the observer from the observations during memoing [Heppner et al. 2008]. Therefore, audio and video recordings of the participants' behavior may be chosen to supplement the observers' field notes.

One of the main advantages of observations is the embedding of the observer into the context of the phenomenon of interest [Heppner et al. 2008]. Thus, instead of receiving a second hand account of the context, the observer can capture it directly. Moreover, participants may not be aware of the significance of parts of their behavior, which an observer may pick up on. Thus, it reduces the bias found in self reports where participants may only report what they find important.

However, while it reduces bias originating from participants' accounts, it introduces the potential of bias from the observer's perspective. Furthermore, the observer — while being a source of objectivity regarding the behavior of participants — introduces an element of subjectivity through the decisions to record certain events as an instance of the phenomenon and to discard others. This issue can be mitigated by employing multiple observers, raising the resource cost as a result. More importantly, observations can only be performed if the phenomenon of interest is actually directly observable [Heppner et al. 2008]. Thus, any internal considerations of participants is lost in observations. Finally, one has to question the representativeness of the behavior captured as many factors, such as the time or circumstance of the observation as well as reactivity from the participants' awareness of being observed, could influence the generalizability of the sample [Heppner et al. 2008].

This last point also lowers the value of observations for the collection of privacy data. It is well documented that people's privacy-regulating behavior changes given the presence of an observer or observation device (e.g., [Choe et al. 2012; Schaub et al. 2012a]). Thus, only a *complete observer* could assume to capture 'real' privacy behavior. However, in virtually all circumstances, such an approach would be highly unethical and thus infeasible [Heppner et al. 2008]. Not to mention that such observations would completely rely on the interpretation of the observer. One possible way of mitigating the reactivity introduced by an observer is through the use of *ethnographic* approaches.

2.4.5 Ethnography

The term ethnography describes "... a portfolio of methods that have been developed to understand the perspectives of people by observing and participating in activities of everyday life." [Salvador et al. 1999]. Thus, ethnography relies both on *observation* of activities by the researcher, as well as *participation* of the researcher in the everyday activities of the target population [Gubrium and Holstein 2014]. Importantly, an ethnographer takes on the (emic) perspective of the population under observation, using their voice and language to express the *culture* of the population [Fetterman 2009]. At the same time, ethnographers have to be conscious of their own (etic) perspective and the influence their own culture has on their experience [Dourish 2006]. This 'active immersion' allows the ethnographer to establish rapport, trust, and social intimacy [Salvador et al. 1999].

The most important procedural aspect of ethnography is the fieldwork itself [Fetterman 2009]. It provides the ethnographer with the grounding and experience to truly understand the context, relationships, and activities that drive people's behavior [Salvador et al. 1999]. In addition to participation and observation, it is common for ethnographers to interview *key actors* or *informants* in order to elicit deep background information [Fetterman 2009]. These interviews often take on an autobiographical character. Furthermore, the ethnographer might take pictures, record videos, or collect genealogies and artifacts from within the field [Salvador et al. 1999]. The most significant output of the process, however, is the writing of the ethnographer, retelling the experience of the people engaged with the ethnographer and providing insight on how to interpret those experience from both the emic and etic perspective [Dourish 2006]. Thus, the writing provides a commentary of the way of thinking and the values of the people under observation [Gubrium and Holstein 2014].

Thus, ethnography has the advantage of focusing on the actual, everyday experience of the people under observation [Salvador et al. 1999]. This allows to capture the unarticulated or unconscious aspects of behavior and valuation. Furthermore, it maintains the context within which the observed interact. It can be seen as a 'point of mediation' between the lived practice of the people and, in our case, the technological domain [Dourish 2006].

However, to be truly effective, ethnography requires researchers to embed themselves into the population they wish to observer, potentially for a long time. This is especially true in the investigation of privacy-related behavior, as the goal for the ethnographer has to be not being seen as an intruder. In other words, establishing the social intimacy required takes time [Salvador et al. 1999]. Furthermore, as with other forms of observation, an ethnographer has to be thoroughly trained and have a large amount of background knowledge about the behavior to be observed. Finally, even with established trust and rapport, some privacy-related behavior might still be beyond the purview of the ethnographer, as cultural barriers or even higher intimacy requirements may exist. Nevertheless, the potential depth of highly contextualized observations, especially in combination with interviews of key actors, collection of artifacts, and recordings, ethnography can provide invaluable real-life insight into the culture and practice of a target population.

2.4.6 Documents and Artifacts

A final approach for gathering data is the collection and examination of documents and artifacts [Heppner et al. 2008]. In this regard, documents include such various data as diaries, emails, literature, field notes, official documents, and laws. Artifacts can refer to both physical and virtual objects such as video recordings, posters, receipts, photographs, etc. In general, we can categorize documents and artifacts into static and dynamic data [Marotzki et al. 2014]. *Static data* are documents and artifacts that are ‘naturally’ occurring without interaction between investigator and participant. They are, furthermore, unchanged while continuously accessible. In contrast, *dynamic data* are the result of the interaction of investigator and participant, which are potentially volatile (i.e., non-persistent).

We can further distinguish documents into primary, secondary, and tertiary documents [Coffey 2014]. *Primary documents* are those documents that were produced by those experiencing events first-hand. This category includes participant diaries and researcher’s field notes about their own experience. Documents that are produced by people other than the ones experiencing an event are referred to as *secondary documents*. An example of such a document might be a field note about a researcher's observation of the behavior of a participant. Finally, *tertiary documents* are catalogs, reference, or gray literature.

Another distinction can be made between private and public documents [Coffey 2014; Heppner et al. 2008]. *Personal documents* are created for personal or non-official use and include diaries, emails, literature, field notes, etc. [Heppner et al. 2008]. *Public documents*, then, refer to documents created for official business, like government documents, laws, contracts, and diplomas. Regardless of their categorization, all documents are purposefully and socially constructed artifacts that use specific conventions [Coffey 2014]. Many research questions and settings cannot be investigated without considering documents and artifacts, yet they should not be seen as replacement for other data [Coffey 2014].

One of the major advantages of collecting and examining documents and artifacts is the relative ease of this approach. Given a phenomenon of interest and the identification of a target population and participant pool participants are either prompted to create certain artifacts (like a diary of their experiences) or asked to contribute already existing documents or artifacts. They can, therefore, serve as *cultural probes* (e.g., [Bernhaupt et al. 2008; Choe et al. 2012; Leonardi et al. 2009]). Additional benefits depend on the medium of the collected artifact or the type of document. *Native video* recordings (i.e., recordings made by people other than the researcher) can provide an invaluable insight into the lives of the target population. Video recordings have the additional advantage of capturing of non-verbal behavior (such as gestures and facial expression), spacial arrangements of objects, as well as the temporal sequence of events [Knoblauch et al. 2014]. Contrastingly, textual documents can provide insight into social and organizational practices — including information about their authors and audiences, reveal the 'register' and narrative structure of interactions surrounding them, and reveal the relationships between multiple different documents [Coffey 2014]. Furthermore, both documents and artifacts offer permanence, allowing for repeated and thorough analysis [Knoblauch et al. 2014].

However, documents and artifacts are not without disadvantages. For instance, documents cannot necessarily be counted as firm evidence for or against a phenomenon, as they may have been intentionally created to obfuscate events or behavior [Coffey 2014]. Similarly, video recordings can be interpreted as being both reductive and constructive [Knoblauch et al. 2014]. Thus, the choice of framing and perspective influences which aspects and modalities are captured. Furthermore, the technology used transforms the reality through its format and quality. Recordings also suffer from the same drawback as observations in terms of reactivity, as the presence of an observer may alter the behavior that is being recorded [Knoblauch et al. 2014]. Finally, without additional interaction with the participants, artifacts and documents require a large amount of interpretation by the researcher [Heppner et al. 2008]. In other words, they do not provide the internal narrative or rationales of participants, which therefore need to be inferred.

Nevertheless, artifacts and documents play an important part in understanding the context and motivation of privacy-regulating behavior. For example, depending on the context, different laws might apply restrictions on the behavior of people [Nissenbaum 2004; Glass and Gresko 2012]. Besides laws, there might be further *rules and regulations* — both implicit and explicit — that govern privacy behavior in a target domain [Spiekermann and Cranor 2009; Westin 1967]. Examining these laws, rules, and regulations provides invaluable insight into the practice of the target population as they are shaped by these documents. This is particularly interesting in domains where laws and regulations run against established practice (e.g., [Baker et al. 2011]). Furthermore, the increasing number of research papers investigating aspects of privacy can be seen as an additional source of information. These efforts examine such diverse phenomena as the influence of social relationships on location sharing behavior [Wiese et al. 2011], the preferences of inhabitants towards the recording of activity in the home [Choe et al. 2012], or the influence of social relationships, location, and type of interaction on both the perception of an intrusion and the strategy employed to mitigate the situation [Radics and Gračanin 2011].

However, while collecting task-related artifacts is a common practice (e.g., in *contextual inquiry* [Hartson and Pyla 2012]), this is not altogether applicable for the privacy domain. First, while privacy-regulating behavior is goal oriented, it can be seen as a supportive measure for a superseding goal. In other words, it is a supporting task, not the main task of a person. Thus, artifacts collected in such scenarios are likely related to that main task and not directly reflective of the privacy-regulating behavior. More importantly, the artifacts themselves may even be the very thing the privacy-regulating behavior is meant to protect! Should that be the case, collecting those artifacts is likely to be met with resistance by the participants. One way of turning this downside into an advantage is through treating the reaction of the participant to the request for an artifact as data in and of itself. Thus, the participants' reactions can reveal the significance and characteristics of the thing they are trying to protect. This may then be used for further inquiry into the participants' motivations for protecting said artifact or document.

2.5 Implications for Collecting Privacy-Related Information

At the beginning of this chapter, we set out to tackle the challenge of capturing data about the privacy preferences and privacy-regulating behavior of the intended users of an application. This data collection is the first step of providing sufficient domain knowledge for the design of the application. The difficulty of acquiring this kind of knowledge stems from the fact that, except for *laws* and *explicit rules and regulations*, many privacy preferences are *implicit* [Spiekermann and Cranor 2009] and much of privacy behavior is *ad-hoc* [Palen and Dourish 2003]. Thus, an analyst has to carefully decide how to collect data about this domain. As we have seen in the previous sections, an analyst has to consider many aspects of the data collection process in order to elicit *valid* data of high quality.

All considerations are centered around the **research question** which determines the kind of information the analyst is looking for. Thus, an analyst needs to have background knowledge not only in the technical domain, but rather also have a general idea of what kind of privacy-regulating behavior might be triggered or influenced by an application. While personal experience might help the analyst in this process, the many differences between people's preferences and behavior mean that it is not sufficient [Westin 1967]. In other words, the analyst has to have additional training in the privacy domain [Shapiro 2010]. Furthermore, the analyst also has to play the role of advocate for the intended users of the application [Salvador et al. 1999]. The analyst needs to make sure that *privacy-related information* is not only collected for its ‘implications for design’ [Dourish 2006], but rather fosters increased understanding of the users and their lived experience. We will therefore define privacy-related information as follows:

> **Definition** ***(Privacy-Related Information)***
>
> Privacy-related information is the collective term for data (regardless of format) containing information about the *privacy-regulating behavior* or *privacy preferences* of potential users of an application elicited through data collection efforts of an analyst. These data are accompanied by the *bracketing* of the analyst, including the reasons for using the chosen data collection methods, their preconceptions and assumptions, and validity criteria for the data.

The very first task of an analyst, once the research question has been determined, therefore, has to be the **identification of the target population** that will be the source of such privacy-related information. Obviously, this step can — and should — be done in tandem with any other efforts of stakeholder analysis within the design team [Hartson and Pyla 2012; Bjørner 2006]. The analyst, furthermore, needs to choose an appropriate **sampling strategy**. These step reveals the relevant *data sources* of any relevant information for the design process.

> **Definition** ***(Data Source)***
>
> Data Source is the collective term for any source of information about the target population of the application under development, including their environment, behavior, artifacts, documents, and the population itself.

Given the data source or sources, the analyst has to **choose an appropriate data collection method**. Each data collection method has distinct advantages and disadvantages (summarized in Table 2.3). Thus, the analyst has to decide which data collection method fits both their data needs and possible time constraints [Heppner et al. 2008]. The analyst even has the option of using multiple methods in order to alleviate any disadvantages. Since the main focus of the data collection effort is gaining information about people’s privacy preferences and behavior, *qualitative* data collection methods should be preferred. Furthermore, sampling and data collection should be seen as an iterative process that can run in parallel with analysis [Flick 2014]. Thus, an analyst could attempt to gain an in-depth view of the privacy preferences and behavior of a select few salient cases through interviewing and later on attempt to confirm hypotheses on the behavior of the entire population by surveying a larger sample. It is, however, of utmost importance that analysts documents their decision, since any data has to be seen in the context of those decisions.

Table 2.3: Advantages/Disadvantages of Data Collection Methods.

Name	**Advantages**	**Disadvantages**
Interviews	• flexible • interactive • detailed • non-intrusive • internal and external view	• expensive (time) • requires training • difficult for sensitive topics
Focus Groups	• flexible • interactive • detailed • non-intrusive • internal and external view • multiple viewpoints	• expensive (time) • requires training • group dynamic • difficult for sensitive topics
Surveys	• cheap (time) • allows anonymity • non-intrusive • allows large sample size	• non-interactive • limited depth • variance in quality
Observations & Ethnography	• contextual • interactive • very detailed • outside viewpoint	• highly expensive (time) • requires training • reactivity • external view only • possibly intrusive • difficult for sensitive topics
Documents/Artifacts	• cheap (time) • persistent • very detailed • non-intrusive	• only supplemental • only external view • interpretive • task focused

Thus, regardless of the actual data collection method used, the collected data usually fall into one of the following categories: forecasting, retrospection, and observation [Acquisti and Grossklags 2004]. Each of these types of data have specific advantages and disadvantages. Both retrospective and predictive accounts have the advantage of being non-intrusive and easily collected (e.g., through surveys, focus groups, interviews, etc.). However, they are problematic in the way that they may not reflect actual operative behavior [Acquisti and Grossklags 2004]. In predictions, the full context of the situation is not available, thus potentially omitting important aspects that might influence the behavior [Suchman 2007]. Retrospective accounts might be more accurate than predictions, since the behavior was actually exhibited. However, they can be inaccurate as memory is not perfect and multiple situations might be merged or misremembered [Eysenck and Keane 2010]. Observations remove this user-based bias. However, they have the severe limitation of changing the behavior under observation when the user is aware of the observation [Choe et al. 2012; Schaub et al. 2012a; Heppner et al. 2008]. Not alerting the user of the observation would preclude these changes of behavior, but raises obvious ethical issues. Furthermore, purely observational data does not reveal the rationale of the user that determined the behavior [Heppner et al. 2008]. Thus, the analyst has to provide evidence for the validity of the data collected by providing the context and influencing factors of the different choices that led to the particular data. Moreover, the analyst has to **bracket the assumptions** that provide the context in which the data have to be seen and **evaluate the validity** of the data.

Thus, we can define the requirements of privacy data collection as follows:

Definition ***(Data Collection Requirements)***

To capture stakeholder *privacy preference* and *practice*, an analyst needs to

- define a **research question**,
- identify the **stakeholders**,
- determine an appropriate **sampling strategy**,
- execute a fitting **data collection method**,
- **bracket** the assumptions of the research design, and
- **evaluate the validity** of the collected data.

As a result of the data collection efforts, the analyst is faced with a potentially large amount of mostly qualitative privacy-related information, likely in a variety of formats. While this collection of information may contain the background knowledge required to understand the privacy preferences and privacy-regulating behavior of the target population, this information is highly unstructured and, thus, not very accessible. Thus, we face a new problem:

(P3) Data gathering approaches result in large amounts of unstructured, qualitative data.

To address this particular problem, we will need to answer the following question:

(Q3) How can we transform unstructured, qualitative data into structured domain knowledge?

We will address this challenge in the following chapter.

Chapter 3

Requirements of a Privacy Data Analysis Process

> "Before one can properly understand requirements, one needs to ask why the proposed system is needed, who is involved, and what relationships exist among various actors. One needs to understand how things are done under current conditions, why they work or do not work, from whose perspective, and according to what criteria. In specifying a new system, that is, the requirements, one is in effect rearranging relationships among the social actors. [...] Current requirements models and techniques, however, provide support only for stating the results of such deliberations. Existing requirements models focus on behaviors and activities, and information entities and relationships among concepts. The understanding and analysis of the social dimension rely on the skills and experience of the analyst, without models or systematic analytical support."
>
> – [Yu et al. 2010, p. 4]

In the previous chapter, we ventured out to address the challenge of capturing the privacy preferences and privacy-regulating behavior of the target population of our application. The review of data collection methodologies left us with some guidance for the collection of *privacy-related* *information*. However, we are left with the challenge of making sense of potentially vast amounts of qualitative, unstructured information. Thus, as Yu et al. [2010] decry in the quote above, the analyst is still left without guidance and support, and therefore has to rely on skill, experience, and training. Yet, to be able to provide support and guidance to analysts trying to make sense of privacy-related information, we first have to understand what it is we are trying to support.

In its essence, attempting to make sense of information is an analysis task [Yu et al. 2010]. In our case — the analysis of privacy-related information — the analysis task lies at the intersection of the social and technical domain. Therefore, it is sensible to consider existing approaches, both within the social sciences as well as in computer science. However, before delving into the exploration of existing approaches, it makes sense to examine the structure of an analysis (or sensemaking) process itself.

3.1 Analysis and Sensemaking

The way humans reason, analyze, and make sense of information has been the subject of study for centuries within many disciplines [Eysenck and Keane 2010]. In general terms, analysis is the process of transforming data into information, and information into knowledge [Sutcliffe 2002]. While there are many theories and viewpoints on the topic (e.g., [Eysenck and Keane 2010; Weick 2000]), we will focus on the observation of a real-world analysis task, namely intelligence analysis.

The Sense-Making Loop for Analysts

Pirolli and Card [2005] developed a descriptive model of a sense-making process by observing the work of intelligence analysts. They observed that analysts employed two interconnected, iterative processes while working towards a report on a particular topic (see Figure 3.1). They named these processes the *foraging loop* and the *sense-making loop*.

The main task within the foraging loop consist on finding and organizing information. Conversely,

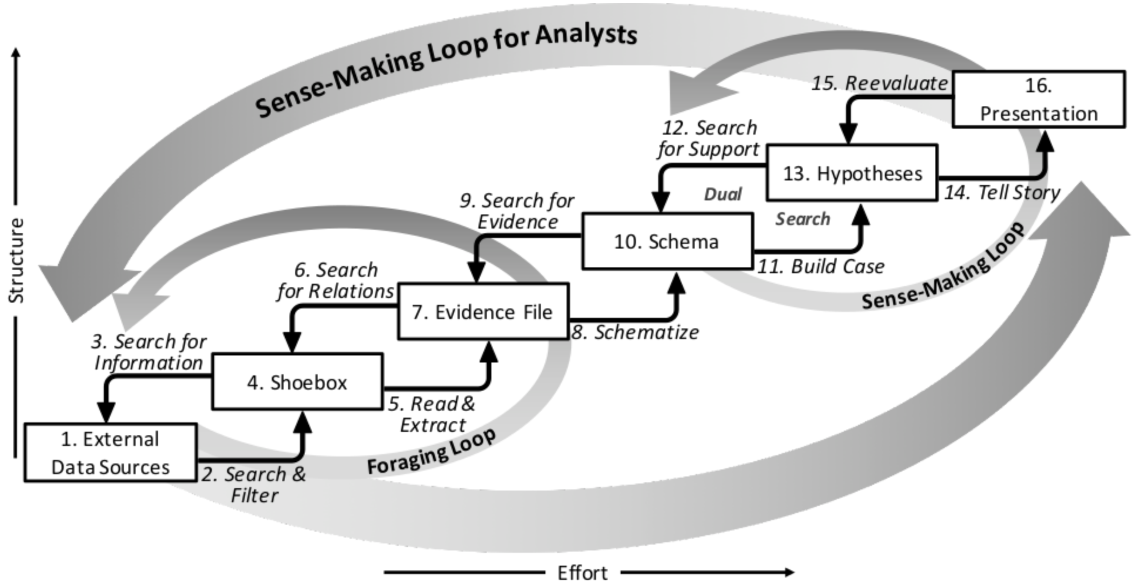


Figure 3.1: The Sense-Making Loop for Analysts (reproduced from [Pirolli and Card 2005]).

in the sense-making loop analysts are iteratively developing a (mental) model of the information gathered. These loops can be driven both by *bottom-up* as well as *top-down* processes.

At the beginning of the bottom-up process the analyst, faced with a vast selection of data sources, has to *forage* for potentially relevant documents within these sources, creating a collection of documents called the ‘shoebox’. In the next step, the analyst determines which documents are relevant to the task at hand, then identifies and extracts key pieces of data from the collected information, storing them in an evidence file. This is an iterative process, as the analyst often has to refer back to the data sources to find additional information sources with new evidence. Given enough evidence, the analyst then starts to schematize the information (e.g., through a timeline visualization). The resulting schema forms the basis of *sensemaking*, as the analyst uses it to iteratively develop and verify hypotheses. The synthesis of the hypotheses into a coherent story in the form of a presentation is the final step of data interpretation. However, the resulting story is also subject to reevaluation, leading to further iteration of the previous steps of both the sense-making and foraging loops.

Conversely, the top-down process starts with the re-evaluation of the hypotheses based on feedback received on a presentation. This leads to a search for support in the schema, which, in turn, can lead to search for evidence within the evidence file. If the evidence file does not contain the required information, the relevant documents are re-examined. Should the required information not be found, a search for new documents can be initiated.

This analysis of the sensemaking process of intelligence analysts reveal some interesting characteristics. First, the analysis process is not a simple, straight-forward progression of predetermined steps, but rather an iterative process of concept formation and re-evaluation. In other words, the analyst practices the *iterative refinement* of the understanding of the information at hand. This is further reflected in the characteristics of the artifacts at different stages of the process. Namely, with every step, the analyst performs *incremental structuring* of the information through filtering, examination, and synthesis with other information. An important aspect of this structuring is the *increased connectivity* within the information. Finally, the distinction between the bottom-up and top-down processes reveals the nature of the iterative structure. Namely, the processes entail both *inductive* and *deductive* reasoning.

These characteristics can focus our search for approaches within the social sciences and computer science. Namely, we need to consider procedural characteristics, artifacts created at different stages of the process, as well as fit to the problem domain of privacy.

3.1.1 Qualitative Data Analysis

Qualitative data analysis can be organized into two major groups based on the strategy employed [Flick 2014]. The first strategy, referred to as *qualitative content analysis*, employs the reduction of volume or complexity of data through *coding*. This entails the classification of information by finding a label for groups of phenomena within the data. The second strategy employs the expansion of the material through interpretation. The goals of the analysis process are either the thick description of phenomena, the explanation of phenomena, or theory development [Flick 2014]. Also, analysis can focus on content, formal aspects of the data, or both. Furthermore, the notion of *sequentiality* is central to the analysis process. In other words, the analysis follows the temporal development within the data [Flick 2014].

Similar to the strategy of intelligence analysts portrayed in Section 3.1, social science researchers frequently analyze qualitative data in parallel to data collection [Gubrium and Holstein 2014]. This practice is not as common in quantitative research. In this regard, data collection can be seen as a process supporting and advancing the analysis process [Flick 2014]. This intertwined data collection often involves *theoretical sampling* [Rapley 2014]. In this regard, data analysis is the driving factor behind data collection, not the other way around [Flick 2014]. Similar to the validity of data collection processes, much of the validity of analysis results depends on the adherence to the strategy chosen for analysis [Flick 2014]. However, there are arguments for adjusting the rigidity of the process to allow for creativity (e.g., [Gubrium and Holstein 2014]).

An extensive overview of considerations and strategies used for qualitative data analysis can be found in [Flick 2014]. Among others, the processes of phenomenological analysis, the documentary method, hermeneutics, and Grounded Theory are described. Of these processes, only Grounded Theory proves applicable to the privacy domain.

Phenomenological analysis is focused on the experience of participants and is based on the work of Edmund Husserl. It is also referred to as *intentional analysis* [Heppner et al. 2008]. The analysis, here, is conducted through 'emphatic' understanding of the experience and epoché [Heppner et al. 2008]. During emphatic understanding, the analyst reflects on the relationships between different parts of the participant's experience while trying to ascertain their contribution to the experience The epoché contains the analyst's reflections on the philosophical underpinnings of their approach, as well as the bracketing of assumptions and judgments. These processes are done within three steps: description, reduction, and interpretation [Heppner et al. 2008]. Phenomenological analysis has only limited applicability for the analysis of privacy-related information, as it relies on the intuition and 'Gedankenspiel' of the analyst. Thus, the analysis is heavily influenced by the experiences of the analyst. Furthermore, phenomenological analysis expands the data through analysis, which may make it even harder for other people to access.

The *documentary method* describes a two-step process. During formulating interpretation, the researcher establishes the topics of an interview, whereas the reflecting interpretation considers the contextual “spheres” that lead to the particular expressions of the topics. However, while it provides procedural guidance, the documentary method results in prose descriptions, which are not inherently more structured than the text they are derived from.

Hermeneutics relies on the sentence-by-sentence analysis of text, distilling meaning from decontextualization of sentences and “thought experiments” as to the possible meaning of the sentences in different contexts. Yet privacy perception and regulation are intimately tied to context. Thus decontextualization of information would render the information useless. *Grounded Theory* [Corbin and Strauss 2008] proves to be a better fit.

Grounded Theory

The notion of analysis being an iterative process of incrementally developing, refining, and verifying concepts to build a theory forms the basis of Grounded Theory. Most importantly, it is inherently *data driven*, i.e., all the generated concepts need to be grounded in data. This grounding helps limit the introduction of bias and also provides an *audit trail* that helps evaluate the validity of the research being done. Corbin and Strauss further stress the importance of capturing as much of the complexity present in data as possible.

Grounded Theory provides the researcher with guidance in the form of procedural steps. The two main steps are open coding and axial coding. *Open coding* describes the process of deriving concepts or terms from data, while also determining the attributes and dimensions of the concept or term. This involves the clustering of elements by their meaning and the eventual conversion of that cluster into a category [Heppner et al. 2008]. *Axial coding* is the process of relating concepts or terms to each other. This involves relating concepts on the same level of abstraction as well as creating a hierarchy between concepts. Thus, through open and axial coding, concepts are inductively described both through their attributes and their relationships with each other. Both coding steps are done in parallel and can be started immediately after the collection of the first data point. Analysis and data collection continue until *conceptual saturation* (also referred to as *theoretical saturation*) — the state where each category or term is fully described — is reached. Data collection can furthermore be guided by the attempt to address specific questions raised by existing data. Corbin and Strauss call this deductive process *theoretical sampling*, which we have encountered in Section 2.3.1. It is important to note that concepts are not meant to be static, but rather need to be iteratively refined to account for additional data. Furthermore, the analyst should capture their reasoning and assumptions through memoing [Heppner et al. 2008]. While Grounded Theory can be based on multiple data sources, interviews are the most common choice of data source [Heppner et al. 2008].

3.1.2 Data Analysis in Software Engineering

Software engineering is the field within computer science that concerns itself with the efficient development of quality software [Bjørner 2006]. Traditionally, this process has been separated into three steps: domain engineering, requirements engineering, and software design (see Figure 3.2). Bjørner states that software design depends on specified requirements, and requirements themselves cannot be created without understanding of the application domain. This structuring also allows for the separation of concerns.

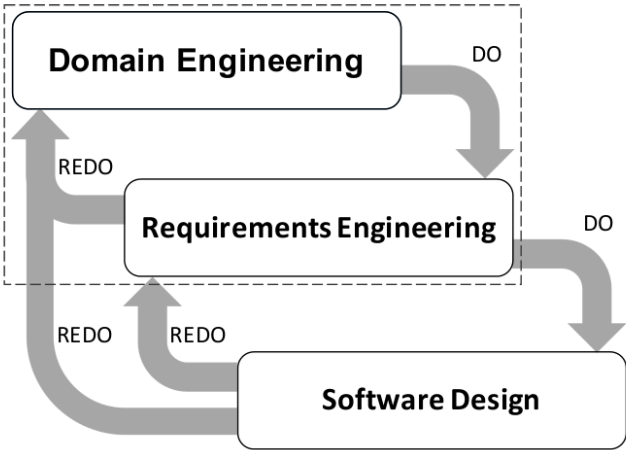


Figure 3.2: The Software Engineering Process (reproduced from [Bjørner 2006, p. 40]).

Domain Engineering (DE) is the process of developing a descriptive model of the application domain through interaction with stakeholders. To that end, the actors and concepts, processes, organization, rules and regulations, as well as behaviors present in the application domain need to be examined. Similarly to Grounded Theory, the analyst needs to strive towards a *complete* representation of the application domain. Furthermore, the resulting model should be *consistent* (i.e., not result in different attributes for a concept) as well as *unambiguous* (i.e., not result in the same description for different concepts). Finally, the domain model needs to be *verifiable* in these regards by the analyst, allow *validation* of its completeness through stakeholders, and be usable for sharing knowledge about the domain.

The *Requirements Engineering (RE)*[1] process aims to create a prescriptive model of the functionality of an application from the domain model. This model consists of a set of *requirements* which prescribe different aspects of the software. Requirements have traditionally been categorized into functional and nonfunctional requirements (e.g., [Yu et al. 2010]). As the name suggests, *functional requirements* specify the functionality of an application. *Nonfunctional requirements*, on the other hand, specify aspects of the application related to concepts like usability, reliability, or performance. This also include social aspects like privacy.

Finally, *Software Design* deals with the actual implementation of the application based on the requirements generated during Requirements Engineering. This process deals with real-world implementation concerns like system architecture, application structure, etc. A common practice during software design is the use of software design patterns (e.g., [Gamma et al. 1994; Borchers 2000; Crabtree et al. 2002; Fowler 2002]).

There are a large number of different approaches to the software engineering process [Kassab et al. 2014]. We will therefore focus on one representative exemplar that addresses nonfunctional requirements, namely the *Grounded and Linguistic-Based Requirements Analysis Procedure*.

[1] The domain engineering and requirements engineering processes are often combined and summarily referred to as requirements engineering (e.g., [Yu et al. 2010; Chakraborty et al. 2015]).

Grounded and Linguistic-Based Requirements Analysis Procedure (GLAP)

Chakraborty et al. [2015] posit that eliciting nonfunctional requirements poses a significant challenge in Software Engineering processes. They argue this is due to the task being more sociological than technological, as it revolves around sensemaking of mostly qualitative data. Thus, their **Grounded and Linguistic-Based Requirements Analysis Procedure** (GLAP) aims to provided systematic support for this sensemaking process by applying Weick's enactment theory [Weick 2000]. Enactment theory describes sensemaking through writing, conversation, and editing. These actions occur in three stages: enactment (acts of categorization to impart order), selection (reduction of ambiguity), and retention (connection to the real world). GLAP applies enactment theory by creating a four-phase process with the goal of creating *traceable*, *unambiguous*, and *verifiable* requirements.

The first phase is based on the Linguistic Analysis of Language Quality [Rosenkranz et al. 2013], and is subdivided into two steps. During *language construct coding*, the analyst identifies symbols (concepts) and concept descriptions and attempts to associate each symbol with a description. During *language quality coding*, the analyst checks the resulting "objects of definition" for deficiencies in quality. Four deficiencies are defined: *incompleteness* (descriptions without assigned symbol), *meaninglessness* (symbol without assigned description), *redundancy* (description assigned to multiple symbols), and *ambiguity* (symbol with multiple assigned descriptions).

The remaining three phases are based on Grounded Theory [Corbin and Strauss 2008]. Phase two involves *open coding* of the data. This is both designed to add more detailed descriptions to the symbols identified in the previous phase and to develop a hierarchy of concepts. This phase is guided by the Volere Typology of nonfunctional requirements [Robertson and Robertson 2006], which can function as top-level concepts. The Volere Typology partitions nonfunctional requirements into *look and feel*, *usability and humanity*, *performance*, *operational and environmental*, *maintainability and support*, *security*, *cultural and political*, and *legal*.

In the third phase, the analyst performs *axial coding* of the taxonomy of concepts resulting from open coding to develop relationships between concepts. This phase is guided by the NFR Framework [Mylopoulos et al. 1999] and employs a top-down approach. The goal of this phase is the creation of so-called *softgoal interdependency graphs* (softgoals referring to the concepts within the taxonomy). To that end, the analyst determines the interdependencies between the different concepts, as well as whether an interdependency contributes to a higher-level concept positively or negatively. The leaves of the resulting graph represent the *operationalization* of the top-level nonfunctional requirements.

Finally, the *selective coding* phase aims to integrate the disconnected softgoal interdependency graphs of the top-level concepts. The resulting “full interdependency graph” is the complete representation of the nonfunctional requirements and their operationalization. The leaf nodes of the graph should be traceable back to the qualitative data on which the analysis is based. Furthermore, the graph and its traceability establish organizational knowledge based on this “shared language”.

Yet while GLAP provides a solid approach for modeling nonfunctional requirements, is falls short of being truly useful for eliciting privacy requirements. This partially relates to the adaptations Chakraborty et al. applied to the Grounded Theory process. Their relegation of open coding to the second step (after linguistic analysis) is based on their assumption that “key conceptual components [. . .] are already well established in practice [. . .]” [Chakraborty et al. 2015, p. App-1]. However, the lack of this knowledge is precisely what leads to the challenges in designing privacy-aware applications. Furthermore, while the Volere typology provides guidance ensures coverage of a broad field of categories of nonfunctional requirements, it does not provide guidance for the elicitation of privacy requirements. In fact, it is not clear which category privacy requirements would fall into, as different requirements could be counted into the “usability and humanity”, “cultural and political”, as well as “legal” categories.

3.2 Evaluation of Analysis Processes and Artifacts

The previous sections reveal a set of common characteristics shared by the analysis processes. These characteristics can be partitioned into characteristics of the analysis process itself and characteristics of the artifacts created by the process. We can use these common characteristics as prerequisites for processes supporting privacy data analysis.

3.2.1 Characteristics of Analysis Processes

The first characteristic shared by all processes discussed is the **incremental structuring** of information. In the Sense-Making Loop for Analysts [Pirolli and Card 2005], this feature is expressed both explicitly through the axis label in Figure 3.1 and implicitly represented through the increased structure of the artifacts in each stage of the process. Thus, the unstructured data from the external data sources is refined more and more over the lifetime of the process, until it is transformed into a cohesive presentation. Similarly, the open coding and axial coding processes of Grounded Theory [Corbin and Strauss 2008] transform the unstructured qualitative data into clusters with shared meaning, before establishing the relationships between the different clusters. We have seen these processes adapted by the Grounded and Linguistic-Based Analysis Procedure [Chakraborty et al. 2015].

Furthermore, the incremental structuring of the information in these processes is not achieved through a single 'push' towards the desired product, regardless of whether that product is a presentation, theory, or interdependency graph. Rather, each process creates its product through the **iterative refinement** of the artifacts created throughout the process. In the Sense-Making Loop, this iterative characteristic is represented through the foraging and sense-making loops, as well as through the ladder-like structure of the process itself (cf. Figure 3.1). Grounded Theory encourages the researcher to address questions arising from data collected through theoretical sampling and the iterative refinement of codes based on the available information. Similarly, the Software Engineering Process explicitly suggests re-doing parts of the process to address shortcomings of the artifacts created in different parts of the process (cf. Figure 3.2).

Finally, all processes contain both **data-driven** and **model-driven** components, revealing support for *inductive* and *deductive reasoning*. In the Sense-Making Loop, the 'bottom-up' process building up a presentation from the given data represents the data-driven part of the process, whereas the evaluation of the artifacts based on feedback (the 'top-down' process) represents the model-driven part (cf. Figure 3.1). In Grounded Theory, open coding is ideally purely data-driven, axial coding has aspects of both model and data-driven analysis, and theoretical sampling is purely model-driven. In GLAP, furthermore, language construct coding represents another data-driven process, whereas language quality coding and selective coding are mostly model-driven.

3.2.2 Desired Characteristics of Analysis Artifacts

The characteristics of the artifacts produced by the analysis processes described above are much more implicit than their procedural counterparts. Furthermore, they are much more *desired* characteristics than actual characteristics, and many aspects of the analysis processes focus on achieving their ideal state. The first of these desired characteristics of process artifacts is **consistency**. Without a doubt, any presentation by an intelligence analyst needs to be consistent to have merit, thus making consistency an implicit goal of the Sense-Making Loop. Similarly, any scientific theory produced by a researcher using Grounded Theory has to be consistent. Bjørner [2006] refers to the process of ascertaining whether an artifact is consistent as **verification**. Chakraborty et al. [2015] even provide us with a set of counter-criteria against which artifact components can be evaluated: *incompleteness*, *meaninglessness*, *redundancy*, and *ambiguity* (cf. Section 3.1.2).

Similar to the completeness of artifact components, each analysis process aims to cover all phenomena of the domain — or at least those phenomena available through data sources. Such a **complete** view of the domain is the explicit goal of an intelligence analyst's report, a researcher's theory, and a software engineer's domain model. However, how can we make sure we have reached completeness? Corbin and Strauss [2008] leave the decision whether *conceptual saturation* has been reached to the judgment of the researcher. In contrast, Bjørner [2006] suggests **validation** of the domain model through collaboration of the analyst with stakeholders.

Finally, one important characteristic desired in the artifacts of each process is their **traceability** to the underlying data. In the Sense-Making Loop, this traceability is established by the analyst through the chain of evidence from the source data all the way to the presentation. Open coding provides an 'audit trail' to the data from which different concepts are derived for both Grounded Theory and GLAP. Furthermore, each additional layer of the concept hierarchy is linked to the underlying layer, providing traceability throughout the concept hierarchy or interdependency graph.

3.2.3 Process and Artifact Requirements

The evaluation in Section 3.2.1 has provided us with common characteristics of analysis processes. We will define these shared characteristics as requirements for any privacy data analysis process.

> **Definition** ***(Process Requirements)***
> A privacy data analysis process needs to support:
>
> 1. the **incremental structuring** of information,
> 2. the **iterative refinement** of artifacts, and
> 3. both **data-driven** and **model-driven** analysis.

Furthermore, we have established the desired characteristics of the artifacts analysis processes produce in Section 3.2.2. These will serve as requirements for the artifacts produced by a privacy data analysis process.

> **Definition** ***(Artifact Requirements)***
> Artifacts produced by privacy data analysis processes need to support:
>
> 1. **verification** of their **consistency**,
> 2. **validation** of their **completeness**, and
> 3. **traceability** to the underlying data.

As we set out to develop a process meeting these requirements, we need to remember the goal we set in Hypothesis 1. Namely, we aim to provide domain models for the design of privacy-aware applications. Thus, our privacy data analysis process needs to allow **integration into existing practice**. As such, generated artifacts should work as a basis for **organizational memory** to allow for learning about the problem domain as well as reuse of knowledge. The Privacy Requirements Engineering process (PREprocess) presented in the following section aims to address all these issues.

3.3 The PREprocess Framework[2]

As we have stated in Hypothesis 1, the goal of our endeavor is the creation of application-specific *privacy domain models*. Chapter 2 has provided us with **data collection requirements** for the collection of *privacy-related information* from *data sources*. The **process requirements** in Section 3.2.3 provide us with the general structure of a process that can transform the privacy-related information into the domain model. Furthermore, the privacy design frameworks in Section 1.3 and the Software Engineering Process described in Section 3.1.2 provide us with information on how to **integrate our framework into existing practice**.

Using these prerequisites as the lattice of our framework and adapting the Sense-Making Loop of Pirolli and Card [2005] results in the Privacy Requirements Engineering process (PREprocess) shown in Figure 3.3. Like the Sense-Making Loop, the process provides **incremental structuring** through separate bottom-up and a top-down processes. These processes can be segmented into a **Requirements Modeling** loop and an **Implementation** loop. The focus of our approach, while providing guidance for both requirements modeling and implementation, is the requirements modeling loop. As mentioned above, the implementation loop is exhaustively covered by existing work (e.g., [Hartson and Pyla 2012; Bjørner 2006; Rosson and Carroll 2002]). We will describe the process through the bottom-up **Design** and top-down **Evaluation** process in sequence, since

[2] An earlier version of the PREprocess was published in [Radics et al. 2013].

these processes are easier to follow.

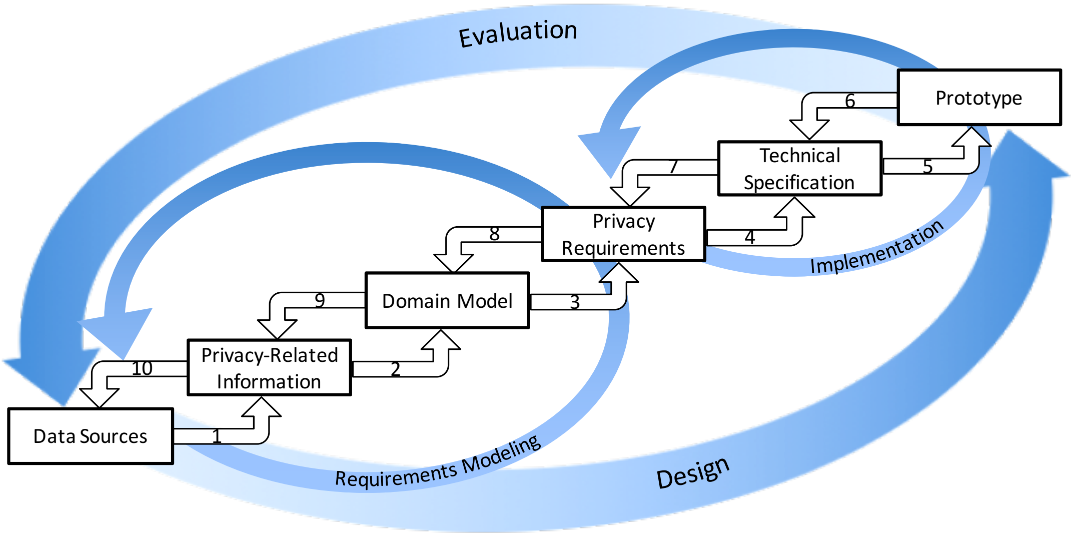


Figure 3.3: The PREprocess. *Design*: (1) Collect Data; (2) Model Information; (3) Synthesize Requirements; (4) Create Technical Specification; (5) Implement Prototype. *Evaluation*: (6) Evaluate Prototype; (7) Search for Alternatives; (8) Refine Requirements; (9) Evaluate Model; (10) Sample Additional Data.

3.3.1 The Design Process

Step 1: Collect Data

The first step of the design process is the **collection of data** from **data sources** (Step (1) in Figure 3.3). In this step, the analyst needs to consider the data collection requirements discussed in Chapter 2. The first task for this step is to determine the *research question* that will produce the information needed. Should the project involve the development of a new application and without previous research, initial data collection should attempt to elicit a wide breadth of information on the privacy preferences and privacy-regulating behavior of the stakeholders. Given a more mature project (e.g., the redesign of an application or given previous research), the analyst should focus on depth. The information need is also heavily influenced by the *purpose* and *setting* of the system [Yu et al. 2010].

Given the research question, the analyst has to identify the *stakeholders* of the application. This can be achieved through activities like brainstorming or market research [McDonald 2015]. Given the stakeholders, the analyst then has to decide on a *sampling strategy* to guide the recruitment of participants for the study (cf. Section 2.3.1). Part of the considerations should be the prioritization of stakeholder groups based on their influence and interest (cf. 2.3.2). The type and maturity of the project further influence this decision. Given a new project, the analyst is probably best served with a larger *heterogeneous sample* to gain the broad overview required. In the case of a more mature project, the analyst should consider *intensity sampling* with a smaller sample size to collect in-depth information.

Similarly, the analyst has to decide and execute an appropriate *data collection methodology*. This choice is heavily constrained by resource availability. The analyst, therefore, needs to consider the advantages and disadvantages of the different methods and make a decision based on the given constraints (cf. Table 2.3). Special consideration should be given to *laws* and written *rules and regulations*, as they can help identify necessary constrains for the applications, and reveal some of the more explicit components of the domains. Finally, the analyst explicitly documents the reasoning behind the choice of research question, stakeholder prioritization, sampling strategy, and data collection methodology in a *bracketing* log. The outcome of this step is **privacy-related information** containing the collected data, the bracketing log, possible field notes of the analyst, and relevant documents like laws or regulations.

Step 2: Model Information

In the second step, the privacy analyst **models** the privacy-related information into a consistent **privacy domain model** (Step (2) in Figure 3.3). This is the analysis task we have discussed in Sections 3.1 and 3.2. Thus, the analyst has the choice between *reduction* of the information through *coding* and its *expansion* through *thick description* (cf. Section 3.1.1). While both approaches have their merits, the artifact requirements discussed in Section 3.2.3 are easier to integrate with coding.

Thus, similar to the Grounded and Linguistics-Based Analysis Procedure (GLAP) [Chakraborty et al. 2015], we recommend a *Grounded Theory*-based approach. The advantage of Grounded Theory lies in its relative simplicity and flexibility, while at the same time providing guidance and structure for the analyst. Furthermore, it is inherently *data driven* and has a strong support for *traceability*. We will, therefore, adapt the general structure of the *open coding* and *axial coding* processes from [Corbin and Strauss 2008], while adopting some of the linguistic features of GLAP. Thus, we suggest the following procedural steps.

Encoding starts with the *chunking* of information into coherent *assertions*. Depending on the granularity desired, the analyst may choose to treat entire responses as a single assertion, or create smaller chunks on the paragraph, sentence, subsentence, or even lexical level. Obviously, part of the consideration for this decision has to be based on available resources, since finer granularities will require more time. Another consideration may be the potential value of capturing and formalizing the particular language used by members of the target population (e.g., in a *privacy dictionary* [Gill et al. 2011]). Furthermore, it may be worthwhile to distinguish between the functions of different chunks (e.g., whether they represent ‘things’ or ‘relations’ between things). To provide traceability, these assertions should reference the data that provides their *support*.

Given the resulting set of assertions, the analyst then proceeds with the *open coding* of the assertions. In this step, the analyst strives to sort the assertions into thematic clusters, and add both a label and description to that cluster. This description should not only highlight the content of the cluster, but rather also include the rationale of the analyst to form this particular cluster (i.e., *bracketing*) as well as references to its assertions. We will refer to the combination of a label and its description as a *term*.

Provided a set of terms, the next step is the *axial coding* of these terms to form a taxonomy of terms (or *terminology*). In other words, the analyst strives to establish hierarchies of terms through sub-term relationships, as well as establish any other types of relationships between the terms. At this point, it becomes necessary to distinguish between *leaf terms* and *taxonomic terms*. Leaf terms are those terms that contain direct references to assertions. Taxonomic terms are the terms generated through axial coding that are not directly supported by assertions. Thus, in contrast to the description of leaf terms, taxonomic terms contain the reasoning for the clustering of terms they represent as well as references to those terms.

The outcome of this step is a descriptive **privacy domain model**.

Step 3: Synthesize Requirements

The third step is the **synthesis** of the conceptualization within the domain model into coherent application-specific **privacy requirements** (Step (3) in Figure 3.3). To that end, the privacy analyst establishes the relationships between the patterns so that they provide a complete image of the privacy implications of the intended application. Alternatively, given the domain knowledge contained in the privacy domain model, the privacy design frameworks discussed in Section 1.3 can now be applied. At this point it is also appropriate to consider the *functional requirements* elicited within traditional requirements engineering processes and examine potential interactions between both sets of requirements. During this process, it may be useful to formally specify the emerging requirements model using one of the notations outlined in Section 1.3. Alternatively, it is common to specify requirements in the form of *use cases* [McDonald 2015] or *scenarios* [Rosson and Carroll 2002].

The outcome of this step is a set of prescriptive **privacy requirements**.

Step 4: Create Technical Specifications

Once the privacy requirements have reached sufficient maturity and coverage, it is time to **create technical specifications** based on the requirements (Step (4) in Figure 3.3). However, it may not be possible to create a perfect technological equivalent of the privacy requirements [Ackerman 2000]. In such cases, the trade-offs embodied in these *first-order approximations* need to be documented. *Patterns* [Borchers 2000] and *claims* [Sutcliffe and Carroll 1999] are two formats specifically geared towards capturing such trade-offs. Furthermore, the analyst can examine repositories of existing technical solutions like software design patterns [Gamma et al. 1994] to support architectural decisions.

The outcome of this step is a set of **technical specifications**.

Step 5: Implement Prototype

Finally, as the last step of the design process and given the technical specifications of the first-order approximations, a **prototype** can be **implemented** (Step (5) in Figure 3.3). The additional technical specifications from parallel technical requirements engineering processes are integrated and aligned. Depending on the stage of the development process, different prototyping techniques need to be chosen to create a prototype of appropriate quality and depth (cf. [Hartson and Pyla 2012; Rosson and Carroll 2002]).

The outcome of this step is a **prototype**.

3.3.2 The Evaluation Process

Step 6: Evaluate Prototype

Conversely, the **Evaluation Process** starts with an existing prototype or application. As the name suggests, the process starts with the **evaluation** of the prototype (Step (6) in Figure 3.3). A good overview of possible methods for evaluating a prototype is provided in [Hartson and Pyla 2012; Rosson and Carroll 2002]. Besides giving **feedback** on the overall quality of the prototype or application, the evaluation serves two purposes in terms of the privacy requirements engineering process. On the one hand, the data generated through the evaluation provides an additional **data source** for the application domain. On the other hand, the evaluation provides insight in the quality of the technical specifications chosen. Thus, it can help identify which trade-offs work, and which do not.

Step 7: Search for Alternatives

If a technical specification does not serve its intended purpose, this information should be documented in the representational format chosen in Step (4). Furthermore, the identification triggers a **search for alternatives** to the technical specification within the privacy requirements (Step (7) in Figure 3.3). To that end, the requirements need to be examined and the mismatch between the requirement and the specification identified. Furthermore, the analyst can consult existing repositories of known solutions to determine alternative candidates (e.g., by examining software design patterns [Gamma et al. 1994]). If possible, the technical specification should be updated to better match the model. Otherwise, it has to be replaced with a new technical specification.

Step 8: Refine Requirements

The analysis may reveal that the problem does not lie in a mismatch between the technical specifications and the privacy requirements, but rather in the requirements themselves. Should this be the case, the privacy requirements need to be **refined** and, if necessary, **expanded** (Step (8) in Figure 3.3). The privacy analyst, therefore, needs to examine the requirements to determine whether they correctly reflect the information in the domain model.

Step 9: Evaluate Model

Should the privacy requirements be deemed sound, the negative feedback elicited through the evaluation is most likely the result of missing or incorrect concepts within the domain model. Therefore, the privacy analyst needs to re-examine the **terminology** and **assertions** and either **refine** the existing statements or **add** new statements extracted from the privacy-related information (Step (9) in Figure 3.3). This is done through **verification of consistency** and **validation of completeness**. Verification, here, refers to testing the quality and consistency of our domain model (i.e., ‘getting it right’ [Bjørner 2006]). We will adapt the metrics of *incompleteness*, *meaninglessness*, and *ambiguity* from GLAP. Thus, a leaf term is incomplete, if it is not supported by any assertions, whereas a taxonomic term is incomplete if not supported by other terms. An assertion is incomplete if it is not supported by any data. Conversely, assertions are meaningless if they do not support a term. Terms, themselves, cannot be meaningless. Furthermore, an assertion is ambiguous if it supports multiple terms at the same time. In contrast to GLAP, *redundancy* (in our case, multiple assertions supporting a term) does not reveal inconsistency or lack of quality of a model, but rather reflects the prevalence of terms within the data.

Should inconsistencies exist within the domain model, the analyst needs to modify the model to eliminate those. Incomplete terms can be removed from the domain model, should they not have a match within the meaningless assertions, in which case those assertions are simply added to the support of the term. If no term matches a meaningless assertion, the analyst has to determine whether the existing terms are ill-defined, or whether the assertion warrants its own term. Finally, in case of ambiguous assertions, the analyst should reconsider the classification of the assertions into terms in order to remove the overlap. Ideally, leaf terms represent a partition of the assertions.

Additionally, the analyst should consult **stakeholders** to receive feedback on the validity of concepts in terms of their categorization and description. In concert with the stakeholders, the analyst furthermore needs to determine whether the concepts cover the provided data, as well as whether the concepts sufficiently describe the target domain. This step also might involve verifying the transcript of the raw data in order to identify possible mistakes. At this stage additional coding can be performed using feedback from the stakeholders.

Step 10: Sample Additional Data

Finally, if the feedback from the evaluation does not reveal an incomplete or incorrect domain model, the current collection of data is insufficient to address **open questions** arising from the analysis. Alternatively, the analysis and evaluation may have revealed concerns regarding the **validity** of the data collected. At this stage, the privacy-analyst needs to determine whether these issues can be addressed through the **sampling of additional data** (Step (10) in Figure 3.3).

Evaluating the validity of the collected data may require re-evaluating the research question, revisiting the definition of the stakeholders, recruiting additional participants, or employing different data collection methods (cf. Section 2.2). Open questions from the data analysis process and stakeholder feedback from the evaluation should influence additional **theoretical sampling** of the target population through a new data collection instrument or data collection methodology to complement existing data. Moreover, the data generated through the evaluation itself may also be used as a new data source for relevant privacy-related information.

3.3.3 Iterative Refinement

It is important to note that the steps of the design and evaluation processes are not meant to be strictly executed consecutively in a waterfall-like fashion. Rather, it is strongly recommended to iterate over the steps of the **Requirements Modeling** and **Implementation** loops (see Figure 3.3). An analyst would first iterate over steps 1–3 and 8–10 of the PREprocess in order to create privacy requirements that adequately represents the privacy preferences and privacy-regulating behavior of stakeholders of the intended system. This is likely to happen multiple times before adequate maturity of the privacy domain model and privacy requirements is reached. Only then would the requirements be passed on to the software engineers to implement and refine an actual prototype (steps 4–7). Alternatively, depending on the maturity of the requirements generated, further iterations of the requirements modeling loop can be performed in parallel with iterations of the implementation loop. This aligns closer to the iterative structure of the Design-Implement-Analyze cycle [Rosson and Carroll 2002] as well as the UX-Wheel [Hartson and Pyla 2012].

3.4 Application Example

In this section we will provide an example of how the PREprocess can be applied to a real-world design problem: the creation of an email system for a large internet company with multiple business locations. The *purpose* of the new system is to meet the *community privacy* needs of the company. The term community privacy is used to refer to the ways a community shares the dissemination of information under its control [Codio et al. 2012]. A community is here defined to denote a group of people with a shared purpose, as well as a shared responsibility for the information under their control. The result of the application of the PREprocess to this problem is the CMail System[3][DeHart 2013].

Given the design task, the privacy analyst has to determine the data sources to consider for the privacy requirements engineering process. The privacy analyst decides that the *data sources* available are insufficient for the intended task and decides to run a focus group study with members of the company [Codio et al. 2012]. This focus group is intended to reveal the community privacy practices of the company. The data gathered in the focus group is **selected** to constitute the relevant **privacy-related information** (PRI).

After transcribing the audio recordings from the focus group study, the analyst starts the process of **encoding** the data. The analyst quickly notices a recurring theme in the utterances of focus group participants. There are many mentions of *annotations* of e-mails to *limit their dissemination*, as the following quote shows.

> ***Quote 1*: *"[. . .] sometime we'll use a prefix in the subject if it says confidential that's a signal that means do not forward this message, it's not appropriate, it's only for your eyes. We use words like 'urgent', 'confidential', 'do not forward'. Things that tell the person reading the message 'hey this is only for you."'*[4]

The analyst decides this to be important enough to warrant its own concept. In order to provide the *traceability* of the concept to its supporting data, the analyst furthermore attaches a supporting reference to Quote 1 to the concept definition.

Concept 1: Annotation

[3] Note that the example in this section is a *simulation* of the process. Both the focus group studies in [Codio et al. 2012] and the development of the CMail system in [DeHart 2013] predate the framework presented here.

[4] This quote and all of the following quotes that establish patterns are part of the first focus group within the study detailed in [Codio et al. 2012].

E-mails are annotated to limit their dissemination.

Support: Quote 1

Amongst the utterances about e-mail annotations, the analyst notices the following quote:

> ***Quote 2*: *"Yeah, one of the things we do, you can tell this by the body of the message or the recipient list; so we have a group people in [location], people that we consider our [location] leadership team. If it is our standard leadership recipient list and in the email it says this is a leadership team topic we're going to talk about it, then that basically signals it stays within that group, it should not be sent out to anybody else so that you can tell who the message is intended for by the recipient list and sometimes just by what's in the body of the message."***

The analyst finds this notion of a community interesting and, going over the transcripts, finds other mentions of pre-existing communities within the company:

> ***Quote 3*: *"Groups are established by your job title. In [location] there is HR team and there is subset of the HR team based on your job title. You don't get added to a certain group unless your title changes to fit the profile of that group."***

> ***Quote 4*: *"Based on the projects and meetings we are part of. In terms of things we discuss in the meetings or take away items. If you were going to email a group on that, you would email just this specific group that was in the meeting, on the project working to resolve an issue."***

Confident this represents another concept within the data, the analyst defines the following concept based on the three supporting quotes:

Concept 2: Community

Communities signify dissemination boundaries.

Support: Quote 2, 3, 4

Further exploration of the transcript reveals the existence of certain circumstances in which information that is usually contained within a certain community is shared nevertheless:

> ***Quote 5***: *"Just today I was asking some advice about salary information about somebody we are going to hire. That's exactly something where he doesn't need to know that information but I just want his professional advice on that information. We both understand the sensitivity of that information. There is a trust relationship that is really making that okay."*

The analyst decides to capture the information of this quote in another concept.

> ***Concept 3: Exception to the Rule***
> There are exceptions that lead to dissemination of information beyond the boundaries of a community.
> *Support:* Quote 5

At this stage, the analyst feels confident that the patterns capture a big enough section of the data and decides to start the **synthesis** process. To that end, the analyst has to establish the relationships between the three patterns. The relationship between Concepts 1 and 2 are quickly established:

> ***Privacy Requirement 1: Community Annotation as Dissemination Boundary***
> To establish the dissemination boundary of an e-mail, it needs to be annotated with the community (or communities) that define the intended dissemination boundary.
> *Support:* Concept 1, 2

Analogously to the annotations within the concept definitions, the analyst provides references to the concepts supporting the privacy requirement. Reviewing Concepts 1 and 3, the analyst quickly realizes that exceptions to boundaries are not related with the mechanism used to establish it. Therefore, the two concepts need not be aligned. The resolution of the tension between Concepts 2 and 3 proves to be more difficult. Thus, the analyst returns to the data in search for the process employed for these exceptions, yet does not find sufficient evidence in the transcripts for a specific strategy. However, the purpose of the application itself provides the missing information: the support of the community privacy needs of the company. As members of a community, people share the responsibility for the appropriate dissemination of information. Thus, decisions about exceptions to typical practices are the shared responsibility of the members of the community in question. The analyst now creates the remaining connections[5].

> ***Privacy Requirement 2: Notice and Choice for Exceptions***
>
> In order to make an exception to a dissemination boundary established, the community in question needs to be notified and agree upon the exception.
>
> *Support:* Concept 2, 3

With all concepts successfully aligned, the analyst considers whether the Privacy Requirements interfere with the general requirements of an e-mail system. Since this is not the case, the analyst moves on to **create technical specifications** for the requirements. The analyst furthermore decides to use *claims* [Sutcliffe and Carroll 1999] to represent the trade-offs represented by first-order approximations and provided links between related claims (similar to those between the *patterns* of a pattern language [Borchers 2000]). The analyst starts off with providing a technical representation of the community tags within Privacy Requirement 1. Since at this stage the analyst does not have information on any downsides of this representation, the claim only contains its positive aspects. Furthermore, since no other claims exist, it is not linked to any other claims. The only addition to the claim, thus, is the support reference to the underlying privacy requirement.

> ***Technical Specification 1: Community Tag***
>
> A community is represented through a "community tag" and defined as a collection of uniquely identified users. Community membership is established through consensus. An e-mail annotated with one or multiple "community tags" cannot be forwarded to any person outside of the community.
>
> $+$ Represents communities.

[5] Note that these privacy requirements align with the community privacy model focusing on *community tags*, *notification*, *exceptions*, and *consensus* in [Codio et al. 2012].

+ Establishes dissemination boundary.

Support: Privacy Requirement 1

The analyst decides to tackle exceptions next. Since this first-order approximation is directly related to Technical Specification 1, the analyst adds a link between the two specifications in addition to the support reference.

Technical Specification 2: Exception

An e-mail annotated with one or multiple "community tags" can be forwarded to a person outside of the community, iff consensus is reached within the communities in question.

+ Establishes exception mechanism.

Support: Privacy Requirement 2
Related: Technical Specification 1

As both membership and exception decisions rely on a definition of consensus, the analyst tackles this next, adding the appropriate cross references and support.

Technical Specification 3: Unanimous Consensus

Decisions within a community are reached through voting. Decisions need to be unanimous. Should a decision be positive, the operation approved by the decision is executed. Should a decision be negative, the operation will not be performed.

+ Establishes shared responsibility within a community.

Support: Privacy Requirement 2
Related: Technical Specification 1, 2

Finally, the mechanism by which users are made aware of decisions within the communities they belong to need to be specified.

Technical Specification 4: Notification

Should an operation require the involvement of the community, all members of the community are notified of the requirement to cast a vote.

+ Provides awareness of activity in the community.

Support: Privacy Requirement 2
Related: Technical Specification 1, 2

These specifications[6] are the basis of the **implementation** of the first **prototype** of the CMail System [DeHart 2013] and allow the transition from the **design loop** to the **evaluation loop**.

The analyst now conducts a user study of CMail within the company [DeHart 2013]. Two main issues emerge from observing the study participants' interaction with the system and their feedback The first issue involves the voting mechanism used. Study participants felt that establishing unanimous consensus took too long to be practical. Thus, the analyst updates the claim of Technical Specification 3 to reflect this disadvantage

Technical Specification 3: Unanimous Consensus (revised)

Decisions within a community are reached through voting. Decisions need to be unanimous. Should a decision be positive, the operation approved by the decision is executed. Should a decision be negative, the operation will not be performed.

+ Establishes shared responsibility within a community.
− Establishing unanimous consensus is too time intensive.

Support: Privacy Requirement 2
Related: Technical Specification 1, 2

Since voting mechanisms are not part of the privacy requirements but rather a purely technical concern, the analyst decides to explore alternatives. The obvious alternative to unanimous consensus is consensus of a majority of the community members, so the analyst establishes a new specification:

[6] Note that these specifications reflect the definitions used for the Community Oriented Privacy System in [Kafura et al. 2011] which is implemented in [DeHart 2013].

Technical Specification 5: Majority Consensus

Decisions within a community are reached through voting. Decisions are reached by a majority of. Should a decision be positive, the operation approved by the decision is executed. Otherwise, the operation will not be performed.

+ Establishes shared responsibility within a community.
+ Not as time intensive as unanimous consensus.

Support: Privacy Requirement 2

Related: Technical Specification 1, 2, 3

The second main issue emerging from the evaluation was the fact that study participants mistook community tags for recipient lists of the e-mail to be sent. Thus, the analyst updates the claim of Technical Specification 1 with this information.

Technical Specification 1: Community Tag (revised)

A community is represented through a "community tag" and defined as a collection of uniquely identified users. Community membership is established through consensus. An e-mail annotated with one or multiple "community tags" cannot be forwarded to any person outside of the community.

+ Represents communities.
+ Establishes dissemination boundary.
− Commonly mistaken for recipient list.

Support: Privacy Requirement 1

After the update, the analyst turns to examining whether this issue arose due to a mismatch of the technical specification with the privacy requirements. However, Technical Specification 1 represents the stipulations of Privacy Requirement 1 almost verbatim, so there is reason to believe that the information within the model itself is not accurate. And indeed, the analyst stumbles over a quotes within the focus group study data that shed light upon a potential mismatch:

> ***Quote 6*****:** *"Keep this within this group!"*

Upon reflecting on this quote, the analyst realizes that annotations like "do not forward" only tag the information, yet do not specify the actual boundary that the information should have. This indicates a problem with the specification in Privacy Requirement 1 that links Concepts 1 and 2. Since the established relationship between the two concepts is logically sound and Concept 1 is reflected almost verbatim in Quote 6, the analyst turns to verifying the content of Concept 2. And in fact, another quote found within the data highlights the issues with the concept:

> ***Quote 7*****:** *"Email chains will start to build up, people add three people they think might need to be part of the conversation, but in fact they don't need to be. And then those three people are on there for the rest of the conversation even though we determined ten emails back they don't need to part of this anymore."*

The quote reveals that, while communities can be considered dissemination borders, they are much more fluid than Concept 2 suggests. Reflecting on the differences of Quotes 3, 4, and 7, the analyst realizes that communities can be nested. While larger communities (like e.g., the HR team, Quote 3) are less fluid, sub communities centered around a specific task can be quite fluid (Quote 7). The analyst decides to call the larger, more static communities *strategic communities*. The smaller, more fluid communities receive the name *tactical communities*. This results in the following changes in Concept 2:

> ***Concept 2: Community (revised)***
> There are two types of communities. *Strategical communities* are centered around strategic goals of the company. They are the *outermost dissemination boundary* of information deemed private within the community. Membership within strategical communities are based on company structure. *Tactical communities* are centered around the day-to-day tasks within the company. They are the *chosen dissemination boundary* for task-related information. Membership in tactical communities is limited to members of their containing strategic community and determined ad-hoc.
> *Support:* Quote 2, 3, 4, 6, 7

Given the revision in Concept 2, the analyst now can either try to further refine the privacy requirements through iteration of the steps of the **Requirements Modeling Loop**, or alternatively go on to revise the privacy requirements and re-iterate the **Implementation Loop**.

3.5 Summary

In this chapter, we set out to address the challenge of transforming unstructured, qualitative data into structured domain knowledge (cf. Q 3). To that end, we examined existing analysis processes in intelligence analysis, the social sciences and software engineering (cf. Section 3.1). Our evaluation of the shared characteristics of these processes in Section 3.2 lead us to three **process requirements** and three **artifact requirements** respectively. Based on these requirements and the **data collection requirements** of Section 2.5, we developed the Privacy Requirements Engineering process (PREprocess; cf. Section 3.3). The application example in the previous section demonstrated the effectiveness of the PREprocess in guiding the iterative refinement and incremental structuring of information throughout the analysis process, as well as its potential for integration into practice.

However, in our description of the PREprocess we not directly address the artifact requirements developed in Section 3.2.3. Furthermore, we face the potential of diminishing the quality of the captured privacy-related information through its transformation into a structured domain model during the execution of the process. Thus, we are faced with the following problem:

(P4) Data models need to fulfill artifact requirements and maintain close representation of complexity while providing appropriate structure.

To address this particular problem, we will need to answer the following question:

(Q4) How can we represent complex social behavior while providing structure and meeting artifact requirements?

We will address this challenge in the following chapter.

Chapter 4

Representational Requirements of Privacy Domain Models

The requirements that a representation has to fulfill to be suitable for the capture of privacy domain information are best developed through an example. The following data sample was taken from a survey on privacy in domestic environments [Radics and Gračanin 2011].

> **Question:** *"Assume you are in the kitchen. Under what circumstances would you be comfortable with another person opening the refrigerator and/or the kitchen cabinets?"*
> **Participant:** *"If I knew them very well, if they lived there, or I knew that they were close friends with someone that lived there and they were getting something specific."*

Figure 4.1: Example of a participant's specific conditions for comfort in a given scenario.

Examining this sample, one can identify a number of components of the domain semantics and user preferences. These components can be interpreted as a number of actors and their properties. The question identifies two actors: inhabitant and intruder, without specifying the identity of the latter. The answer of the participants introduces a potential third actor: a cohabitant.

All actors have a set of properties that further define them and their relationships to each other. Both inhabitant and intruder are located in the kitchen. The potential intruder is opening the refrigerator and kitchen cabinets while they are in the kitchen. The participant's answer establishes a number of different relationships between the inhabitant and the intruder: familiarity, cohabitation, and shared acquaintance. These properties, however, cannot be interpreted as *static properties* of the actors that hold over arbitrary periods of time. Arguably all properties mentioned have a certain *duration*. For example, neither inhabitant nor intruder are likely to permanently stay in the kitchen. We will refer to these properties as *temporal properties*.

It is furthermore important to note that there is no absolute timing information available. For example, the sample does not contain information about how long the rummaging of the intruder took. However, it can be established that the rummaging took place while both inhabitant and intruder were located in the kitchen. This is a *partial order* of the beginnings and endings (or *semi-intervals* [Freksa 1992]) of events. Moreover, the duration of the intruder being in the kitchen establishes a *temporal constraint* on the duration of the rummaging.

Furthermore, while one can establish that the rummaging started after the actors entered the kitchen and ended before they left, it is impossible to say whether the intruder first opened the refrigerator and then the cabinet or vice versa. This is an example of a *parallel episode* [Patnaik et al. 2008]. Finally, all the semantic information provided in the sample can be interpreted as prerequisites of the participant feeling comfortable. They establish a *semantic temporal constraint* as the the participant's comfort is dependent on the semantic information being valid,

Thus, we can define our representational requirements:

Definition ***(Representational Requirements)***

A representational format for privacy domain models needs to support:

1. static and temporal properties
2. durations
3. partial ordering of time points
4. parallel episodes
5. temporal constraints, and
6. semantic temporal constraints.

4.1 Review of Semantic and Temporal Representations

Since we need to represent the privacy related data, we must first examine existing semantic and temporal representations in order to determine whether they can be used for the representation of application-specific privacy models.

Description Logics (DL) [Nardi and Brachmann 2003], often referred to as Ontologies, are frequently used both within ubiquitous computing and other domains for their power of semantic representation [Biamino 2011]. They allow to distinguish between intensional knowledge (the terminology defined through general knowledge of a domain, called the ‘T-Box) and extensional knowledge or assertional knowledge (the knowledge specific to a particular problem in the domain, referred to as ‘A-Box’). In their core, DL represent knowledge in atomic concepts (unary predicates), atomic roles (binary predicates), and individuals (constants). Given the intensional and extensional knowledge, it is often useful to reason about this knowledge. DL were developed specifically to address the shortcomings of languages like KL-ONE [Brachman and Schmolze 1985], as reasoning in those languages is intractable [Baader and Nutt 2003]. DL reasoners can decide the satisfiability of the T-Box as well as establish the subsumption relationship between concepts as predicates are restricted to binary predicates. Furthermore, they can check the consistency of the A-Box and establish the instance-relationship between individuals and concepts.

A downside of DL is their lack of support for capturing dynamic data as they do not contain a notion of time [Krieger 2010]. It is, however, possible to extend them with temporal reasoning capabilities. Krieger identifies four approaches: addition of a temporal argument, application of a meta-logic predicate, event reification, and the use of time slices [Krieger 2010]. One can further distinguish extensions by whether they use intervals or time-points to represent time; whether temporal relationships are expressed explicitly through temporal operators or are contained implicitly in the representation of state changes; and whether a concept is represented as a series of time slices or as a collection of distinct parts (for an extensive discussion, see [Artale and Franconi 2000]). Finally, it is important to note the inverse relationship between expressivity of a temporal representation and its decidability [Artale and Franconi 2000]. Thus, while DL can be used to represent *static properties*, they are not well suited to represent *temporal properties*.

Mörchen [2007] provides a detailed overview of the options for representing temporal relationships. Primarily, approaches can be categorized into *time point* based approaches and *time interval* based approaches. Both time points and time intervals can be grouped into sets and sequences. Sequences can further be contiguous (without gaps), univariate (consisting of single series), or multivariate (consisting of multiple, potentially differently sampled series). The data can further be of symbolic or numerical nature. There is a large number of representations that directly address the representation of such temporal relationships.

Among the most often cited works in this area is Allen's temporal logic [Allen 1983]. His work was motivated by the necessity of dealing with incomplete knowledge about the concrete timing of events, the desire to support varying grains of modeling, as well as persistence of facts over time. As a result, he defined 13 temporal operators on intervals: before, after, equal, meets, met by, overlaps, overlapped by, during, contains, starts, started by, finishes, and finished by. These 13 relationships establish a strict order on interval boundaries.

Freksa [1992] observes the difficulty of modeling data containing very little information about the concrete relationships between events using Allen's representation. He states that Allen's relationships require the temporal relations between event boundaries to be completely known, which is not always realistic. To address this issue, Freksa introduces 17 relationships on semi-intervals (the start and end points of an interval) that only require the knowledge of between one and three relationships between the semi-intervals (as opposed to requiring all four in Allen's model). Formally, Freksa's model allows the representation of a partial order between event boundaries. Furthermore, Allen's 13 relationships can be represented using Freksa's 17 relationships. The representational power of Allen and Freksa's work has been used in the ubiquitous computing community (e.g., [Kostakis et al. 2011]) as well as other domains. While both Allen's and Freksa's representation meet the requirements of representing durations, partial ordering of time points, as well as temporal properties, they lack the expressive power to represent temporal constraints or semantic temporal constraints. To be precise, they allow specifying the order of events, but not their timing.

Table 4.1: Capabilities Across Approaches.

	Temporal Property		**Temporal Order**		**Semantic Property**		
Approach	Temporal Constraint	Duration	Partial Order	Parallel Episode	Static Property	Temporal Property	Semantic Temporal Constraint
DL						(X)	
Allen			X	X		X	
Freksa			X	X		X	
SISP		X	X				
SIPO		X	X	X	X		
TSKR	X	X	X	X	X		
TRL	X	X	X	X	X	X	

Mörchen and Fradkin [2010] proposed using semi-intervals in two forms, semi-interval sequential patterns (SISPs) and semi-interval partial orders (SIPOs), to provide a richer and more flexible representation of patterns among interval and point data. SISPs are a way to represent an ordered set of semi-intervals, whereas SIPOs adds the support for the representation of parallel episodes. Mörchen [2006] presents a related approach: Time Series Knowledge Representation (TSKR), an extension to Unification-based Temporal Grammar (UTG) [Ultsch 2004]. It introduces the temporal concepts of duration, coincidence, and synchrony to provide a way to represent temporal constraints. However, TSKR lacks the capabilities to represent temporal properties. The Temporal Reference Language (TRL) [Panayiotopoulos 2000] creates a unifying representation for temporal points and intervals. It can be used to represent durations, parallel episodes, temporal constraints, and temporal properties. However, it falls short in representing semantic temporal constraints.

Table 4.1 presents an overview of the capabilities supported by the approaches discussed previously. No current representational approach covers all requirements. To cover all requirements, the representational power of current approaches have to be combined. Thus, a privacy analysis process has to meet the requirements outlined in section 3.2 *and* provide a representation that meet the requirements shown in Table 4.1.

4.2 The Privacy Domain Modeling Language (PDML)

The goal of the Privacy Domain Modeling Language (PDML) is to provide a representational syntax for a **domain model** that meets the requirements presented in sections 3.2.3 and 4.1. Moreover, following the reasoning of Corbin and Strauss [2008], PDML should capture the complexity of the underlying data as closely as possible. We adopt a data-centric approach and define the domain model as a knowledge base consisting of a sequence of **statements** about the underlying data[1]:

knowledgeBase ::= ’KnowledgeBase(’ **knowledgeBaseID** **label** { **statement** } ’)’
label ::= ’label(’ *xsd:string* ’)’

As we have seen in Section 3.3.1, both Grounded Theory [Corbin and Strauss 2008] and the Grounded and Linguistic-Based Requirements Analysis Procedure (GLAP) [Chakraborty et al. 2015] rely on the extraction of concepts through *open coding* and their relationships through *axial coding*. Thus it follows that concepts and relationships need to be represented in PDML. Examining open and axial coding, it becomes apparent that concepts can be described based on their distance to the actual data. This aligns well with the distinction between terminology (intensional knowledge) and assertions (extensional knowledge) found in ontologies [Nardi and Brachmann 2003]. Thus, we can distinguish between a **concept** on the intensional level and its **instances** on an assertional level. Similarly, we can distinguish between an intensional **role** and its **relationship** instances. Furthermore, concepts and roles are collectively referred to as **“terms”**, whereas instances and relationship are called **assertions**.

statement ::= **assertion**
| **term**
assertion ::= **instance**
| **relationship**

[1] We provide the syntax of PDML in the Extended Backus-Naur Form used for the definition of the abstract syntax of the Web Ontology Language (OWL) with XML Schema Datatypes [World Wide Web Consortium (W3C) 2004a,b] from the *xsd* namespace. The initial version of PDML was created collaboratively with Chreston Miller. The current version incorporates feedback from the research community and adjustments to improve fit for the privacy domain.

term ::= **concept**

| **role**

We adopt the distinction between a symbol and its description found in GLAP, and require that every term and assertion have both a **label** and a **description**. Furthermore, to enable traceability of terms and assertions back to the underlying data, we provide the option to specify **support** containing links into the data. To allow for the creation of hierarchies, both concepts and roles can specify their ancestors through instantiation of the **super** relationship. Similarly, assertions can be linked to the terms they instantiate through the **type** relationships. Also, while terms — as intensional definitions — are universally valid, assertions can either be universally valid or only valid for a certain **duration**. Assertions with limited validity are also called *fluents* [McCarthy and Hayes 1969]. However, terms can specify whether their instances are universally valid (‘endurant’) or have limited validity (‘perdurant’) by specifying their **validity**. These characteristics are sufficient to provide a definition of concepts and instances:

instance ::= ’Instance(’ **instanceID label description** [**duration**]

{ ’type(’ **conceptID** ’)’ } { **support** } ’)’

concept ::= ’Concept(’ **conceptID label description** [**validity**]

{ ’super(’ **conceptID** ’) } { **support** } ’)’

description ::= ’description(’ *xsd:string* ’)’

support ::= ’support(’ *xsd:anyURI* ’)’

validity ::= ‘endurant’ |‘perdurant’

For the definition of roles we have to address the question of whether they should relate *any combination* of terms to each other, or whether their **domains** and **ranges** should be limited to concepts only. This also affects whether relationships are only defined between instances or between arbitrary assertions. The example in Figure 4.1 provides the answer. In the question, the participant is asked under which circumstances they would be comfortable with another person opening their refrigerator. This question relates two relationships to each other. Namely, “opening” and “being comfortable with”. Thus, we define roles as relations between arbitrary terms, and relationships as relations between arbitrary assertions. Furthermore, we allow relationships relate an arbitrary number of domains with an arbitrary number of ranges, implying the creation of unnamed groups. This leads to the following definitions:

relationship ::= ’Relationship(’ **relationshipID** **label** **description** [**duration**]
{ ’type(’ **roleID** ’)’ } { **support** }
domain **range** ’)’
domain ::= ’domain(’ **assertionId** ’)’ { **domain** }
range ::= ’range(’ **assertionId** ’)’ { **range** }

role ::= ’Role(’ **roleID** **label** **description** **validity**
{ ’super(’ **roleID** ’) } { **support** }
{ ’domain(’ **termID** ’) } { ’range(’ **termID** ’) } ’)’

termID ::= **conceptID** | **roleID**
assertionID ::= **instanceID** | **relationshipID**

At this point, we need to define our notion of duration. We adopt the notion of Freksa [1992], defining a duration as a time interval of a certain **length** that is represented by two **semi-intervals**, namely its beginning and end. Since we have to be able to account for incomplete knowledge about exact timing of semi-intervals, we cannot require an exact time point to be known for a semi-interval. Similarly, we can allow for the length of a duration to exist without knowing the exact timing of its beginning or end. Moreover, we might know neither length nor timing of a duration. However, we do know that every duration has a beginning and an end. This leads to the following definition:

semiInterval ::= ’SemiInterval(’ **semiIntervalID** [**timepoint**] ’)’

duration ::= ’Duration(’ **durationID** ’beginning(’ **semiInterval** ’)’
’end(’ **semiInterval** ’)’ [**length**] ’)’

timepoint ::= ’timepoint (’ *xsd:dateTime* ’)’.
length ::= ’length(’ *xsd:duration* ’)’.

Finally, to allow for temporal constraints, semantic temporal constraints, and ordering, we need to define the **order** of both durations and semi-intervals. Note that this definition allows for the comparison of durations and semi-intervals *without* requiring knowledge about the concrete length or points in time, respectively. The order of durations and semi-intervals are defined as top-level statements.

statement ::= **order**
order ::= ’Order(’ **orderID** **durationID** **comparator** **durationID** ’)’
| ’Order(’ **orderID** **semiIntervalID** **comparator** **semiIntervalID** ’)’

comparator::= ’<’ | ’≤’ | ’=’ | ’≥’ | ’>’

These definitions provide the syntax of the Privacy Domain Modeling Language. A full reference is provided in Appendix A.

4.3 Example of Domain Modeling with PDML

To show that PDML meets the **representational requirements** presented at the beginning of this chapter, we need to demonstrate support for temporal properties, durations, partial ordering of time points, parallel episodes, temporal constraints, and semantic temporal constraints. Of these requirements, temporal properties, durations, and partial ordering of time points are trivially supported through the definition of term validity and assertion durations. Thus we only need to show support for parallel episodes, temporal constraints, and semantic temporal constraints.

Recall the data samples presented at the beginning of this chapter:

> **Question:** *"Assume you are in the kitchen. Under what circumstances would you be comfortable with another person opening the refrigerator and/or the kitchen cabinets?"*
> **Participant:** *"If I knew them very well, if they lived there, or I knew that they were close friends with someone that lived there and they were getting something specific."*
> [Radics and Gračanin 2011]

We can start modeling by identifying the different *instances* provided in the question. There are two actors, the participant and another person we will call the 'intruder'. Furthermore, we are given the location of the scenario, namely the kitchen. Finally, the intruder interacts with two objects, one (or more) cabinet and the refrigerator. This leads to the following definitions:

Instance(`I-1`, label('*Participant*'), description('*The participant.*'))
Instance(`I-2`, label('*Intruder*'), description('*The intruder – the other person in the kitchen.*'))
Instance(`I-3`, label('*Kitchen*'), description('*The kitchen – location of the scenario.*'))
Instance(`I-4`, label('*Cabinet*'), description('*The kitchen cabinet being rummaged through.*'))
Instance(`I-5`, label('*Refrigerator*'), description('*The refrigerator being searched.*'))

We omit the fact that each of these instances represents a *fluent* with limited validity, since each instance is valid for the entire duration of the scenario. We can now model the fact that both the participant and the intruder are located within the kitchen:

Relationship(`R-1`, label('*hasLocation*'),
        description('*The participant is in the kitchen.*'),
        domain(`I-1`), range(`I-3`),
        Duration(`D-1`, beginning(**SemiInterval**(`SI-1`))
                end(**SemiInterval**(`SI-2`))))
Relationship(`R-2`, label('*hasLocation*'),

description('*The intruder is in the kitchen.*'),
domain(`I-2`), range(`I-3`),
Duration(`D-2`, beginning(**SemiInterval**(`SI-3`))
end(**SemiInterval**(`SI-4`))))

We can, furthermore, assert that both participant and intruder are in the kitchen at roughly the same time. This means, that the participant leaves the kitchen after the arrival of the intruder, and vice versa. Or, as Freksa [1992] states, the events *overlap*:

Order(`O-1`, `SI-2` $\geq$ `SI-3`)
Order(`O-2`, `SI-4` $\leq$ `SI-1`)

We also know that the intruder opens the cabinets and the refrigerator:

Relationship(`R-3`, label('*opens*'),
description('*The intruder opens the cabinet.*'),
domain(`I-1`), range(`I-2`),
Duration(`D-3`, beginning(**SemiInterval**(`SI-5`))
end(**SemiInterval**(`SI-6`)))
Relationship(`R-4`, label('*opens*'),
description('*The intruder opens the refrigerator.*'),
domain(`I-1`), range(`I-4`),
Duration(`D-4`, beginning(**SemiInterval**(`SI-7`))
end(**SemiInterval**(`SI-8`)))

We also know that the intruder can only open the cabinets or refrigerator while being in the kitchen. Thus, we can establish these *temporal constraints* as through the following temporal orders:

Order(`O-3`, `SI-3` $\leq$ `SI-5`)

Order(`O-4`, `SI-4` $\geq$ `SI-6`)
Order(`O-5`, `SI-3` $\leq$ `SI-7`)
Order(`O-6`, `SI-4` $\geq$ `SI-8`)

Furthermore, as we do not know in what order the intruder opens the cabinet and refrigerator, these statements also establish a *parallel episode*. The above statements fully describe the base components of the scenario given in the question. The response of the participant is more complex. Therefore, we will only tackle the first part of the statement.

The first part of the response establishes a relationship between the participant and the intruder: 'knowing'. Furthermore, the participant qualifies this relationship with a value, namely 'very well'. We can represent this statement with one instance and two relationships:

Instance(`I-6`, label('*VeryWell*'), description('*A qualifier signifying strength of a relationship.*'))
Relationship(`R-5`, label('*knows*'),
description('*The participant knows the intruder.*'),
domain(`I-1`), range(`I-2`),
Duration(`D-5`, beginning(**SemiInterval**(`SI-9`))
end(**SemiInterval**(`SI-10`)))))
Relationship(`R-6`, label('*hasQualifier*'),
description('*The participant knows the intruder very well.*'),
domain(`R-5`), range(`I-6`),
Duration(`D-6`, beginning(**SemiInterval**(`SI-11`)))))
end(**SemiInterval**(`SI-12`))

Relationship `R-6` highlights the advantage of defining relationships between arbitrary assertions, as this statement relates the relationship 'knows' with the instance 'VeryWell'. Finally, the *semantic temporal constraint* of the participant knowing the intruder very well as prerequisite for feeling comfortable can be modeled as follows:

```
Relationship( R-7, label('isComfortableWith'),
              description('The participant is comfortable with the intruder's rummaging.'),
              domain( I-1 ), range( R-3, R-4 ),
              Duration( D-7, beginning( SemiInterval( SI-13 ) )
                             end( SemiInterval( SI-14 ) ) ) )
Relationship( R-8, label('isPrerequisiteFor'),
              description('The participant needs to know the intruder very well to be comfortable.'),
              domain( R-6 ), range( R-7 ),
              Duration( D-8, beginning( SemiInterval( SI-15 ) )
                             end( SemiInterval( SI-16 ) ) ) )
Order( O-7, SI-11 < SI-13 )
```

Thus, a semantic temporal constraint can be represented by combining a relationship with a temporal order, whereas temporal constraints only require the establishment of one or more temporal orders. Moreover, relationship `R-7` demonstrates the benefit of using a set of assertions as range.

4.4 Summary

In this chapter, we set out to address the challenge of finding a representation that allows to represent complex social behavior while providing structure and meeting the artifact requirements defined in Section 3.2.3 (see also Q 4). To that end, we characterized the complexity of a representative example (cf. Figure 4.1) into a set of six **representational requirements**. Consequently, we evaluated existing representational approaches in Section 4.1 and determined that no representation met all requirements (cf. Table 4.1). Thus, we developed the Privacy Domain Modeling Language (PDML) to address our need (cf. Section 4.2) and demonstrated its expressiveness in the previous section. However, while we have shown support for the representational requirements, we now face the challenge of evaluating the **artifact requirements** presented in Section 3.2.3.

This is the focus of the following chapter.

Chapter 5

Evaluation Methodology

In Hypothesis 1, we claim that “it is possible to leverage domain-knowledge and requirements gathering approaches to construct application-specific privacy domain models.” We have introduced the Privacy Requirements Engineering process (PREprocess) in Section 3.3 and the Privacy Domain Modeling Language (PDML) in Section 4.2 to support this hypothesis. We have claimed that, together, they allow an analyst to collect data on privacy phenomena (Q 1) and to transform the resulting unstructured information into a structured domain model (Q 3) with sufficient expressivity (Q 4) that is suitable for the use in privacy design frameworks (Q 2). Now we are faced with the challenge of validating these claims.

While we have provided application examples for both the PREprocess (cf. Section 3.4) and PDML (cf. Section 4.3), these examples are not sufficient, as they are simulations of their use. Thus, validation needs to be conducted through the application of the PREprocess and PDML to a real modeling task. Yet their application itself, while likely producing some outcome, does not yield validation of our claims. Thus, we need criteria for the evaluation of the process and its outcomes, and demonstrate their integration with existing approaches.

Following our reasoning in Section 3.2.3 and the beginning of Chapter 4, we have four sets of requirements that can serve as evaluation criteria. The *data collection requirements* provide us with a checklist of step to be performed, and thus can be demonstrated through the application of the PREprocess to a real modeling task. This method can also be applied to the *process requirements* (support of incremental structuring, iterative refinement, data and model-driven analysis), as they are also purely procedural in nature. Similarly, the *representational requirements* (static and temporal properties, durations, partial order, parallel episodes, temporal and semantic temporal constraints) are embodied within the syntax of PDML and can be shown through its use. This leaves us with the *artifact requirements*: support for **verification of consistency**, **validation of completeness**, and **traceability**.

Of these criteria, *traceability* is arguably the easiest to evaluate, as it relies on either manual linking of statements to the data by the analyst or through architectural support. Furthermore, PDML explicitly provides the capability of establishing such links in the form of 'support' for both assertions and terms, as well as through the term hierarchy (cf. Section 4.2). Thus, evaluation of traceability simply entails answering the question "Can every statement be traced back to the source data?"

Verification of consistency and the **validation of completeness** prove more challenging. Bjørner [2006] states that "Verification gets the domain model right." whereas "Validation gets the right domain model." We will address both of these processes in turn.

5.1 Verification of Consistency

As suggested in Section 3.3 we can adapt the metrics of Chakraborty et al. [2015] from the Grounded and Linguistics-Based Analysis Process (GLAP). They define four deficiencies. *Incompleteness* refers to descriptions without assigned symbol. Symbols without assigned description are called *meaningless*. *Redundancy* identifies all those descriptions assigned to multiple symbols, whereas *ambiguity* refers to symbols with multiple assigned descriptions.

To determine whether these metrics can be applied to the statements of a PDML knowledge base, we have to adapt their definitions to reflect our components. Whereas GLAP deals with *symbols* and *descriptions*, PDML contains *assertions* and *terms*. Furthermore, as mentioned in Section 3.3, it is useful to distinguish between *leaf terms* and *taxonomic terms*:

> **Definition** ***(Leaf Terms and Taxonomic Terms)***
>
> A **leaf term** is a term that does not have any sub-terms.
>
> Conversely, a **taxonomic term** it a term that has sub-terms.

We will furthermore require that only leaf terms be used for the categorization of assertion. To adapt the above definitions, it is possible to map symbols to assertions and descriptions to terms. Alternatively, we can interpret chunks within the data as symbols, and assertions as their descriptions. A third option would be interpreting leaf terms as symbols and taxonomic terms as their descriptions. This leads to the following definitions of *incompleteness*:

> **Definition** ***(Incompleteness)***
>
> An *assertion* is **incomplete**, if it is not supported by any *data*.
>
> A *leaf term* is **incomplete**, if it is not supported by any *assertions*.

Taxonomic terms cannot be incomplete, as lack of support through sub-terms would make them leaf terms. Similarly, we can define *meaninglessness* as follows:

> **Definition** ***(Meaninglessness)***
>
> An *assertion* is **meaningless**, if it does not support any *term*.

We could establish meaninglessness for both data (in case it does not give rise to assertions) and leaf terms (in case they do not support taxonomic terms). However, the former goes beyond the scope of PDML and would establish an additional architectural requirement. The latter, only has merit if we require the taxonomy to have a single source. This, however, is a modeling decision or convention we will not enforce.

Finally, *ambiguity* can be defined as:

> **Definition** ***(Ambiguity)***
>
> An *assertion* is **ambiguous**, if it supports multiple *terms*.

Similar to the meaninglessness of leaf terms, defining the ambiguity of assertions is a modeling choice. We suggest using this convention to allow leaf terms to form a partition of the assertions. Once again, it would be possible to define the ambiguity of data, requiring a one-to-one relationship between chunks and assertions. This would establish another architectural requirement beyond the scope of PDML. Ambiguity of leaf terms makes only limited sense, as multiple classifications enrich the taxonomy.

For the same reason we will not adapt the notion of *redundancy*. In our case, we encourage the support of assertions by multiple data points, as well as the support of leaf terms by multiple assertions, and so on. Redundancy does not reveal inconsistency or lack of quality of a model, but rather reflects the strength of support of assertions and terms within the data.

5.2 Validation of Completeness

In Chapter 3 we introduced the concepts of *conceptual saturation* and *completeness*. Corbin and Strauss [2008] define *conceptual saturation* as the state where running more participants will not introduce new information into the domain model. Completeness is the (desired) degree of coverage of phenomena present in the domain by the domain model [Bjørner 2006]. It is apparent that the two concepts are inherently linked, with conceptual saturation being a prerequisite for a notion of completeness.

However, neither definition includes a readily available metric or measure to determine whether concept saturation or completeness have been achieved. Corbin and Strauss [2008] rely on the judgment of the researcher (or analyst) to gauge concept saturation, whereas [Bjørner 2006] recommends validation of completeness and accuracy through conversation with stakeholders. This validation process can be interpreted as further *theoretical sampling* of the target domain, since stakeholders are asked to provide information on the accuracy and coverage of the domain model. Should this process not yield contradicting or additional information, the domain model is said to be complete. This is arguably the case once the validation process reaches conceptual saturation (i.e., does not change based on new data). Therefore, a measure of conceptual saturation could be used to determine completeness of the domain model. We can even interpret reaching a certain threshold of this measure as the criterion for the termination of the domain modeling phase.

The remaining challenge, thus, lies in determining an appropriate measure or metric for the concept of conceptual saturation. Naturally, this measure is in great part dependent on the representation chosen for the domain model. Namely, a domain model based on categories elicited by pure Grounded Theory [Corbin and Strauss 2008] will certainly require an at least slightly different approach than a domain model in PDML. The naive approach of simply counting the number of concepts after each participant can give a quick-and-dirty insight into whether or not the domain has been fully explored. However, it does not easily yield information on what concepts are strongly supported by the data or which concepts require further investigation. In other words, it does not quantify the information contributed by different parts of the model. Therefore, we will investigate whether notions of information content and information gain used in information theory can be applied to domain models.

5.2.1 Entropy and Information Gain

Since its inception in the mid twentieth century, information theory has dealt with the quantification, compression, encoding, and transmission of information (e.g., [Shannon 1948; Tribus 1961; Rényi 1961]). Among the most important concepts of the field are *self information* and *entropy*.

Definition ***(Self Information and Entropy)***
Let X be a discrete random variable with possible values $\{x_1, \ldots, x_n\}$ and
let $P(X)$ denote its probability mass function.
The **self information** of x_i with symbol $I(x_i)$ is given as:

$$I(x_i) = \log_2 \frac{1}{P\left(x_i\right)} = -\log_2 P\left(x_i\right) \tag{5.1}$$

Self information is also referred to as the **surprisal** of encountering x_i [Tribus 1961].

Shannon [1948] defines the **entropy** of X with symbol $H\left(X\right)$ as the expected value of $I(X)$:

$$H(X) = E\left[I(X)\right] = \sum_{i=1}^{n} P(x_i)I(x_i) = -\sum_{i=1}^{n} P(x_i)\log_2 P(x_i) \tag{5.2}$$

This is the equivalent of the weighted average of the self information of the x_i.

The unit of the Shannon entropy are *shannons* or *bits*.

Formally, the Shannon entropy[1]is a quantification of the randomness of a system. In simpler terms, it represents the minimum amount of information required to represent the state of the system. Besides providing a measure for information entropy also has some desirable characteristics. First, Hartley [1928] found that the *maximum entropy* of a system is determined by the size of its support. Second, it is possible to determine the *redundancy* of information in any given system.

Definition ***(Maximum Entropy, Relative Entropy, and Redundancy)***

Let X be a discrete random variable with possible values $\{x_1, \ldots, x_n\}$.

Hartley [1928] shows that the entropy of X is highest when the x_i are uniformly distributed. Thus, the **maximum entropy** (also called Hartley entropy) H_0 has the value:

$$H_0(X) = \log n = \log|X| = -\log\frac{1}{|X|} = -\sum_{x_i \in X}\frac{1}{|X|}\log_2\frac{1}{|X|} \tag{5.3}$$

The **relative entropy** H_r is given as the ratio of the entropy of X to the maximum entropy:

$$H_r(X) = \frac{H(X)}{H_0(X)} \tag{5.4}$$

Finally, Shannon [1948] defines the **redundancy** $D(X)$ of information in X as:

$$D(X) = 1 - H_r(X) \tag{5.5}$$

The value of $D(X)$ lies between 0 and 1, and can be interpreted as the maximum compression ratio for messages using $\{x_1, \ldots, x_n\}$.

Entropy provides us with an easy measure of both the total information content of a system and

[1] Other formulations of entropy exist with different bases of the logarithm. Rényi [1961] generalized the concept of entropy to entropies $H_\alpha(X)$ with order α (the Shannon entropy being $H_1(X)$ and the Hartley entropy being $H_0(X)$).

the redundancy within it. However, we might want to know the information contained in the partitioning of assertions into terms (i.e., the relationship between two random variables). Thus, we need definitions for the *joint entropy* of two variables, as well as for the *conditional entropy* of one variable given another. Shannon [1948] provides the following definitions:

Definition *(Joint and Conditional Entropy)*
Let $X = \{x_1, \ldots, x_n\}$ and $Y = \{y_1, \ldots, y_m\}$ be discrete random variables, and let $P(x_i, y_j)$ and $P(x_i|y_j)$ denote their joint probability and conditional probabilities. The **joint entropy** of X and Y, denoted by $H(X, Y)$ is defined as:

$$H(X,Y) = -\sum_{x_j \in X} \sum_{y_j \in Y} P(x_i, y_j) \log_2 P(x_i, y_j) \tag{5.6}$$

The **conditional self information** $I(X = x_i|Y = y_j)$ of x_i given y_j is defined as:

$$I(X = x_i|Y = y_j) = -\log_2 P(x_i|y_j) \tag{5.7}$$

The **conditional entropy** $H(X|Y = y_j)$ of X given y_j is defined as:

$$H(X|Y = y_j) = -\sum_{x_i \in X} P(x_i|y_j) \log_2 P(x_i|y_j) \tag{5.8}$$

The **conditional entropy** of X given set Y is defined as:

$$\begin{aligned} H(X|Y) &= \sum_{y_j \in Y} P(y_j) H(X|Y = y_j) \\ &= -\sum_{y_j \in Y} P(y_j) \sum_{x_i \in X} P(x_i|y_j) \log_2 P(x_i|y_j) \\ &= -\sum_{x_i \in X, y_j \in Y} P(x, y) \log_2 P(x_i|y_j) \\ &= -\sum_{x_i \in X, y_j \in Y} P(x, y) \log_2 \frac{P(x_i, y_j)}{P(y_j)} \\ &= \sum_{x_i \in X, y_j \in Y} P(x, y) \log_2 \frac{P(y_j)}{P(x_i, y_j)} \end{aligned} \tag{5.9}$$

$$= -\sum_{x_i \in X, y_j \in Y} P(x,y) \log_2 P(x,y) + \sum_{x_i \in X, y_j \in Y} P(x,y) \log_2 P(y_j)$$
$$= H(X,Y) - H(Y)$$

This is the equivalent of the weighted sum of all $H(X|Y = y_j)$ by the $P(y_j)$.

The joint entropy provides us with the information when jointly observing both variables. The conditional entropy provides us with the amount of information of one variable given some information about the other. However, what is the *mutual* information of the two variables? Or what information do we *gain* from partitioning one variable to create the other? One particular instance where this issue is of importance is when deciding branching order of a decision tree in machine learning (e.g., Quinlan [1986][Quinlan 1986; Harris 2001; Russell and Norvig 2003; Ibrahim et al. 2012]). *Mutual information* (or *information gain*) provides a measure for this information.

Definition ***(Mutual Information)***
Let X be a discrete random variable with possible values $\{x_1, \ldots, x_n\}$,
let Y be a discrete random variable with possible values $\{y_1, \ldots, y_m\}$, and
let $P(x_i, y_j)$, $P(x_i|y_j)$, $P(y_j|x_i)$ denote their joint and conditional probabilities.
The **mutual information** [Peng et al. 2005] or **information gain** [Quinlan 1986] of X and Y with symbol $I(X;Y)$ is defined as:

$$I(X;Y) = \sum_{y_j \in Y} \sum_{x_i \in X} P(x_i, y_j) \log_2 \frac{P(x_i, y_j)}{P(x_i)P(y_j)} \tag{5.10}$$
$$= H(X) - H(X|Y)$$
$$= H(Y) - H(Y|X)$$
$$= H(X) + H(Y) - H(X,Y)$$
$$= H(X,Y) - H(X|Y) - H(Y|X)$$

The binary partitioning of X by a single value y_j into subsets $\{X|Y = y_j\}$ and $\{X|Y \neq y_j\}$ is particularly interesting. We will use $H(X| \vdash y_j)$ and $I(X; \vdash y_j)$ to refer to these cases.

Figure 5.1 visualizes the relationships between the entropies of each random variable, their conditional and joint entropies, as well as their mutual information. Note that each of the values is always positive. Furthermore, the mutual information $H(X, Y)$ is zero, if the variables X and Y are completely independent, and $H(X, Y) = H(X) = H(Y) = I(X; Y)$ if they are identical. Should the variable Y be completely dependent on X, then $I(X; Y) = H(Y)$.

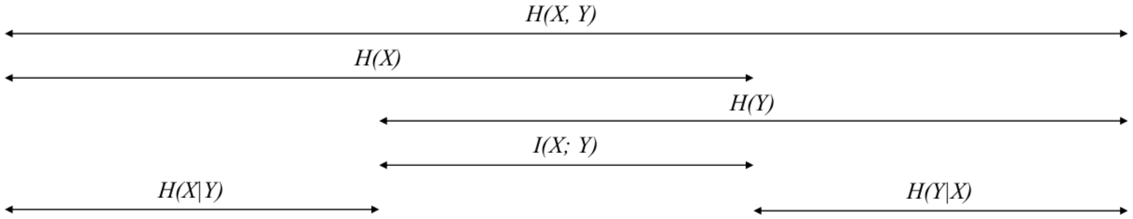


Figure 5.1: Relationships between the Entropies of Two Random Variables (reproduced from [Press et al. 2007, p. 760]).

One of the issues of using information gain as a measure of information gained through partitioning a random variable is its bias towards attributes with a larger number of possible values. To counteract this bias, the information gain value can be adjusted by the entropy of the partitioning random variable, yielding an adjusted *information gain ratio* [Harris 2001; Ibrahim et al. 2012; Mehdi et al. 2010; Qin et al. 2014].

Definition ***(Information Gain Ratio and Symmetric Uncertainty Coefficient)***
Let X be a discrete random variable with possible values $\{x_1, \ldots, x_n\}$ and
let Y be a discrete random variable with possible values $\{y_1, \ldots, y_m\}$
The **information gain ratio** $IGR(X|Y)$ is then given by:

$$IGR(X|Y) = \frac{I(X;Y)}{H(Y)} = \frac{H(X) - H(X|Y)}{H(Y)} = U(Y|X) \tag{5.11}$$

This ratio is also referred to as the **uncertainty coefficient** $U(Y|X)$ [Press et al. 2007]. Note that the information gain ratio has the opposite directionality of the uncertainty coefficient. The information gain ratio $IGR(X|Y)$ denotes the information we gained about X by knowing Y. Conversely, the uncertainty coefficient $U(Y|X)$ yields the reduction of the information (or entropy) of X from knowing Y.

Taking the weighted average of the two uncertainty coefficients $U(Y|X)$ and $U(X|Y)$ provides us with a measure for the redundancy (or correlation) of the two random variables [Witten et al. 2011]. This **symmetric uncertainty coefficient** $U(X,Y)$ is defined as:

$$U(X,Y) = 2\,\frac{I(X;Y)}{H(X)+H(Y)} \tag{5.12}$$

In summary, the above concepts used in information theory give us candidates for the quantification of *conceptual saturation*. Specifically, the change in *entropy* of a system based on adding new values — and thus changing the probability distribution — could potentially be used to gauge the value of collecting more data with a given data collection instrument. Similarly, the *redundancy* of information in a system could potentially be applied to a domain model to quantify the uniformity of the support of concepts by responses. The *information gain ratio* could provide a quantification of how much information is contributed to the domain model by categorization, as well as through the responses contributed by specific questions or participants. Finally, the *symmetric uncertainty coefficient* can provide us with the redundancy of information within the answers of two participants, or the answers of a group of participants with those of an additional participant.

However, in order to be able to apply the above concepts to our domain model, we first have to formally define how the definitions can be applied to the artifacts and transformations of the domain modeling process. To do so, we have to define one or more appropriate *discrete random variables* to serve as the basis of our notion of information. These require well defined *support sets* (i.e., the set of states a variable can take on) and *probability mass functions*.

5.2.2 Application of Entropy and Information Gain to Domain Models

It is not immediately apparent how to apply the information theory concepts to our domain modeling process (steps (3) and (4) in Figure 3.3). Particularly, the choices of random variables with well defined supports and probability mass functions is not obvious. It is, therefore, useful to recall the relevant processes and artifacts of the domain modeling phase.

There are two kinds of artifacts involved in this process. First, privacy-related information (PRI) in formats specific to the data collection instruments employed serves as the input of the process. Second, a domain model in the format specific to the encoding process used is the outcome of the process. In the remainder of this section we will develop the required definitions through a simple example. The example uses the approach outlined in Chapter 3.

> **Example** ***(Scenario)***
>
> Let us assume that we had an idea for an application, but are not entirely certain about the composition of our target population. More specifically, we were interested in the age and gender of our target population, and thus designed a **survey** with **two questions**. Because of limited time and resources, we decided to collect data through a telephone survey. Due to the sensitivity of the data and the limitations of our data collection instrument we had a very low response rate. In fact, we only managed to recruit **three participants**. To make matters worse, one of the participants was not comfortable to provide their age, yielding us a total of **five responses**. These comprise the **privacy-related information** of our example scenario.

In general, we can formally define privacy-related information as follows:

> **Definition** ***(Privacy-Related Information, Question, Participant, and Response)***
>
> We will define **privacy-related information** with the symbol I as the triple
>
> $$I = (Q, P, R) \tag{5.13}$$
>
> where
>
> $Q = \{q_1, \ldots, q_n\}$ is the set of **questions** asked in the study,
>
> $P = \{p_1, \ldots, p_n\}$ is the set of **participants** who contributed to the study, and
>
> $R = \{r_1, \ldots, r_n\}$ is the set of **responses** (or answers) elicited through the study.

Note that, depending on the chosen data collection method, a response might take the form of a description of behavior or even a transcript of a recording. Furthermore, data collection might not involve direct inquiry (i.e., not employ questions explicitly). However, even observational studies should be based on research questions to guide data collection [Heppner et al. 2008]). Thus, the definition of privacy-related information as a collection of questions, participants, and responses is fairly robust. Finally, should multiple data sources be used, we can see the information as the union of the produced questions, participants, and responses. For our example, this yields:

Example ***(Privacy-Related Information)***
$I = (Q, P, R)$ as our privacy-related information,
$Q = \{q_1, q_2\}$ as our questions (q_1: "How old are you?", q_2:"What is your gender?"),
$P = \{p_1, p_2, p_3\}$ as our participant pool, and
$R = \{r_1, r_2, r_3, r_4, r_5\}$ as the responses we received.

As we are interested in the contributions of individual questions and participants to our domain model, we need to formally establish their relationship to the responses. Furthermore, responses contain data in terms of statements. We can formally define these relationships as the follows:

Definition ***(Response Information)***
Let $r_i \in R$ be a response.
We define the **response-by function** $\mathrm{responseBy}$ that maps a response to its participant as:

$$\mathrm{responseBy}\colon r \mapsto p\colon R \to P \tag{5.14}$$

We define the **response-to function** $\mathrm{responseTo}$ that maps a response to its question as:

$$\mathrm{responseTo}\colon r \mapsto q\colon R \to Q \tag{5.15}$$

Finally, we define the **data function** data that maps a response to its data as:

$$\mathrm{data}\colon r \mapsto d\colon R \to \mathfrak{D} \tag{5.16}$$

Where $\mathfrak{D}$ is the set of all possible statements (e.g., all possible sentences in English).

These definitions allow us to better grasp the information collected and to form associations between the responses an their origins. Table 5.1 illustrates their utility by providing the response information of our example scenario.

Table 5.1: Example: Response Information

	$\boldsymbol{r_1}$	$\boldsymbol{r_2}$	$\boldsymbol{r_3}$	$\boldsymbol{r_4}$	$\boldsymbol{r_5}$
responseBy $(\boldsymbol{r_i})$	p_1	p_1	p_2	p_2	p_3
responseTo $(\boldsymbol{r_i})$	q_1	q_2	q_1	q_2	q_2
data $(\boldsymbol{r_i})$	“18”	“male”	“19”	“female”	“female”

Following the suggested approach in Chapter 3, the steps following data collection are the *open coding* and *axial coding* of the privacy-related information. During open coding, an analyst transforms the data contained in the responses into formal *assertions*. During axial coding, an analyst classifies the assertions by developing *terms*. Thus, the open coding of responses into assertions can be seen as function relating a response to a set of assertions. Similarly, the initial axial coding of assertions into terms can be seen as function relating a leaf term to a set of assertions (as detailed in Chapter 3, taxonomic terms are not directly linked to assertions). Furthermore, the analyst establishes the *temporal order* within the assertions. We can define these processes as follows:

Definition *(Response Encoding)*

Let $r_i =\in R$ be a response.

Let $d = \mathrm{data}(r_i)$ be the data of the response (i.e., the statements made in the response).

We define the **encoding function** $\mathrm{encoding}$ representing *open coding* as:

$$\mathrm{encoding}\colon d \mapsto \{a_1, \dots a_n\} : \mathfrak{D} \to \{A \subset \mathfrak{A}\} \tag{5.17}$$

where $\mathfrak{A}$ is the set of all possible assertions.

Furthermore, we define the **encoding** of r with symbol $E(r)$ as:

$$E(r) = \mathrm{encoding}(data(r_i)) \tag{5.18}$$

We will refer to the encoding of the set of responses R as $E(R)$:

$$E(R) = \bigcup_{r_i \in R} E(r_i) \tag{5.19}$$

Let $t_i \in T$ be a term.

We define the **instance function** $\mathrm{instance}$ representing *axial coding* as:

$$\mathrm{instance}\colon t_i \mapsto \{a_1, \ldots a_n\} : T \to \{A \subset \mathfrak{A}\} \tag{5.20}$$

Let $o_i \in O$ be a temporal order.

We define the **temporal ordering function** order as:

$$\mathrm{order}\colon o_i \mapsto \{a_j, a_k\} : O \to \left\{A \subset \mathfrak{A} \middle| |A| = 2\right\} \tag{5.21}$$

The encoding function establishes the *traceability* of the open coding step. The instance function does the same for the axial coding step, yet only for the terms representing the bottom-most layer of the taxonomy without sub-terms (i.e., leaf terms). As suggested in Section 3.3, taxonomic terms (terms with sub-terms) should not be directly linked to assertions. Moreover, it is important to avoid *ambiguity* of leaf terms as it would lead to overlap of the produced sets (i.e., no longer represent a partition of the set of assertions A). Before providing an example, we will therefore provide a definition for the PDML domain model (cf. Section 4.2):

Definition *(Knowledge Base, Term, Assertion, and Temporal Order)*

We will define a **knowledge base** (or domain model) with the symbol K as the triple

$$K = (T, A, O) \tag{5.22}$$

where

$T = \{t_1, \ldots, t_n\}$ is the set of **terms** in the knowledge base,

$A = \{a_1, \ldots, a_n\}$ is the set of **assertions** in the knowledge base, and

$O = \{o_1, \ldots, o_n\}$ is the set of **temporal orders** in the knowledge base.

Table 5.2 illustrates these definitions by applying them to our example. Our hypothetical analyst modeled the data as a simple triad of “participant”–“relationship”–“value”. The low number of assertions per response reflects the simplicity of both the questions and answers. More complex questions may yield to a larger amount of assertions. Note that only three assertions are reused (the assertions representing p_1 and p_2, and the assertion representing “female”).

Table 5.2: Example: Encoding Results

(a) Open Coding

	$\boldsymbol{r_1}$	$\boldsymbol{r_2}$	$\boldsymbol{r_3}$	$\boldsymbol{r_4}$	$\boldsymbol{r_5}$
$\boldsymbol{E(r_i)}$	$\{a_1, a_2, a_3\}$	$\{a_1, a_4, a_5\}$	$\{a_6, a_7, a_8\}$	$\{a_6, a_9, a_{10}\}$	$\{a_{11}, a_{12}, a_{10}\}$

(b) Axial Coding

	$\boldsymbol{t_1}$	$\boldsymbol{t_2}$	$\boldsymbol{t_3}$	$\boldsymbol{t_4}$	$\boldsymbol{t_5}$
Description	“Human”	“hasAge”	“Age”	“hasGender”	“Gender”
instance ($\boldsymbol{t_i}$)	$\{a_1, a_6, a_{11}\}$	$\{a_2, a_7\}$	$\{a_3, a_8\}$	$\{a_4, a_9, a_{12}\}$	$\{a_5, a_{10}\}$

We can safely assume that $E(R) \subseteq A$, since, ideally, all assertions are grounded in the responses of participants, in which case $E(R) = A$. However, in some cases, the analyst might add certain assertions representing her assumptions to the knowledge base to make those assumptions explicit (i.e., *bracketing*). In those cases, the equality is not guaranteed. This is not the case in our example, leading to the following domain model:

Example ***(Domain Model)***
$K = (T, A, O)$ representing the domain model,
$A = \{a_1, a_2, a_3\}$ representing the assertions generated through open coding, and
$T = \{t_1, t_2, t_3, t_4, t_5\}$ representing the terms resulting from the axial coding step.

These definitions present us with two potential candidates for the support of the discrete random variable that should serve as the basis of our notion of information. The assertions can be seen as the smallest building blocks of the knowledge base, as they give rise to both the terminology and the temporal orders. Similarly, establishing the temporal order of two assertions can be seen as a function relating a temporal order to a tuple of assertions. Thus, we could use the set of assertions for the states of our random variable. Just as assertions are the building blocks of the knowledge base, so are responses in respect to privacy-related information. In fact, we have defined three functions that yield the participants, questions, and data from the responses. Thus, we could also use the responses as the support of our random variable.

If, however, we use the set of assertions A for the support, the probability of picking a value a_j out of the set is exactly $1/n$, where n is the number of elements in A. The same is true for picking a value r_i out of the set of responses R. In other words, without any additional information, each of the values within the sets are equally likely to be chosen. The entropy of such uniformly distributed random variables, however, is simply the maximum entropy, as shown in Definition (5.3). Thus, we know that the entropy of a random variable X with support R is given as $H(X) = log_2|R|$, whereas support A leads to $H(X) = log_2|A|$. However, we are not simply interested in the *number* of assertions or responses, but rather the *support* of assertions within the responses of the participants. Thus, we need to reconsider the link between responses and assertions.

While providing a direct relationship between the study and the knowledge base, the encoding $E(R)$ still results in a uniformly distributed set of assertions, since any redundancy is discarded in the encoding process. In fact, we have explicitly stated above that our domain model does not contain bracketing assertions, and thus $E(R) = A$. Therefore, to establish the importance of the support of an assertion by a response, we have to provide a stronger definition of the *traceability* between the assertion and the response. We will do so by defining this *support statement*:

Definition ***(Support Statement)***
Let $r_i \in R$ be a response.
Let $a_j \in E(r_i)$ be an assertion contained in the encoding of r_i.
We define a **support statement** with symbol s_k as the tuple:

$$s_k = (r_i, a_j) \tag{5.23}$$

We will use the phrase "r_i supports a_j" and "a_j is supported by r_i to signify this relationship. We furthermore define the functions re and as to return the components of the statement:

$$\mathrm{re}\colon s_k \mapsto r_i\colon S \to R \tag{5.24}$$

$$\mathrm{as}\colon s_k \mapsto a_j\colon S \to R \tag{5.25}$$

A response can support multiple assertions and an assertion can be supported by multiple responses. However, a support statement is a unique combination of a response and an assertion. Thus, the support statements represent another candidate for our desired discrete random variable. We will therefore examine their probability mass function:

> **Definition** ***(Support Set and Probability Mass Function of Support Statements)***
>
> The **support set** $S = \{s_1, \ldots, s_l\}$ containing all support statements is defined as:
>
> $$S = \bigcup_{r_i \in R, a_j \in E(r_i)} (r_i, a_j) \tag{5.26}$$
>
> The **probability** $P(s_k)$ of selecting any contribution $s_k \in S$ is given as:
>
> $$P(s_k) = \frac{|\{s_k \in S| \, \mathrm{re}(s_k) = r_i, \mathrm{as}(s_k) = a_j\}|}{|S|} = P(R = r_i, A = a_j) = P(r_i, a_j) \tag{5.27}$$
>
> As we can see, the probability mass function $P(S)$ is the joint probability mass function $P(R, A)$ of R and A.

Taking into consideration that each combination of r_i and a_j can only appear once in the support set, it becomes apparent that $P(S)$ is a uniform distribution. We can illustrate this definition using the encodings in Table 5.2a:

> **Example** ***(Support Set, Support Entropy, Support Redundancy)***
>
> The support set is given as:
>
> $$\begin{aligned} S = \{&(r_1, a_1), (r_1, a_2), (r_1, a_3), (r_2, a_1), (r_2, a_4), (r_2, a_5), (r_3, a_6), (r_3, a_7), \\ &(r_3, a_8), (r_4, a_6), (r_4, a_9), (r_4, a_{10}), (r_5, a_{11}), (r_5, a_{12}), (r_5, a_{10})\} \end{aligned}$$
>
> As S is uniformly distributed, its entropy and redundancy are given as:
>
> $$\begin{aligned} H(S) &= H_0(S) = \log_2 |S| = 3.9069 \\ D(S) &= 1 - \frac{H(S)}{H_0(S)} = 0 \end{aligned}$$

The centrality of the support statements lies in the fact that each s_k represents a value of the *joint probability distribution* of the assertions and responses. Furthermore, we can use S as the support of probability mass functions for both R and A. In other words, instead of looking at the probability of a single support statement, we can determine the probability of encountering a support statement of a particular assertion or response. These probabilities depend on the size of the contribution of a response to the assertions and the size of the support of an assertion within the responses respectively.

Definition ***(Contribution and Probability of a Response)***

Let $r_i \in R$ be a response.

We define the **contribution** of r_i with symbol $C(r_i)$ as the set of its support statements:

$$C(r_i) = \bigcup_{a_j \in E(r_i)} (r_i, a_j) = \bigcup_{s_k \in S | \operatorname{re}(s_k) = r_i} s_k \tag{5.28}$$

The contribution $C(R)$ of the set of responses R is given as:

$$C(R) = \bigcup_{r_i \in R} C(r_i) = \bigcup_{r_i \in R, a_j \in E(R)} (r_i, a_j) = S \tag{5.29}$$

The **probability** $P(r_i)$ of selecting a contribution $s_k \in C(r_i)$ of r_i from S is given as:

$$P(r_i) = \frac{|\{s_k \in S | \operatorname{re}(s_k) = r_i\}|}{|S|} = \frac{|C(r_i)|}{|S|} \tag{5.30}$$

We will write $P(R)$ to denote the probability mass function of R given the support S.

The definition of the support of an assertion as the mirror image of the contribution of a response. It is worth mentioning that, if the knowledge base contains bracketing assertions of the analyst, these assertions are only considered if they find support in the responses of the participants. Otherwise, they do not contribute to the information within the knowledge base. Should this be the case after data collection has been completed, they should be closely examined and potentially removed.

Definition ***(Support and Probability of an Assertion)***

Let $a_j \in A$ be an assertion.

We define the **support** of a_j with symbol $S(a_j)$ as the set of its support statements:

$$S(a_j) = \bigcup_{r_i | a_j \in E(r_i)} (r_i, a_j) = \bigcup_{s_k \in S | \operatorname{as}(s_k) = a_j} s_k \tag{5.31}$$

Analogously, we define the support $S(A)$ of the set of assertions A as:

$$S(A) = \bigcup_{a_j \in A} S(a_j) = \bigcup_{r_i \in R, a_j \in E(R)} (r_i, a_j) = S \tag{5.32}$$

The **probability** $P(a_j)$ of selecting any support $s_k \in S(a_j)$ of a_j from S is given as:

$$P(a_j) = \frac{|\{s_k \in S | \operatorname{as}(s_k) = a_j\}|}{|S|} = \frac{|S(a_j)|}{|S|} \tag{5.33}$$

We will write $P(A)$ to denote the probability mass function of A given the support S.

Note that $C(R) = S(A) = S$ since $E(R) \subseteq A$. Thus, only supported assertions contribute to the probability. Given these probabilities and definitions (5.1), (5.2), and (5.5), the definitions of the self information, entropy, and redundancy of responses and assertions are straight-forward:

Definition ***(Self Information, Entropy, and Redundancy of Responses and Assertions)***

Let $r_i \in R$ be a response and

let $a_j \in A$ be an assertion.

The **self information** $I(r_i)$ and $I(a_i)$ of r_i and a_i are defined as:

$$I(r_i) = \log_2 \frac{1}{P(r_i)} = -\log_2 P(r_i) \tag{5.34}$$

$$I(a_j) = \log_2 \frac{1}{P(a_j)} = -\log_2 P(a_j) \tag{5.35}$$

The **entropies** $H(R)$ of R and $H(A)$ of A are given as:

$$H(R) = \sum_{r_i \in R} P(r_i) I(r_i) = \sum_{r_i \in R} P(r_i) \log_2 P(r_i) \tag{5.36}$$

$$H(A) = \sum_{r_j \in A} P(a_j) I(a_j) = \sum_{a_j \in A} P(a_j) \log_2 P(a_j) \tag{5.37}$$

The **redundancies** $D(R)$ of R and $D(A)$ of A are given as:

$$D(R) = 1 - H_r(R) = 1 - \frac{H(R)}{H_0(R)} = 1 - \frac{H(R)}{\log_2 |R|} \tag{5.38}$$

$$D(A) = 1 - H_r(A) = 1 - \frac{H(A)}{H_0(A)} = 1 - \frac{H(A)}{\log_2 |A|} \tag{5.39}$$

These definitions allow us to calculate the values for our example:

Example ***(Response Entropy and Redundancy, Assertion Entropy and Redundancy)***

The entropies and redundancies of responses and assertions are given as:

$$\begin{aligned}
H(R) &= 2.3219 \\
D(R) &= 1 - \frac{H(R)}{H_0(R)} = 1 - \frac{2.3219}{\log_2 |R|} = 1 - \frac{2.3219}{2.3219} = 0 \\
H(A) &= 3.5069 \\
D(A) &= 1 - \frac{H(A)}{H_0(A)} = 1 - \frac{3.5069}{\log_2 |A|} == 1 - \frac{3.5069}{3.5850} = 0.022
\end{aligned}$$

These values are not very surprising, given the small size of our example. The entropy of the responses achieving its maximum reflects that each response contributed the same amount of information in terms of assertions to the support set. For real data, this is relatively unlikely, since the equal number of assertions stems simply from the fact that both questions were multiple-choice questions. The relatively small redundancy value within the set of assertions reflects the fact that three assertions were mentioned more than once. Given these values and the nature of the open coding process — namely, that each response is treated as a separate entity, resulting in almost exclusively unique assertions — we can already anticipate that examining only the entropy and redundancy of responses and assertions will not yield our measure of conceptual saturation. Thus, we need to examine the remaining measures from section 5.2.1. We also need to consider whether examining terms, participants, or questions provide a better match to our needs.

In order to examine the remaining measures from section 5.2.1, we need to define the conditional probability distribution of assertions given responses and vice versa. Given the joint probability

$P(r_i, a_j)$ in definition (5.27) and the probabilities $P(r_i)$ and $P(a_j)$ in definitions (5.30) and (5.33), respectively, the conditional probabilities are given as:

Definition ***(Conditional Probabilities of Responses and Assertions)***

Let $r_i \in R$ be a response and

let $a_j \in A$ be an assertion.

The **conditional probabilities** $P(a_j|r_i)$ and $P(r_i|a_j)$ are defined as:

$$P(a_j|r_i) = \frac{P(r_i, a_j)}{P(r_i)} = \frac{|\{s_k \in C(r_i)|\,\mathrm{as}(s_k) = a_j\}|}{|C(r_i)|} \tag{5.40}$$

$$P(r_i|a_j) = \frac{P(r_i, a_j)}{P(a_j)} = \frac{|\{s_k \in S(a_j)|\,\mathrm{re}(s_k) = r_i\}|}{|S(a_j)|} \tag{5.41}$$

Given these conditional probabilities, we can use definition (5.9) to define the conditional entropies of the responses[2].

Definition ***(Conditional Entropy of Responses)***

Let $r_i \in R$ be a response and

let $a_j \in A$ be an assertion.

The **conditional self-information** of $I(a_j|r_i)$ and $I(r_i|a_j)$ are defined as:

$$I(a_j|r_i) = -\log_2 P(a_i|r_i) \tag{5.42}$$

$$I(r_i|a_j) = -\log_2 P(r_i|a_j) \tag{5.43}$$

The **conditional entropies** $H(A|r_i)$ and $H(R|a_j)$ are defined as:

$$H(A|r_i) = \sum_{a_j \in A} P(a_i|r_i) I(a_i|r_i) = -\sum_{a_j \in A} P(a_i|r_i) \log_2 P(a_i|r_i) \tag{5.44}$$

$$H(R|a_j) = \sum_{r_i \in R} P(r_i|a_j) I(r_i|a_j) = \tag{5.45}$$

The **conditional entropies** $H(A|R)$ and $H(R|A)$ are given as:

$$H(A|R) = \sum_{r_i \in R} P(r_i) H(A|r_i) = H(R, A) - H(R) = H(S) - H(R) \tag{5.46}$$

[2] In the following definitions, we will write $P(X|y)$ to denote $P(X|Y = y)$.

$$H(R|A) = \sum_{a_j \in A} P(a_j)H(R|a_j) = H(R,A) - H(A) = H(S) - H(A) \tag{5.47}$$

As we can see, the above definitions resulted from simply plugging the appropriate probabilities into the definitions given in section 5.2.1. The definitions, furthermore, allow us to calculate the values for the individual responses and assertions of our example, given in Table 5.3.

Table 5.3: Example: Support, Probability, and Entropy of Responses and Assertions

(a) Responses

	$\boldsymbol{C(r_i)}$	$\boldsymbol{P(r_i)}$	$\boldsymbol{I(r_i)}$	$\boldsymbol{H(A\|r_i)}$
$\boldsymbol{r_1}$	$\{(r_1, a_1), (r_1, a_2), (r_1, a_3)\}$	$3/15$	2.3219	1.5849
$\boldsymbol{r_2}$	$\{(r_2, a_1), (r_2, a_4), (r_2, a_5)\}$	$3/15$	2.3219	1.5849
$\boldsymbol{r_3}$	$\{(r_3, a_6), (r_3, a_7), (r_3, a_8)\}$	$3/15$	2.3219	1.5849
$\boldsymbol{r_4}$	$\{(r_4, a_6), (r_4, a_9), (r_4, a_{10})\}$	$3/15$	2.3219	1.5849
$\boldsymbol{r_5}$	$\{(r_5, a_{11}), (r_5, a_{12}), (r_5, a_{10})\}$	$3/15$	2.3219	1.5849

(b) Assertions

	$\boldsymbol{S(a_i)}$	$\boldsymbol{P(a_i)}$	$\boldsymbol{I(a_i)}$	$\boldsymbol{H(R\|a_i)}$
$\boldsymbol{a_1}$	$\{(r_1, a_1), (r_2, a_1)\}$	$2/15$	2.9069	1
$\boldsymbol{a_2}$	$\{(r_1, a_2)\}$	$1/15$	3.9069	0
$\boldsymbol{a_3}$	$\{(r_1, a_3)\}$	$1/15$	3.9069	0
$\boldsymbol{a_4}$	$\{(r_2, a_4)\}$	$1/15$	3.9069	0
$\boldsymbol{a_5}$	$\{(r_2, a_5)\}$	$1/15$	3.9069	0
$\boldsymbol{a_6}$	$\{(r_3, a_6), (r_4, a_6)\}$	$2/15$	2.9069	1
$\boldsymbol{a_7}$	$\{(r_3, a_7)\}$	$1/15$	3.9069	0
$\boldsymbol{a_8}$	$\{(r_3, a_8)\}$	$1/15$	3.9069	0
$\boldsymbol{a_9}$	$\{(r_4, a_9)\}$	$1/15$	3.9069	0
$\boldsymbol{a_{10}}$	$\{(r_4, a_{10}), (r_5, a_{10})\}$	$2/15$	2.9069	1
$\boldsymbol{a_{11}}$	$\{(r_5, a_{11}))\}$	$1/15$	3.9069	0
$\boldsymbol{a_{12}}$	$\{(r_5, a_{12})\}$	$1/15$	3.9069	0

Doing the same for the definitions of mutual information, information gain ratio, and the symmetric uncertainty coefficient (definitions (5.10), (5.11), and (5.12), respectively), we get the values shown in Table 5.4 for our example.

Table 5.4: Example: Shared Information Measures of Responses and Assertions

$\boldsymbol{H(R\|A)}$	$\boldsymbol{H(A\|R)}$	$\boldsymbol{I(R;A)}$	$\boldsymbol{U(R\|A)}$	$\boldsymbol{U(A\|R)}$	$\boldsymbol{U(A,R)}$
0.4000	1.5850	1.9219	0.8277	0.5480	0.6594

These values highlight the strong predictive relationship between the responses and assertions. Given information about the assertions, one requires very little information to encode a response. In fact, obtaining information about the assertions allows us to predict almost 83% of the responses. While not quite as strong, the reverse direction gives us 55% chance of predicting the values of assertions given information on the responses. Both the high amount of mutual information and high redundancy expressed through the symmetric uncertainty coefficient reinforce this interpretation.

Furthermore, the values indirectly provide information about our data collection instrument (in this case, predominantly the questions asked) and encoding process. Once again, we could have predicted the high correlation between the responses and assertions from the fact that the questions allowed only very limited choices. They did not provide participants with the opportunity to provide responses of varying length, thus increasing the entropy of the responses. As mentioned before, the open coding process yields predominantly unique assertions, leading to their high entropy. However, given larger response sets, we would expect multiple choice questions to achieve higher levels of redundancy (i.e., more re-use of assertions between responses). In fact, when using triads of “participant”–“relationship”–“value” for the open coding of multiple-choice questions, we would expect about 33% redundancy for a question about gender (given a heterogeneous participant pool and binary interpretation of gender).

What these values do not provide is a clear candidate for our measure of conceptual saturation. While we can assume that both the mutual information and symmetric uncertainty coefficient will decrease due to expected lower entropy of the responses and assertions themselves, it is not clear whether the values will converge and, if they do, what value they will approach. Barring the existence of such a value (which can be determined empirically), we have two remaining options. First, we can examine the individual contribution of the responses to the assertions (the reverse not being very interesting for our purposes). Second, we can determine whether the contributions of questions, participants, and terms provide more insight.

To determine the contribution of a single response, we have to separate its contributed support statements from the support statements of the other responses. In other words, we have to *partition* the support set S into the contribution $C(r_i)$ of a single r_i and the contribution $S \setminus C(r_i)$ of all the remaining responses. This is the "interesting case" we mentioned in definition (5.10). Thus, we need to determine the definitions of the conditional entropy, mutual information, information gain ratio, and symmetric uncertainty coefficient for A given the partitioning of $R \vdash r_i$.

Definition *(Response Partitions)*

Let $r_i \in R$ be a response,
let $\neg r_i = \{r_k \in R | r_k \neq r_i\}$ be the remainder of R without r_i,
let $\vdash r_i = \{r_i, \neg r_i\}$ be the partition of R by r_i, and
let $a_j \in A$ be an assertion.

The **probability** $P(r_i)$ is given in Definition (5.30). The probability $P(\neg r_i)$ is defined as:

$$P(\neg r_i) = \frac{|\{s_k \in S | \operatorname{re}(s_k) \neq r_i\}|}{|S|} = \frac{|C(\neg r_i)|}{|S|} = \frac{|S \setminus C(r_i)|}{|S|} = 1 - P(r_i) \tag{5.48}$$

The **entropy** $H(\vdash r_i)$ of the partition is then:

$$H(\vdash r_i) = -P(r_i)\log_2 P(r_i) - P(\neg r_i)\log_2 P(\neg r_i) \tag{5.49}$$

The **conditional probability** $P(a_j|r_i)$ is given in Definition (5.40). The conditional probability $P(a_j|\neg r_i)$ of the remainder is given as:

$$P(a_j|\neg r_i) = \frac{|\{s_k \in C(\neg r_i) | \operatorname{as}(s_k) = a_j\}|}{|C(\neg r_i)|} \tag{5.50}$$

The **conditional entropy** $H(A|r_i)$ is provided in Definition (5.44). $H(A|\neg r_i)$ is defined as:

$$H(A|\neg r_i) - \sum_{a_j \in A} P(a_i|\neg r_i)\log_2 P(a_i|\neg r_i) \tag{5.51}$$

The **conditional entropy** of the partition $H(A| \vdash r_i)$ is then:

$$H(A| \vdash r_i) = P(r_i)H(A|r_i) + P(\neg r_i)H(A|\neg r_i) \tag{5.52}$$

The **mutual information** $I(A; \vdash r_i)$ is then:

$$I(A; \vdash r_i) = H(A) - H(A| \vdash r_i) \tag{5.53}$$

The **information gain ratio** $IGR(A|\vdash r_i)$ is then given by:

$$IGR(A|\vdash r_i) = \frac{I(A;\vdash r_i)}{H(\vdash r_i)} = U(\vdash r_i|A) \tag{5.54}$$

Finally, the **symmetric uncertainty coefficient** $U(A,\vdash r_i)$ is defined as:

$$U(A,\vdash r_i) = 2\,\frac{I(A;\vdash r_i)}{H(A) + H(\vdash r_i)} \tag{5.55}$$

Given these definitions, we can calculate the values of the individual contributions of the responses of our example, given in Table 5.5.

Table 5.5: Example: Contributions of Individual Responses

	$\boldsymbol{H(\vdash r_i)}$	$\boldsymbol{H(A|\vdash r_i)}$	$\boldsymbol{I(A;\vdash r_i)}$	$\boldsymbol{U(\vdash r_i|A)}$	$\boldsymbol{U(A|\vdash r_i)}$	$\boldsymbol{U(A,\vdash r_i)}$
$\boldsymbol{r_1}$	0.7219	2.9183	0.5886	0.8153	0.1678	0.2784
$\boldsymbol{r_2}$	0.7219	2.9183	0.5886	0.8153	0.1678	0.2784
$\boldsymbol{r_3}$	0.7219	2.9183	0.5886	0.8153	0.1678	0.2784
$\boldsymbol{r_4}$	0.7219	2.8126	0.6943	0.9618	0.1980	0.3284
$\boldsymbol{r_5}$	0.7219	2.9183	0.5886	0.8153	0.1678	0.2784

Examining the values in Table 5.5, we are once again shown the homogeneity of our example. Since every response contributed the same amount of assertions to the support set, the information $H(\vdash r_i)$ of partitioning R by an individual response r_i is identical for every response. Similarly, the values for every response save r_4 produced the same values in terms of conditional entropy, mutual information, information gain ratio, and symmetric uncertainty coefficient. This shows that those questions all contributed two unique and a single shared assertions. Response r_4, on the other hand, contributed only one unique assertion, which results in the lower conditional entropy as well as higher values for the shared information and information gain ratio. Thus, these values may allow us to distinguish between responses with high amount of unique assertions, giving rise to lower mutual information and symmetric uncertainty coefficients, as compared to responses with larger amounts of shared responses. In other words, these values could potentially be used for outlier detection.

Given larger amounts of data, we can expect that the entropy of partitioning by individual responses will decrease, as the remainder $\neg r_i$ will have a much higher probability than the individual response. We can expect the conditional entropy of A given $\vdash r_i$ to grow, as the amount of information in the knowledge base grows with the number of assertions. With the growth of total information in the knowledge base, we can expect the mutual information of the partition with the assertions to decrease, reflecting the comparatively lesser contribution of each response. It is hard to predict whether the information gain ratio will grow or decrease since it depends both on the entropy of the partition as well as the mutual information of the partition with the set of assertions, both of which we expect to decrease. Thus, it is likely that the information gain ratio will retain its utility to detect outliers. Finally, the value of the symmetric uncertainty coefficient can be expected to decrease due to the decrease in mutual information and increase in the entropy of the assertions.

However, none of the measures yields a good measure for conceptual saturation. Thus, we will examine whether the contributions of participants, questions, and terms can provide such a measure. To that end, we simply need to define their probability mass functions and conditional probability mass functions with respect to the set of assertions.

Definition ***(Contribution and Probability of a Participant or Question)***
Let $p_i \in P$ be a participant.
Let $q_i \in Q$ be a question.
We define the **contribution** of p_i and q_i with symbols $C(p_i)$ and $C(q_i)$, respectively, as the union of the contributions of their responses:

$$C(p_i) = \bigcup C(r_j) \Big| \text{responseBy}(r_j) = p_i \tag{5.56}$$

$$C(q_i) = \bigcup C(r_j) \Big| \text{responseTo}(r_j) = q_i \tag{5.57}$$

The **probability** $P(p_i)$ and $P(q_i)$ of selecting a contribution s_k of p_i or q_i from S is given as:

$$P(p_i) = \frac{|C(p_i)|}{|C(R)|} \tag{5.58}$$

$$P(q_i) = \frac{|C(q_i)|}{|C(R)|} \tag{5.59}$$

We will write $P(P)$ and $P(Q)$ to denote the probability mass functions of P and Q.

The **conditional probabilities** $P(a_j|p_i)$ and $P(a_j|q_i)$ are defined as:

$$P(a_j|p_i) = \frac{P(p_i, a_j)}{P(p_i)} = \frac{|\{s_k \in C(p_i)|\,\mathrm{as}(s_k) = a_j\}|}{|C(p_i)|} \tag{5.60}$$

$$P(a_j|q_i) = \frac{P(q_i, a_j)}{P(p_i)} = \frac{|\{s_k \in C(q_i)|\,\mathrm{as}(s_k) = a_j\}|}{|C(q_i)|} \tag{5.61}$$

The values for the individual participants and questions of our example are given in Table 5.6.

Table 5.6: Example: Information Measures of Individual Participants and Questions

(a) Participants

	$C(p_i)$	$P(p_i)$	$I(p_i)$	$H(A\|p_i)$
p_1	$\{(r_1,a_1),(r_1,a_2),(r_1,a_3),(r_2,a_1),(r_2,a_4),(r_2,a_5)\}$	6/15	1.3219	2.2516
p_2	$\{(r_3,a_6),(r_2,a_7),(r_2,a_8),(r_4,a_6),(r_4,a_9),(r_2,a_{10})\}$	6/15	1.3219	2.2516
p_3	$\{(r_5,a_{11}),(r_5,a_{12}),(r_5,a_{10})\}$	3/15	2.3219	1.5850

(b) Questions

	$C(q_i)$	$P(q_i)$	$I(q_i)$	$H(A\|q_i)$
q_1	$\{(r_1,a_1),(r_1,a_2),(r_1,a_3),(r_3,a_6),(r_3,a_7),(r_3,a_8)\}$	6/15	1.3219	2.5850
q_2	$\{(r_2,a_1),(r_2,a_4),(r_2,a_5),(r_4,a_6),(r_4,a_9),$ $(r_4,a_{10}),(r_5,a_{11}),(r_5,a_{12}),(r_5,a_{10})\}$	9/15	0.7370	2.9477

Provided these contributions and probabilities, this leads to the values for the participants and questions in our example given in Table 5.7.

Table 5.7: Example: Information Measures of Participant and Question Sets

X	$H(X)$	$D(X)$	$H(A\|X)$	$H(X\|A)$	$I(A;X)$	$U(X\|A)$	$U(A\|X)$	$U(A,X)$
P	1.5219	0.0398	2.1183	0.1333	1.3886	0.9124	0.3960	0.5523
Q	0.9710	0.0290	2.8026	0.2667	0.7043	0.7253	0.2008	0.3146

As we can see, compared to the entropy of the responses with value $H(R) = 2.3219$, the partitioning of the responses by participants and questions leads to a reduction in entropy. Given that the partitioning of the responses represents a reduction of the number of possible symbols within the support of the distribution, this is not surprising. Furthermore, we can see that, given an assertion, we can predict which participant has provided the response that supports that assertion with about 91.24% probability. This relationship between assertions and participants is not further surprising, since assertions are highly likely to refer to specific entities and relationships of the participants. Only shared assertions would reduce this relationship, which are not prevalent in this example data set. While not quite as strong, a similar predictive relationship also exists between assertions and questions. We can attribute this relationship to the lack of thematic overlap between our example questions. Should we inquire about the same entities or relationships in multiple questions, we can expect this relationship to get weaker.

Examining the values in Table 5.6b, it is obvious that the second question yielded more information than the first. This is compensated by the fact that the first question did not yield any shared assertions, whereas the second question did. It is also worthwhile to note that the values of the information measures in Table 5.7 reflect the partitioning of the questions by the individual values.

Similarly, values in Table 5.6a, suggest that participants 1 and 2 contributed equal amounts of information to the assertions, whereas participant 3 contributed much less in comparison. However, it is worthwhile to examine the partitioning of the participants by individual participants to investigate whether that observation holds true. The values for our example are given in Table 5.8.

Table 5.8: Example: Contributions of Individual Participants

	$\boldsymbol{H(\vdash p_i)}$	$\boldsymbol{H(A\vert \vdash p_i)}$	$\boldsymbol{I(A; \vdash p_i)}$	$\boldsymbol{U(\vdash p_i\vert A)}$	$\boldsymbol{U(A\vert \vdash p_i)}$	$\boldsymbol{U(A, \vdash p_i)}$
$\boldsymbol{p_1}$	0.9710	2.5359	0.9710	1	0.2769	0.4337
$\boldsymbol{p_2}$	0.9710	2.6693	0.8376	0.8626	0.2388	0.3741
$\boldsymbol{p_3}$	0.7219	2.9183	0.5886	0.8153	0.1678	0.2784

As we can see, the assumption that the first two participants contribute the same amount of information to the knowledge base does not hold up. Rather, we can see that the first participant contributed the largest amount of unique assertions, allowing to perfectly predict that participant's contribution when picking one of the unique assertions. Since participants 2 and 3 both contributed a shared assertion, predicting their contributions is more difficult and thus less likely. The values further reinforce that the last participant contributed the least to the information, yet show that the difference in terms of the prediction in either direction is not significantly less.

As it was the case with the responses, the information theoretical measures provided us with feedback on the individual contributions of the questions and participants and their relationships among themselves. Once again, however, no clear candidate for the measure of conceptual saturation emerges. Therefore, we will investigate whether the terms of our knowledge base provide a match.

Definition ***(Support and Probability of a Term)***

Let $t_i \in T$ be a term.

We define the **support** of t_i with symbol $S(t_i)$ as the union of the support of its assertions:

$$S(t_i) = \bigcup_{a_j \in \text{instance}(t_i)} S(a_j) \tag{5.62}$$

The **probability** $P(t_i)$ of selecting any support of t_i from $S(A)$ is given as:

$$P(t_i) = \frac{|S(t_i)|}{|S(A)|} \tag{5.63}$$

We will write $P(T)$ to denote the probability mass function of the set of terms T.

The **conditional probability** $P(a_j|t_i)$ is defined as:

$$P(a_j|t_i) = \frac{P(t_i, a_j)}{P(t_i)} = \frac{|\{s_k \in S(t_i)|\,\text{as}(s_k) = a_j\}|}{|S(t_i)|} \tag{5.64}$$

This results in the values for the measures of the individual terms of our example in Table 5.9.

Table 5.9: Example: Support, Probability, and Entropy of Terms

	$\boldsymbol{S(t_j)}$	$\boldsymbol{P(t_j)}$	$\boldsymbol{I(t_j)}$	$\boldsymbol{H(A\|t_j)}$
$\boldsymbol{t_1}$	$\{(r_1, a_1), (r_2, a_1), (r_3, a_6), (r_4, a_6), (r_5, a_{11})\}$	5/15	1.5850	1.5219
$\boldsymbol{t_2}$	$\{(r_1, a_2), (r_3, a_7)\}$	2/15	2.9069	1
$\boldsymbol{t_3}$	$\{(r_1, a_3), (r_3, a_8)\}$	2/15	2.9069	1
$\boldsymbol{t_4}$	$\{(r_2, a_4), (r_4, a_9), (r_5, a_{12})\}$	3/15	2.3219	1.5850
$\boldsymbol{t_5}$	$\{(r_2, a_5), (r_4, a_{10}), (r_5, a_{10})\}$	3/15	2.3219	0.9183

The resulting measures for all terms in the example are given in Table 5.10.

As we can see, the terms in our example contain a similar amount of information to the responses, since the partitioning of the assertions by the terms is relatively uniform. This is reflected by the

Table 5.10: Example: Information Measures of the Term Set

X	$H(T)$	$D(T)$	$H(X\|T)$	$H(T\|X)$	$I(X;T)$	$U(T\|X)$	$U(X\|T)$	$U(X,T)$
A	2.2323	0.0386	1.2746	0	2.2323	1	0.6365	0.7779

low redundancy value. However, given a more realistic data set, it can be expected that the support of the term representing "Human" (see Table 5.2b) will eventually dominate the remaining terms. Furthermore, the values show us the existential dependency between terms and their assertions in the uncertainty coefficient $U(T|A)$. This is by design, as the leaf terms are supposed to represent a partitioning of the assertions. Thus, the terms are also good predictors of the assertions, although this relationship can be expected to decrease given more data (and more terms). Due to the existential dependency of terms on their assertions, we cannot expect the contributions of individual terms to be of much value. The values for our example are given in Table 5.11.

Table 5.11: Example: Contributions of Individual Terms

	$H(\vdash t_i)$	$H(A\|\vdash t_i)$	$I(A;\vdash t_i)$	$U(\vdash t_i\|A)$	$U(A\|\vdash t_i)$	$U(A;\vdash t_i)$
t_1	0.9183	2.5886	0.9183	1	0.2619	0.4150
t_2	0.5665	2.9404	0.5886	1	0.1678	0.2781
t_3	0.5665	2.9404	0.5886	1	0.1678	0.2781
t_4	0.7219	2.7850	0.7219	1	0.2059	0.3414
t_5	0.7219	2.7850	0.7219	1	0.2059	0.3414

In fact, we can see that the assertions remain a certain predictor for each individual terms. Furthermore, the uncertainty coefficients $U(A|\vdash t_i)$ along with the symmetric coefficients $U(A, \vdash t_i)$ reveal that the contributions of a term depends solely on the number of assertions in its support.

Neither the measures of individual terms, nor the shared measures of terms with assertions provide a clear measure for conceptual saturation. However, we have only examined these values at a fixed point of the domain modeling process: after its completion. Thus, looking at different measures over time should yield a better view of how each of them develops. Moreover, our analysis up to this point suggests that, while the shared measures like conditional entropy or mutual information provide valuable insight, they highlight the relationships between the different sets and not the total information in either of the sets. Therefore, we will focus on examining the development of the entropies of the various sets over time. Table 5.12 shows how the change of the entropies of our example, ordered both by response/participant (5.12a) and by question (5.12b).

Table 5.12: Example: Entropies over Time (Support Set S is the union of each row)

(a) Ordered by Participant

$\boldsymbol{r_i}$	$\boldsymbol{p_i}$	$\boldsymbol{q_i}$	$\boldsymbol{S}$	$\boldsymbol{H(R)}$	$\boldsymbol{H(A)}$	$\boldsymbol{H(P)}$	$\boldsymbol{H(Q)}$	$\boldsymbol{H(T)}$
$\boldsymbol{r_1}$	p_1	q_1	$\{(r_1, a_1), (r_1, a_2), (r_1, a_3)\}$	0	1.5850	0	0	1.5850
$\boldsymbol{r_2}$	p_1	q_2	$\{(r_2, a_1), (r_2, a_4), (r_2, a_5)\}$	1	2.2516	0	1	2.2516
$\boldsymbol{r_3}$	p_2	q_1	$\{(r_3, a_6), (r_3, a_7), (r_3, a_8)\}$	1.5850	2.9477	0.9183	0.9183	2.1972
$\boldsymbol{r_4}$	p_2	q_2	$\{(r_4, a_6), (r_4, a_9), (r_4, a_{10})\}$	2	3.4183	1	1	2.2516
$\boldsymbol{r_5}$	p_3	q_2	$\{(r_5, a_{11}), (r_5, a_{12}), (r_5, a_{10})\}$	2.3219	3.5069	1.5219	0.9710	2.2323

(b) Ordered by Question

$\boldsymbol{r_i}$	$\boldsymbol{p_i}$	$\boldsymbol{q_i}$	$\boldsymbol{S}$	$\boldsymbol{H(R)}$	$\boldsymbol{H(A)}$	$\boldsymbol{H(P)}$	$\boldsymbol{H(Q)}$	$\boldsymbol{H(T)}$
$\boldsymbol{r_1}$	p_1	q_1	$\{(r_1, a_1), (r_1, a_2), (r_1, a_3)\}$	0	1.5850	0	0	1.5850
$\boldsymbol{r_3}$	p_2	q_1	$\{(r_3, a_6), (r_3, a_7), (r_3, a_8)\}$	1	2.2516	0	0	1.5850
$\boldsymbol{r_2}$	p_1	q_2	$\{(r_2, a_1), (r_2, a_4), (r_2, a_5)\}$	1.5850	2.9477	0.9183	0.9183	2.1972
$\boldsymbol{r_4}$	p_2	q_2	$\{(r_4, a_6), (r_4, a_9), (r_4, a_{10})\}$	2	3.4183	1	1	2.2516
$\boldsymbol{r_5}$	p_3	q_2	$\{(r_5, a_{11}), (r_5, a_{12}), (r_5, a_{10})\}$	2.3219	3.5069	1.5219	0.9710	2.2323

As we can see, the entropy of responses grows in every step, regardless of whether we encode by participant or by question. The fact that it always takes on its maximum entropy stems from the fact that each response contributes the same amount of assertions. Similarly, the entropy of the assertions also grows each step. As mentioned before, this is to be expected from treating each participants' experiences as separate instances, and only sharing generalizable assertions like gender or age between participants.

Grouping the responses of each participant, we can see that their entropy also grows each step. This can be attributed to the existential dependency of responses on participants, meaning that each participant will grow the total number of responses and result in more information. Analogously, grouping responses by question shows that each additional question adds to the total entropy of all questions. Hence we can expect the entropy of the question set to grow, should questions be added.

The only entropy that does not strictly grow each step is the entropy of the set of terms. Moreover, we can detect a relationship between the growth of the entropy of the questions and the entropy of the terms. This reflects that participants are more likely to volunteer new concepts if provided with another question. However, as we suggested in Section 5.2 of this chapter, we can expect additional questions to be asked only for the purpose of validation. In other words, we can assume the set of questions to be fixed until validation of the domain model is attempted. Furthermore, we can assume that validation will not start until conceptual saturation given the existing, fixed question set is reached.

Thus, we can use the entropy of terms to gauge whether or not that state is achieved. Note that this coincides with the naive approach of terminating the study once no more concepts (in this case, terms) are added. However, using the entropy can provide additional insight beyond that of a simple count of terms. As mentioned before, the entropy of a random variable (and its redundancy) reflects the uniformity of its probability distribution. Therefore, given additional participants, we can expect that the support of each term through assertions will eventually reflect its support within the target population. This would mean that the entropy will converge onto a particular value. As we can see in Table 5.12, it is quite likely that the value will oscillate around that value. In other words, the entropy achieves *stability*.

However, through encoding responses as experiences of participants, we can also expect the term representing "Human" to gain support through virtually every response. Thus, the probability of this term will strictly increase with each participant. Therefore, we can expect that the support of this term will start to dominate the distribution as the support of other terms stabilizes. In other words, we can expect the value of the entropy of all terms to approach a certain value, stabilize around that value, then continuously decline as more participants are added. This could serve as an additional indicator for contextual saturation.

In summary, we can use the entropy of the terms $H(T)$ to monitor the overall development of the amount of information in the domain model. We can gauge how evenly terms are supported by calculating the redundancy within the set. Finally, we can use the uncertainty coefficient to monitor the contribution of information of particular responses, participants, and questions.

5.3 Summary

At the beginning of this chapter, we set out to determine the means for evaluating whether the Privacy Requirements Engineering process (PREprocess) in combination with the Privacy Domain Modeling Language (PDML) provide sufficient support for Hypothesis 1. We identified four sets of criteria for the evaluation: the **data collection requirements** of Section 2.5, the **process requirements** and **artifact requirements** defined in Section 3.2.3, as well as the **representational requirements** defined at the beginning of Chapter 4. *Traceability*, data collection, process, and representational requirements can be demonstrated through the application of the PREprocess and PDML to a real-world example. *Verification of consistency* and *validation of completeness* are more challenging in comparison. Section 5.1 shows how the metrics of *incompleteness*, *meaningless*, and *ambiguity* can be used for verification. To address the validation of completeness, we adapt the information-theoretical concept of *entropy* to provide a metric for both *conceptual saturation* and *stability* of the domain model.

In the following chapter, we demonstrate how the PREprocess in concert with PDML meets these criteria and show its seamless **integration with existing approaches**.

Chapter 6

Evaluation

The previous chapter detailed the evaluation methodology we are going to use to determine the utility and validity of our approach. To do so, we will apply the PREprocess (cf. Figure 3.3) to a real-world example, focusing on the *requirements-modeling loop*. Thus, we first have the choice between creating the concept for a new application with potential privacy implications, and employing the process for its development; or to employ the process to evaluate and improve upon an existing application. Due to resource constraints, the development of a new application was not possible. Furthermore, it is easier to elicit information on applications users are already familiar with, which is why we opted for the second option. As the focus of the process, we chose the tools available to students at Virginia Tech to manage their *directory information* and *education record*. There are multiple interfaces for access and management of this information (e.g., VT Search, Hokie SPA, and *my*VT). However, they all are front-ends for the Banner® Enterprise Resource Planning software [Ellucian 2016].

This application has obvious privacy implications, and is furthermore interesting, since access to students' directory information and education record are governed under the Federal Education Rights and Privacy Act (FERPA; 20 U.S. Code §1232g). Furthermore, there are a large number of stakeholders involved, going beyond just the students of at Virginia Tech, including faculty, staff, administration, and other entities. Lastly, this choice of target application has the advantage of relatively easy access to the main stakeholders and users (i.e., students). Before examining the functionality and settings of the Banner for the management of directory information and education record, it is worthwhile examining the language and regulations within FERPA.

6.1 The Federal Education Rights and Privacy Act (FERPA)

FERPA was passed in 1974 to regulate the access of parents to the education records of their children and apply to any institution or educational agency which wants to receive federal funding. While the law primarily talks about parents' rights, these rights are transferred over to the student at the age of eighteen [20 U.S. Code §1232g (d)]. Among the most important aspects of this law is the fact that it not only establishes the right to review and request corrections to an education record, but the stipulation that releasing any parts of the education record requires express permission of the parents (or adult student). In this regard, it is important to note the distinction between what the law calls *education record*, and what information is contained in *directory information*. Thus, education record is defined as:

> [...] those records, files, documents, and other materials which—
>
> (i) contain information directly related to a student; and
>
> (ii) are maintained by an educational agency or institution or by a person acting for such agency or institution [20 U.S. Code §1232g (a)(4)(A)].

It is noteworthy that section 20 U.S. Code §1232g (a)(4)(B) excludes the personal notes of administrative or educational personnel (given that only that person has access to them), employee records (should the student be employed by the institution), record by law enforcement, physicians, psychologists, or psychiatrists. Conversely, the law defines directory information as:

> [...] the student's name, address, telephone listing, date and place of birth, major field of study, participation in officially recognized activities and sports, weight and height

> of members of athletic teams, dates of attendance, degrees and awards received, and the most recent previous educational agency or institution attended by the student [20 U.S. Code §1232g (a)(5)(A)].

The protection of directory information is weaker than that of education records, as institutions or educational agencies need only inform parents or students of age of which of the categories of directory information they intend to make public, which parents and students then have the opportunity to veto. Thus, to maintain compliance with the law, educational institutions — such as Virginia Tech — send out annual FERPA notices to students and their parents.

An interesting situation arises once a student comes of age, if that student's parents desire access to their child's education record. While section 20 U.S. Code §1232g (d) clearly transfers the rights from the parents to the student once the student comes of age, yet 20 U.S. Code §1232g (b)(1)(H) *allows* the release of education records to the parents of a *dependent* student. Furthermore, in the Commonwealth of Virginia, Va. Code §231.1-1303 even *requires* such access. The intention of the law is, arguably, to provide parents access to the results of the education they pay for. However, while the law is very explicit about this particular aspect, it would be interesting to see how these rules influence the lived experience of parents and their adult children.

These statutes provide the legal framework which any application managing access to education records and directory information has to abide by.

6.2 The Application

As mentioned before, the Banner Enterprise Resource Planning software is used to manage student information at Virginia Tech. This application is not only used for the management of the education record of students, but its scope goes far beyond those purposes. We are going to focus exclusively on the aspects of the system involved with students' education records and directory information. Since students do not have direct access to the Banner system, this is done by exploring two of its front-ends, namely VT Search (public) and Hokie Spa (private).

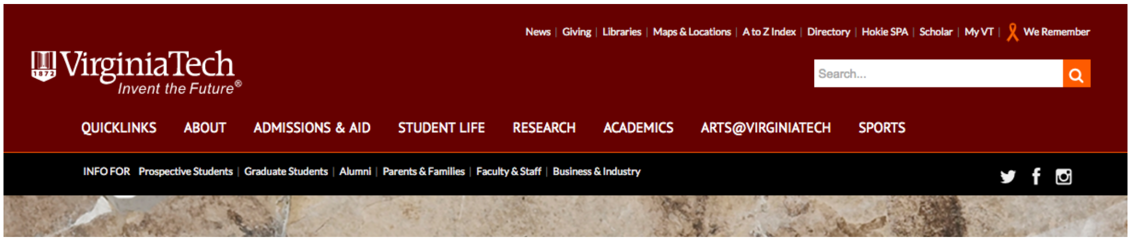
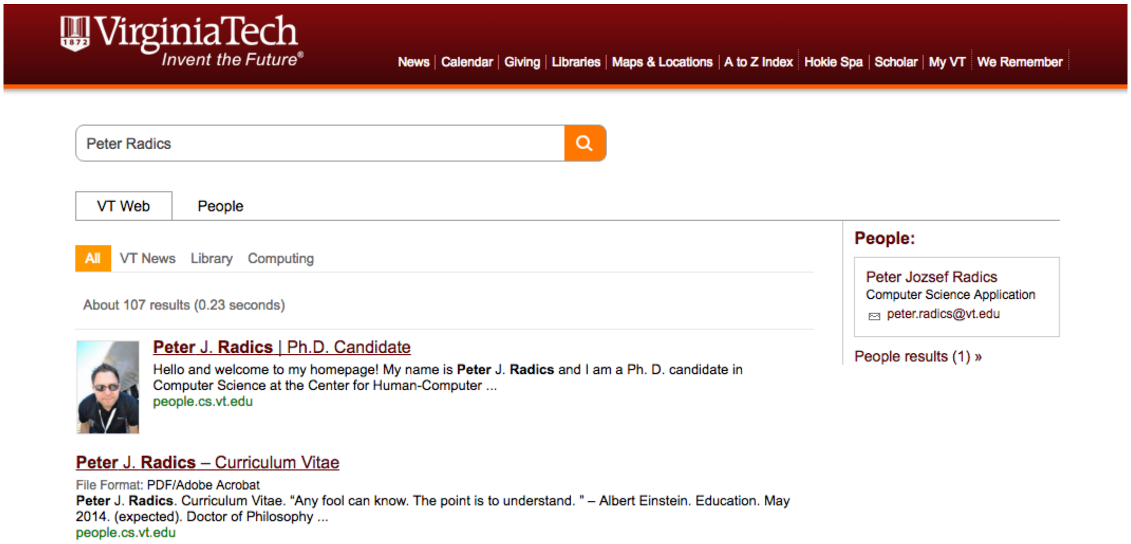

News | Giving | Libraries | Maps & Locations | A to Z Index | Directory | Hokie SPA | Scholar | My VT | We Remember
VirginiaTech
Invent the Future®
Search...
QUICKLINKS
ABOUT
ADMISSIONS & AID
STUDENT LIFE
RESEARCH
ACADEMICS
ARTS@VIRGINIATECH
SPORTS
INFO FOR Prospective Students | Graduate Students | Alumni | Parents & Families | Faculty & Staff | Business & Industry

Figure 6.1: VT Search on the Virginia Tech Homepage.

VT Search (shown in Figure 6.1) is the search functionality integrated into Virginia Tech's homepage. It presents itself to visitors of the site as a simple search field at the top-right of the homepage. In its current iteration, the search field does not reveal that, besides providing quick access to content within the webpages of Virginia Tech, VT Search can be also used to search for directory information of students, faculty, and staff. Previous iterations of the search bar made this functionality explicit by either providing a radio button, allowing to select either 'Web' or 'People'; or a prompt to 'Search pages and people'. Thus, part of the evaluation of the system needs to include whether stakeholders of the application are aware of this functionality. Figure 6.2 shows the result of entering 'Peter Radics' into the search field, revealing both a 'People' tab within the results, and a list of 'People results' in a side-bar on the right.

Another point of interest for the VT Search front-end is its default configuration. Namely, the 'Person Details' page accessible from the search results (see Figure 6.3), by default, is set to publish a wide array of information. Thus, besides the student's *full name*, *academic major*, *email address*, and personal identifier (*PID*), the page will also display both *mailing address* and *phone number*. These options, however, are configurable, which explains the much smaller information presented in Figure 6.3. Nevertheless, this raises the question of whether students are aware of the permissiveness of the default settings. This becomes quite important should the students' preferences deviate from these settings. Thus, the evaluation should address these issues concerning the management of *directory information*.

Regarding the management of *education records*, the relevant front-end is Hokie Spa[1]. Besides


VirginiaTech
Invent the Future®
News | Calendar | Giving | Libraries | Maps & Locations | A to Z Index | Hokie Spa | Scholar | My VT | We Remember
VT Web
People
All
VT News
Library
Computing
People:
People results (1) »

Peter Radics

About 107 results (0.23 seconds)

Peter J. Radics | Ph.D. Candidate
Hello and welcome to my homepage! My name is **Peter** J. **Radics** and I am a Ph. D. candidate in Computer Science at the Center for Human-Computer ...
people.cs.vt.edu

Peter J. Radics – Curriculum Vitae
File Format: PDF/Adobe Acrobat
Peter J. **Radics**. Curriculum Vitae. "Any fool can know. The point is to understand. " – Albert Einstein. Education. May 2014. (expected). Doctor of Philosophy ...
people.cs.vt.edu

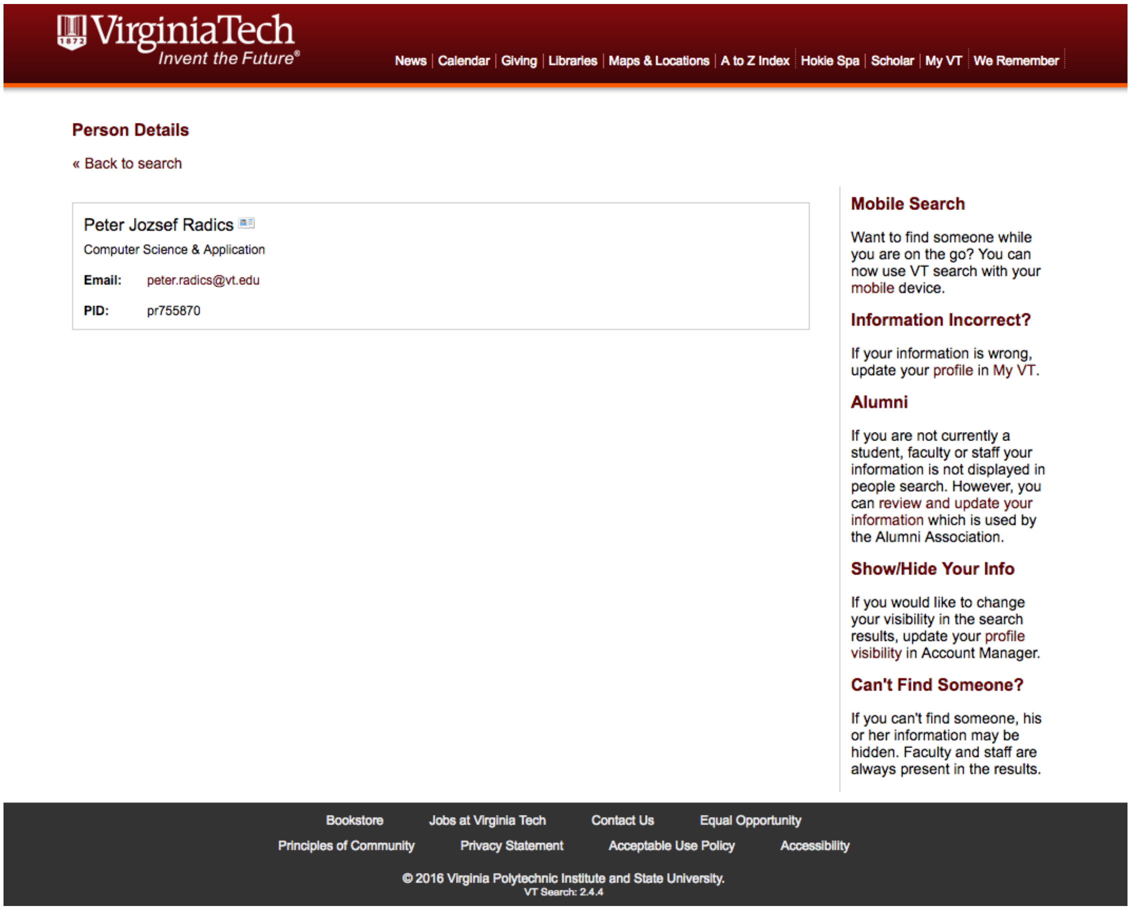
Peter Jozsef Radics
Computer Science Application
peter.radics@vt.edu

Figure 6.2: General search results for 'Peter Radics' in VT Search.

providing access to course registration and schedule; grades; transcripts; university account information; and much more, Hokie Spa also contains an option to authorize the release of education records to third parties. As shown in Figure 6.4, this can be done by providing the name of the person to authorize, along with information on their relationship to the student and the student's tax dependency status to them. Given that information, plus an eight character alphanumeric pass code, the so authorized person can get access to the *entirety* of the student's education record. Thus, the questions regarding this interface are, whether students would prefer providing more fine-grained access to their records (i.e., restrict access to only parts of it), and whether providing access on a per-individual basis is too fine-grained.

In addition to these question from a purely engineering perspective, the implications of required access by parents of tax dependent students (cf., Section 6.1) deserves further consideration. From a social science perspective, the behavior around this sharing of information (and the influence of said requirement) are worth exploring. More generally, students' attitudes towards their grades and their practice around sharing information on them should be part of the evaluation. These practices, then, can yield further implications for design.

[1] Spa, here, stands for single-purpose access, not a place for relaxation.


VirginiaTech
Invent the Future®
News | Calendar | Giving | Libraries | Maps & Locations | A to Z Index | Hokie Spa | Scholar | My VT | We Remember

Person Details

« Back to search

Peter Jozsef Radics

Computer Science & Application

Email: peter.radics@vt.edu

PID: pr755870

Mobile Search

Want to find someone while you are on the go? You can now use VT search with your mobile device.

Information Incorrect?

If your information is wrong, update your profile in My VT.

Alumni

If you are not currently a student, faculty or staff your information is not displayed in people search. However, you can review and update your information which is used by the Alumni Association.

Show/Hide Your Info

If you would like to change your visibility in the search results, update your profile visibility in Account Manager.

Can't Find Someone?

If you can't find someone, his or her information may be hidden. Faculty and staff are always present in the results.

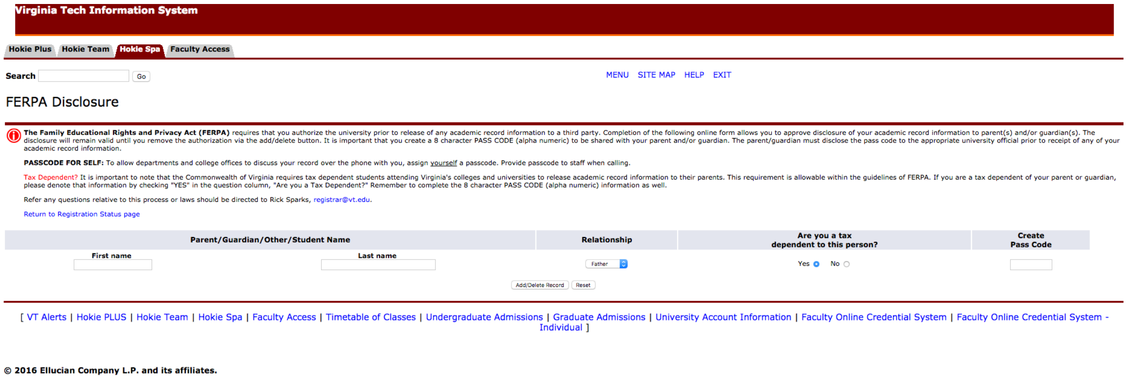
Figure 6.3: Directory Information for 'Peter Radics' in VT Search.

6.3 Research Design

Given the full description of the target application and its context, we have sufficient information to make decisions about the details of the data collection step (Step (1) in Figure 3.3). Thus, we will first describe the stakeholders of our application, choose an appropriate sample, and decide on the data collection methodology to use for the evaluation.

6.3.1 Stakeholder Analysis

The principal stakeholders of the application are easily identified: they are the intended users of our application, namely, the *students* at Virginia Tech. We will further subdivide this group into



FERPA Disclosure

The Family Educational Rights and Privacy Act (FERPA) requires that you authorize the university prior to release of any academic record information to a third party. Completion of the following online form allows you to approve disclosure of your academic record information to parent(s) and/or guardian(s). The disclosure will remain valid until you remove the authorization via the add/delete button. It is important that you create a 8 character PASS CODE (alpha numeric) to be shared with your parent and/or guardian. The parent/guardian must disclose the pass code to the appropriate university official prior to receipt of any of your academic record information.

PASSCODE FOR SELF: To allow departments and college offices to discuss your record over the phone with you, assign yourself a passcode. Provide passcode to staff when calling.

Tax Dependent? It is important to note that the Commonwealth of Virginia requires tax dependent students attending Virginia's colleges and universities to release academic record information to their parents. This requirement is allowable within the guidelines of FERPA. If you are a tax dependent of your parent or guardian, please denote that information by checking "YES" in the question column, "Are you a Tax Dependent?" Remember to complete the 8 character PASS CODE (alpha numeric) information as well.

Refer any questions relative to this process or laws should be directed to Rick Sparks, registrar@vt.edu.

Return to Registration Status page

Parent/Guardian/Other/Student Name		Relationship	Are you a tax dependent to this person?	Create Pass Code
First name	Last name			
		Father	Yes ● No ○	

[VT Alerts | Hokie PLUS | Hokie Team | Hokie Spa | Faculty Access | Timetable of Classes | Undergraduate Admissions | Graduate Admissions | University Account Information | Faculty Online Credential System | Faculty Online Credential System - Individual]

© 2016 Ellucian Company L.P. and its affiliates.

Figure 6.4: FERPA Disclosure Settings in Hokie Spa.

undergraduate students and *graduate students*. Since we are dealing with a university setting, we can furthermore count *faculty*, *staff*, and *university administrators* among the stakeholders of our application. Section 6.1, furthermore, reveals two additional stakeholder groups: *parents* and *government officials*. Each of these groups has different characteristics, especially in terms of factors relevant for stakeholder management (cf. Section 2.3.2). Thus, through brainstorming, we can determine the *influence* and *interest* of each group with regards to the redesign of the application.

Among the stakeholder groups, undergraduate students represent by far the largest group with 25,318 enrolled students in the 2015–2016 academic year [Virginia Tech 2016]. They are primary users of the application, as it is used to manage their directory information and education record. Therefore, they are among the groups with the highest interest in the outcomes of the project. However, studies have shown that adolescents and young adults exhibit less concern towards their online presence than older adults [Squicciarini and Griffin 2012; Yardi and Bruckman 2011], thus decreasing the overall interest. In terms of influence, the sheer number of group members give undergraduate students significant clout towards the university (which is amplified through their close relationship with the parent/guardian stakeholder group). Furthermore, FERPA provides undergraduates with particular protection and possible legal remedies in case of the violation of their rights. Thus, this stakeholder group should be *managed closely*.

Graduate students, in comparison, are a much smaller group with only 4,793 members (5,280 if also counting professional students)[Virginia Tech 2016]. This significantly reduces the influence of this group towards the university — especially, since many graduate students are also employed by the university. Nevertheless, they are primary users of the application, since they also manage both their directory information and education record through the system. Furthermore, their rights are also protected through FERPA. As members of this group are, in general, older than undergraduate students, we can assume that their interest in the outcomes of this project are higher than that of the undergraduate students. Given their relatively low influence, graduate students should therefore *kept informed* about the project's progress and outcomes.

The faculty stakeholder group is slightly smaller than the graduate student group, with a total of 4,079 members in 2015–2016 [Virginia Tech 2016]. They can be counted among the secondary users of the application, since it also allows them to manage parts of their directory information available through VT Search. Furthermore, they are mainly responsible for the safeguarding of students' education records by not divulging information to non-authorized individuals. Moreover, they face disciplinary action should they fail in this responsibility, thus giving them a high interest in the outcomes of this project. Their status as faculty provides them with influence regarding the outcomes of the project. However, their influence might be less pronounced than that of the undergraduate student group, as their interest is secondary to that group's preferences. This places faculty somewhere between groups to *manage closely* and groups to *keep informed*.

Similar in size to both the graduate student and faculty group, the supporting staff at Virginia Tech makes up 3,467 members [Virginia Tech 2016]. They are also part of the secondary users of the application, since their directory information is available through VT Search as well. However, staff are often not as extensively involved in the management of education records, reducing their interest in the outcome of this project. Moreover, they are not as influential as faculty or undergraduate students. Thus, they should be *monitored*, but not given as much priority as the other groups.

Parents and guardians have a vested interest in the protection of their children's education records and directory information. Moreover, both FERPA and Virginia law provide them with access rights to their children's records, provided the child is younger than 24 and their tax dependent. This makes them potential secondary users of the system. However, a big part of their significant influence is a result of their financial involvement. In the vast majority of the cases, they are paying their children's tuition to the university. Yet, we can assume that their direct interest in the project is not as high as that of faculty or graduate students for two reasons. First, it is somewhat likely they will receive information about their children's education record directly from their children. Second, unless there are blatant violations of their children's rights, they might simply not be as aware of FERPA-related issues. Nevertheless, due to their influence, they should be *managed closely*.

The last two groups, university administrators and government officials, are similar both in terms of influence and interest. Due to their position as primary responsible parties for the enforcement of applicable laws, they have among the highest influence on the direction of the project. As part of their responsibility, they also have a vested interest in the project itself. However, this interest is restricted to the above mentioned enforcement of the rules. In other words, as long as the rules are adhered to, it can be assumed that their involvement in the project will be limited. Thus, both of these groups should be *kept satisfied*. This analysis leads to the stakeholder map in Figure 6.5.

Besides providing us with a clear picture of how to prioritize each stakeholder group, the stakeholder map also identifies the best candidates for the target population of the data collection effort. Namely, parents/guardians, undergraduate students, and faculty are obvious choices. Graduate students and university administrators, while not as important, can also contribute valuable data. In this regard, two additional factors should be considered. First, primary users should get preference over other groups in terms of data collection, as they are the people most likely to interact with the system. Furthermore, secondary users should get preference over non-users. Second, access to each group is vastly different. Thus, it is far easier to recruit undergraduate and graduate students than, for example, faculty or parents. Following this rationale, we selected undergraduate and graduate students as the target population for our inquiry.

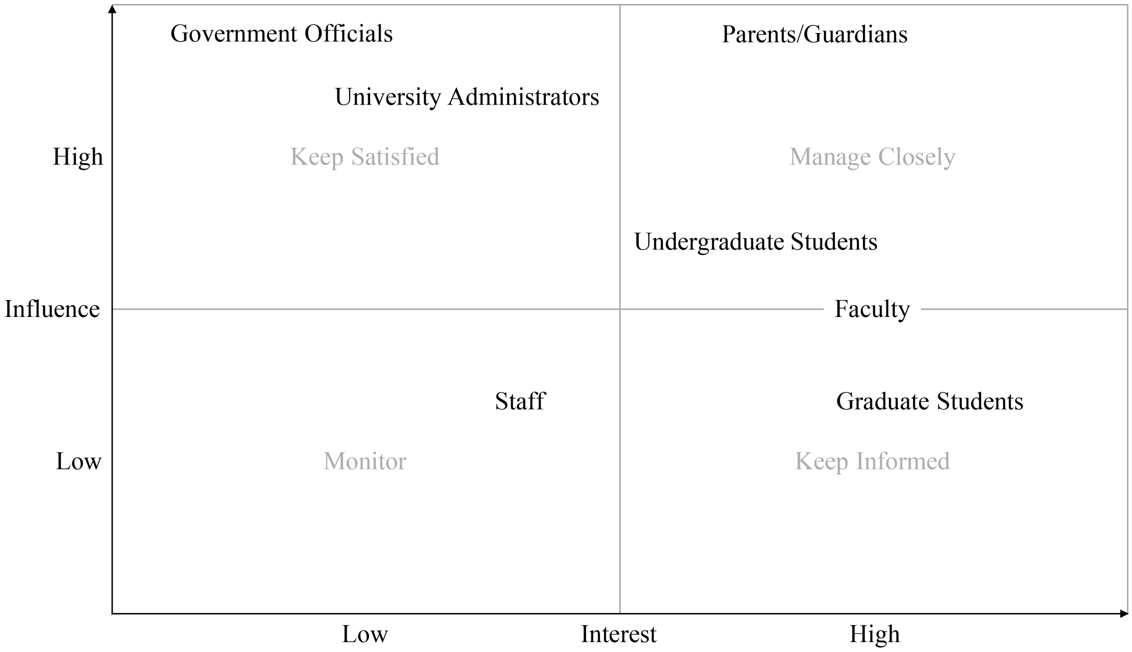


Figure 6.5: Stakeholder Map of the Evaluation Project.

6.3.2 Data Collection Strategy

Given the target population and project description, we need to determine the appropriate data collection strategy. Some of the considerations from Section 6.2 help with this task. First, we are dealing with an existing application, which requires a different approach than a completely new design would require. Thus, the inquiry need not focus on determining *what* functionality needs to be implemented, but rather on *how* existing functionality can be improved upon. We have identified two separate areas of focus: managing access to *directory information* and managing access to *education records*. In regards to directory information, we have determined a need to establish whether members of our target population are aware of the functionality and default settings of VT Search. Furthermore, we need to establish their preferences regarding the sharing of the distinct categories of directory information. Since the functionality regarding control of access to education records is much more limited, we need to establish whether the available settings are too limited, and how students would do or would want to share information about their records. These questions indicate that a combination of qualitative and quantitative data is desirable to be able to clearly delineate priorities and preferences on the one hand and receive qualitative feedback and insight into behavior on the other.

A further restriction is introduced through characteristics of the target population. First of all, the sheer combined size of the desired stakeholder groups (totaling at 30,598 members) prohibits total sampling. Furthermore, with a population of this size and diversity, a somewhat larger sample size is desirable, both in order to include minority opinions and to receive a broad cross section of preferences and behavior. This, however, excludes at least observation and ethnography from the list of possible approaches, since observing large sample sizes would require immense amounts of resources (cf. Table 2.3). Furthermore, except for the actual sharing behavior regarding education records, our application design will profit more from an internal viewpoint (i.e., from the students' perspective) than from the observations of an outside observer.

Finally, a major consideration regarding the recruitment of students is the time requirement of the study. Experience tells us that recruiting students for longer studies is generally more difficult than for shorter studies. Thus, recruitment for interviews and focus groups would face larger challenges than recruitment for a survey. Adding to that the desired larger sample size reveals surveys as the best fit for data collection.

In terms of sampling strategy we face the problem of incentive. Without any incentive for participation, student response rates tend to be relatively low. Thus, sampling is limited to those students who can be incentivized to participate. Furthermore, since we desire a combination of qualitative and quantitative data, considerations regarding validity of the quantitative portion suggest an at least partially random approach. While a heterogeneous sample would fit our requirements quite well, we lack strong criteria for determining heterogeneity between students regarding privacy behavior. Whereas cultural background or gender, for example, do influence privacy behavior in general, we still cannot expect the preferences or behavior within such groups to be uniform. This lack of clear distinction criteria also includes most other purposive sampling strategies, limiting us to purposive random sampling and convenience sampling. Of the two, purposive random sampling is clearly the better choice. Provided the sampling strategy and data collection method, we need to develop an appropriate data collection instrument. This requires us to reflect on our preconceptions and expectations of the phenomena of interest, and, based on this bracketing, determine the particular questions to ask.

6.3.3 Bracketing and Survey Question Development

There are three topics that the survey need to cover. We have already mentioned two topics before, namely questions about the management of directory information and the management of education records. The fact that we are dealing with two separate stakeholder groups requires us to furthermore determine characteristics of each of those groups, requiring us to ask demographic questions as well.

Demographic Information

In terms of demographic information, an important factor is maintaining the anonymity or at least confidentiality of participants, since being able to link responses to participants may influence the veracity and quality of responses. Thus, it is important to not ask too many demographic questions, since every question increases the likelihood of being able to identify a participant. However, at the very least, we need to be able to establish membership within the stakeholder groups. Beyond that, we need to limit demographic questions to factors that may influence the privacy preferences and practice of participants.

As we have seen in Section 1.2, some of the factors influencing overall privacy preferences and practice are *age*, *gender*, and *cultural background*. Of these three factors, age is the easiest to query, as there are no ambiguities about the term. Gender is at least slightly more complex, as we need to consider differences in the interpretation of the term. For instance, we could provide choices for the binary interpretation, namely ‘female’ and ‘male’. However, this excludes any participant who may not identify as either of these. Adding an ‘other’ category may be seen as dismissive. Thus, the simplest choice is to let participants provide their own values for this term.

Cultural background is a much more difficult concept to determine, especially, as it is an umbrella term for various subcategories. For example, cultural background is influenced by where a person lived throughout their life, which may be in multiple different places and cultures. Furthermore, even within cultures, there are sub-cultures that might be hard to elicit. Keeping in mind that we should not ask too specific demographic questions to avoid identifiability, we therefore will only ask participants to identify their race or ethnicity; their country of citizenship; and country of origin.

Besides these questions, a stipulation of FERPA in combination with Virginia law requires us to add additional questions. Namely, as we have seen in Section 6.1, Va. Code §231.1-1303 requires tax dependent students under the age of 24 who are Virginia residents to release their education record to their parents or guardians. Thus, we need to establish whether participants are Virginia residents, and whether — to their knowledge — they are claimed as tax dependents of their parents or guardians.

Directory Information

Regarding directory information, we first need to establish whether participants are aware of the functionality of VT Search. In addition, it may be interesting to determine whether or not they actually used VT Search to search for faculty, staff, or other students, and for what purpose. If they had not used VT Search, it is furthermore valuable to find out whether they attempted to find that information somewhere else. Additionally, we need to determine whether participants are aware of its permissive default settings regarding their directory information. We expect that participants may not be aware and that many of them, in general, would prefer their phone number and mailing address not to be shown. It would, furthermore, be interesting to see how strongly they feel either way regarding the default settings.

More importantly, however, we need to determine their preferences regarding the protection of their directory information. There are multiple options to consider here. First, we can adopt the current, binary settings of "public" and "confidential", and ask participant for each category of directory information, which they would prefer by default. However, as Kelley et al. [2011] succinctly stated, a simple opt-in/opt-out approach is often not appropriate for safeguarding information. Some of the privacy design frameworks discussed in Section 1.3 can provide alternatives. For example, both Chakraborty et al. [2011] as well as Poolsappasit and Ray [2008] use concepts of trust and quality of information in their frameworks. Thus, it would be worthwhile to investigate whether participants' preferences vary based on certain groups of people (like, for example, friends vs. faculty and staff), and try to deduce which groups are trusted more. Similarly, it would be valuable to see how participants would change the quality of their address based on the group that desires access to this piece of information. However, as with any prediction task in the privacy domain, it would be insufficient to simply provide participants with simple choices and ignore other contextual factors. Therefore, at the very least we have to also inquire about situations in which they may deviate from stated preferences.

Education Records

Finally, collecting information on participants' preferences and practice regarding the management of their education record requires probably the most consideration, as the controls in Hokie Spa are quite simplistic (cf. Figure 6.4). Furthermore, while the management of personally identifiable information (like the directory information discussed above) has been researched thoroughly (e.g., [Zang et al. 2015; Lee and Song 2011]), this is not really the case regarding education records. Thus, the very first question should be whether or not participants consider their education record to be private. While we expect this to overwhelmingly be the case, it nevertheless worth asking.

Further consideration should be given to participants' current practice regarding the sharing of their education records with others. From own experience, we at least expect undergraduate students to semi-regularly talk to their parents or guardians about their grades. In addition, friends oftentimes serve as a sounding board for issues regarding grades. Finally, fellow students in a class could serve as information source to determine one's own standing amongst one's peers. As there may be any number of additional groups or individuals that students talk to about their grades, a question should inquire about whether that is the case.

As grades are potentially sensitive information and since expectations regarding achieved grades might differ from actual grades — whether they be the student's own expectations, their friends', or even their parents — a student may feel motivated to deceive members of these groups about their actual grades. Different groups might, furthermore, provide different motivations for deception. And, while there is a certain amount of risk involved in deceptions, particularly in close-knit groups, the anticipated benefits of lying might outweigh the perceived risks. Iachello et al. [2005] have observed occurrences of deception in close-knit groups regarding location information, and it would be interesting to see whether their findings translate to education records.

Last, we need to determine whether or not the granularity of access to the education record provided through Hokie Spa is appropriate. Kalloniatis et al. [2008] suggest to treat both authentication and authorization as part of the privacy goals of users. Thus, in addition to determining whom participants would consider giving access to their education record, we need to determine the right access granularity, as well as the appropriate authentication and authorization strategy for the access. We expect preferences regarding these strategies to be somewhat varied, depending on personal differences between participants.

All of the considerations in this section are integrated in the design of the survey, which is provided in full in Appendix B. With the stakeholders identified and the data collection strategy laid out, we can now turn to the actual data collection and its results.

6.4 Data Collection Results

We advertised the study through graduate student mailing lists and the Virginia Tech SONA system. As an incentive for participation, undergraduate students signing up through the SONA system were offered one research credit towards requirements in undergraduate psychology classes. Graduate students could participate in a raffle for one of two $10 gift cards to a local book store. The survey was made accessible online through Virginia Tech's Qualtrics survey system.

6.4.1 Sample Composition and Demographics

A total of 212 students participated. Unfortunately, five results had to be discarded, as no useful information was provided within those results. Furthermore, our recruitment only yielded a total of 11 responses from graduate students. This only represents 5.31% of the remaining sample of 207 participants, which is much lower than their actual representation of 17.26% within the target population. Thus, we decided to exclude the graduate student responses from the analysis, as the number of members of this group would not have sufficed to establish any kind of generalizability for the whole group.

Another anomaly of the sample compared to the characteristics of the undergraduate population is the predominance of female participants. Out of the remaining 196 participants, 151 participants (77.04%) identified as female, 44 participants (22.45%) identified as male, and one participant (0.51%) identified as non-binary. In comparison, 57.43% of the undergraduate population at Virginia Tech identify as male and 42.52% identify as female [Virginia Tech 2016]. This distribution within the sample may arise from a higher percentage of females within the psychology program at Virginia Tech. Unfortunately, we do not have any numbers for the actual distribution. This imbalance decreases the generalizability of the findings to the entire population. However, since we are more concerned with exploring the phenomena related to the management of directory information and education records and not with the concrete distribution of phenomena within the population. Thus, gender-specificity of any phenomenon is not a large concern for our application,

Participants on average were 19.52 years old, with a median age of 19 years within the sample ($\sigma = 1.2225$). The youngest student was 18 years old (as per the survey's requirement), whereas the oldest was 23 years old. Thus, the participants represents a relatively young sample. Yet without an available age distribution for the entire undergraduate population, we cannot clearly tell whether the sample represents a strong deviation from the population as a whole.

In terms of diversity, Table 6.1 reveals that our sample is highly representative of the undergraduate population as a whole. The table shows adjusted values for the population, as the original values

Table 6.1: Race and Ethnicity of Participants (Population values reported in [Virginia Tech 2016]).

Race/Ethnicity	**Count**	**Percentage**	**Percentage in Population**
American Indian or Alaska Native	1	0.51%	0.15%
Asian	18	9.18%	9.91%
Black or African American	8	4.08%	3.99%
Hispanics of any race	6	3.06%	5.83%
Native Hawaiian or other Pacific Islander	1	0.51%	0.11%
White	152	77.55%	71.90%
Two or more races	9	4.59%	4.73%
Not reported	1	0.51%	3.39%

contained a category for ‘nonresident aliens’. We did not specifically ask for residency status from participants, only for country of citizenship and country of origin. In those categories, participants from the United States dominate the sample (with 184 or 93.88% U.S. citizens and 178 or 90.82% of participants born in the U.S.). The remaining 6.12% and 9.18%, respectively, come from a diverse set of countries, namely Canada, Panama, South Korea, Poland, Iran, Turkey, China, Germany, Nigeria, India, Japan, South Africa, and Slovenia. Of these, three participants (1.53%) hold dual citizenship in the United States and another country.

Of the participants, 148 (75.51%) were Virginia residents, 46 participants (23.47%) stated they were not residents, and 2 participants (1.02%) did not answer. Moreover, 174 participants (88.78%) stated they were tax dependents of their parents or guardians, 18 participants (9.18%) were not tax-dependent, and 4 participants (2.04%) did not know. A total of 136 participants (69.39%) were both Virginia Residents and tax dependent of their parents or guardians, and thus would fall under the provisions of Va. Code §231.1-1303 which requires them to provide their parents or guardians with access to their education records.

Thus, with the exception of the unusually large percentage of female participants, we can assume that our sample is mostly representative of the undergraduate population as a whole. For our examination of VT Search and Hokie Spa, the sample is furthermore applicable as a data source. If generalizability becomes a factor later on in the project, a factorial evaluation based on separating the male and female population should be considered. Therefore, before starting the analysis process, we will examine the quantitative results within the data for our two topic areas.

6.4.2 Quantitative Results regarding Directory Information

The part of our survey focusing on directory information contains the majority of the quantitative questions (namely, Questions II.1a, II.2a, II.3, II.4a, and II.5a; cf. Appendix B). The first question in this part (cf. Question II.1a) asked participants whether they had ever used VT Search to find information on faculty, staff, or other students at Virginia Tech. Of the participants, 98 (50%) responded that they had used VT Search before, 86 (43.88%) had not used it in the past, and 12 (6.12%) participants could not remember whether they had used it in the past. Among the students who had not used VT Search, 73 (84.88%) were not aware the functionality existed at all. In other words, 37.24% of the participants in total were not even aware of VT Search. This confirms our assumption from Section 6.3.3 that students may not have strong awareness of the capabilities of VT Search.

Turning to the question regarding their awareness of the permissive default settings of VT Search (cf. Question II.2a), 112 (57.14%) of the participants stated they were aware of these settings. Conversely, 84 (42.86%) participants were not aware. Interestingly, while the number of participants unaware of the default settings is almost the same as the number of non-users of VT Search, the two groups do not completely overlap. Thus, only 56 participants that did not use VT Search were not aware of the settings, whereas 29 of them were. On the opposite side, 24 participants did use VT Search and were, nevertheless, not aware of its permissive settings, compared to 73 that were. This lack of awareness, in combination with the permissiveness of the settings, should raise some concern.

Turning to Question II.3 reveals the disconnect between the default settings of VT Search from the reality of preferences voiced by the participants. Figure 6.6 shows that participants would prefer their mailing address (92.86%) and phone number (90.31%) to be treated confidential by default. An even 25% of participants would even prefer their email address not to be listed in search results. This confirms our predictions in Section 6.3.3 regarding the confidentiality of Mailing Addresses and Phone Numbers. Not surprisingly, neither full name nor academic major being publicly available raise too many concerns.

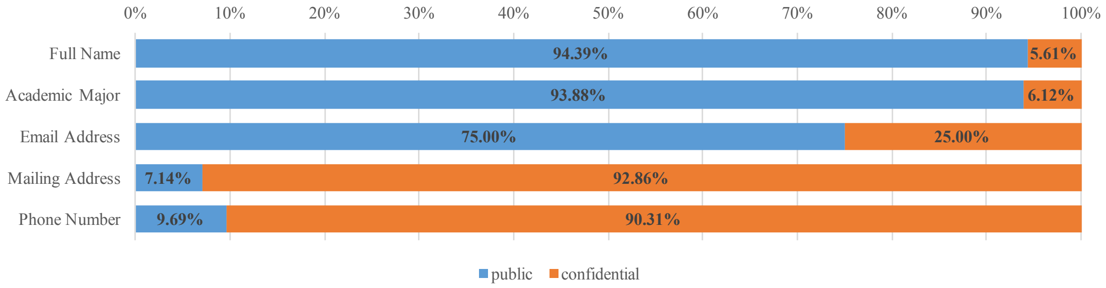


Figure 6.6: Preferences regarding Confidentiality of Directory Information (Question II.3).

An interesting phenomenon shown in Figure 6.6 is the fact that the protection of the (physical) mailing address is given higher priority than that of the (immaterial) phone number. The question arises whether this reflects a gender-specific preference introduced by the larger percentage of female participants, as physical security is a much stronger concern for females than for males. In fact, testing for independence between gender and preference regarding confidentiality reveal a significant dependence at $p < 0.01$ (two-tailed Fisher's exact test leads to $p = 0.0038$; two-tailed chi-square test with Yates' correction yields $\chi^2 = 8.3, p = 0.0040$). Regardless, it is obvious that there is sufficient cause to consider changing the default values for both mailing address and phone number, should a generic authorization approach be maintained.

However, Figure 6.7 shows that a more nuanced approach may be warranted. While the values for providing access to both full name and academic major from Figure 6.6 are strongly reflected in this figure, many of the other categories show a much more varied image. In the case of their email address, participants' preferences lean towards providing most of the provided groups with access. The overly generic 'everyone else' category, receiving by far the lowest value in terms of access granted, therefore, can be thought of as dominating the preferences for the other groups, resulting in the 25% value in Figure 6.6. In other words, given the choice only between giving everyone or no-one access to their information, participants will err on the side of caution.

Similarly, the relatively high values in favor of disclosure of both mailing address and phone number to relatives and friends in Figure 6.7 barely seem to have any impact on participants' strong preference to curtail that information shown in Figure 6.6. This raises the question whether, given only the limited opt-in or opt-out choice of VT Search, students would simply use other mechanisms to convey this information to appropriate recipients and eschew use of VT Search for this purpose entirely. In either case, these data points can be used to prioritize protection of information, with mailing addresses being the most sensitive and full names being the least.

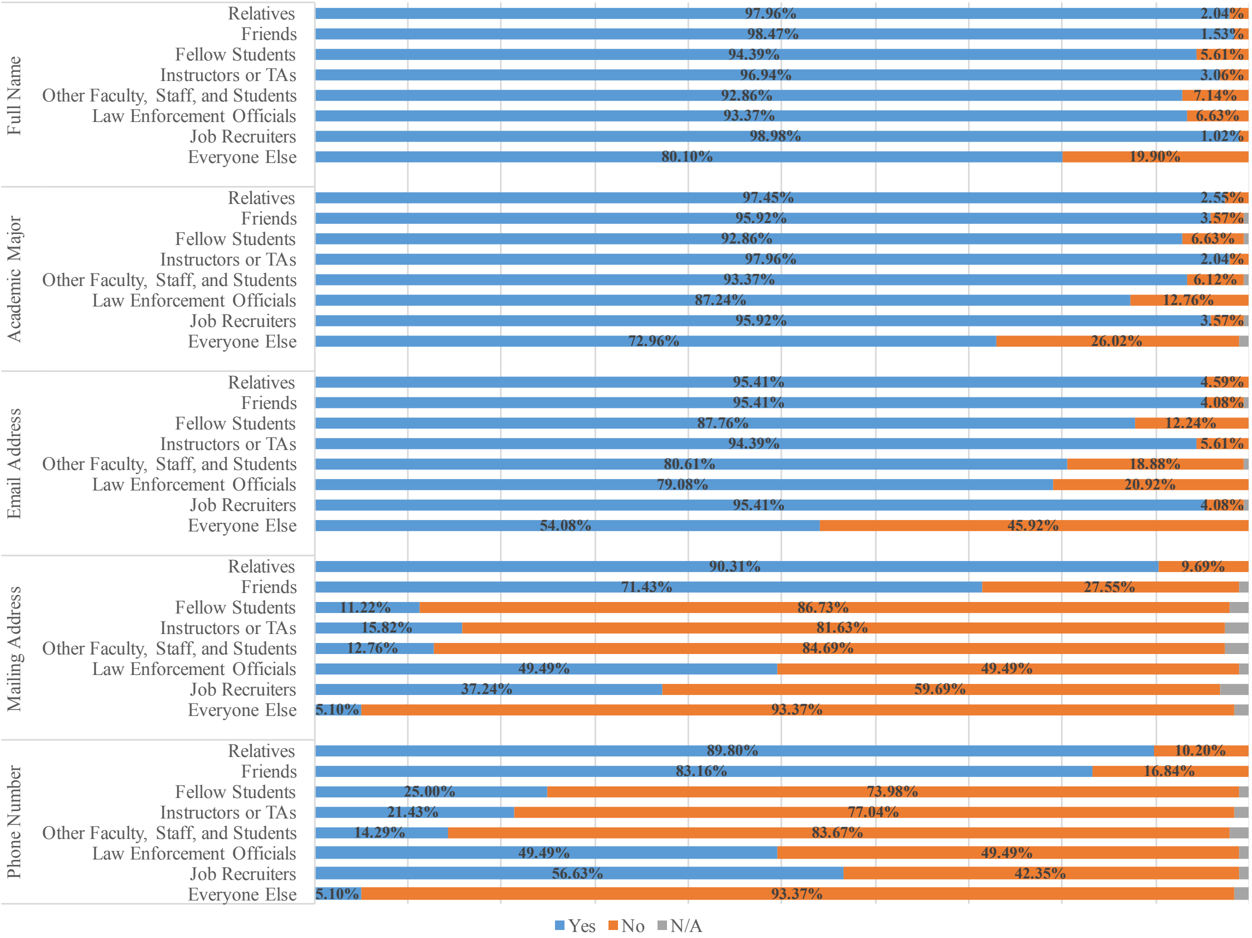


Figure 6.7: Preferences regarding Access to Directory Information (Question II.4a).

A further benefit of the data in Figure 6.7 is the fact that it reveals different levels of *trust* towards different groups. Not surprisingly, relatives and friends are the most trusted groups, with relatives being slightly more trusted than friends. In this regard, it would be interesting to see whether this ordering is influenced by the relatively young age of the participants, or whether this finding would translate into other populations as well. The groups that, somewhat surprisingly, is attributed a comparatively high amount of trust are job recruiters. Thus, 95.92% of participants would give recruiters access to their email, 56.63% would entrust them with their phone number, and 37.24% would even provide them with their mailing address. This high level of trust even goes so far that job recruiters beat out every other group in terms of access to participants' full name (with only 1.02% prohibiting their access). One can only assume that the pressure of finding employment drives up students' willingness to reveal their directory information. Therefore, it would be worthwhile to examine, whether this high level of trust is exhibited by older populations as well. In any case, the findings in Figure 6.7 strongly suggests examining group-based authentication strategies.

Turning to Question II.5a, Figure 6.8 reveals participants' attitudes towards sharing their mailing address at different levels of quality. The values for providing access to a participant's full address strongly coincide with the access preferences regarding mailing addresses in Figure 6.7. Probably the most notable addition by this figure is the large percentage of participants who would provide members of their community (i.e., fellow students, instructors, TAs, as well as other faculty, staff, or students) access to information on which city they live in. Similarly, both job recruiters and law enforcement officials receive a strong boost by these values as well. Therefore, during redesign of VT Search, a quality of information based approach for address sharing should at least be considered.

6.4.3 Quantitative Results regarding Education Records

Having covered the quantitative results regarding directory information, we can now turn to the third part of the survey and the quantitative questions regarding education records (Questions III.1, III.5, III.6, and III.7) in it. Recall that, in Section 6.3.3, we determined that the assumption of grades being considered private information bears confirmation. Presented with this question, 181 (92.35%) participant confirmed grades to be private, whereas 15 (7.65%) did not. This reflects the overwhelming support of the assumption we expected. The qualitative questions in this part of the survey need to be considered to determine the actual practice surrounding the sharing of this information.

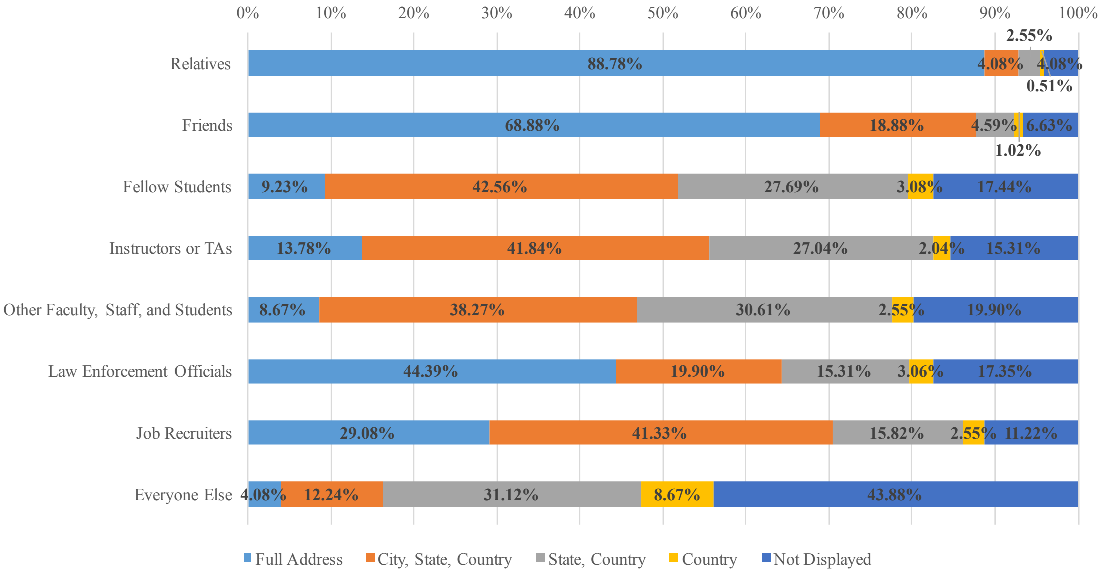


Figure 6.8: Preferences regarding Quality of Address (Question II.5a).

Regardless of the outcomes of those questions, we provided participants with different choices regarding the management of their education record. Namely, in Question III.5 we asked participants to choose the granularity of access, ranging from access to their entire record to access grade-by-grade. We will refer to this choice as the *access strategy* for the education records. Similarly, in Question III.6 we wanted to know whether participants preferred giving access to individuals, to all members of a group, or a combination of both. We call this choice the *authentication strategy*. Furthermore, we inquired whether participants would rather create rules regarding the access of their records up-front, or rather make decisions case-by-case. We use the term *authorization strategy* for this choice. Figure 6.9 reveals the preferences of the participants.

The immediate take-away from Figure 6.9 is that a binary decision strategy for providing access to education records is not appropriate. Only 30.10% of participants preferred providing access to their entire record, meaning that more than two-thirds of the sample would not agree with this choice. It is, furthermore, apparent that a per-semester access is the most strongly preferred option, with 40.82% of the participants stating this strategy as their preference. Despite these two groups making up more than 70% of the participants, one should not ignore the fact that almost a third of the participants preferred vastly more granular access.

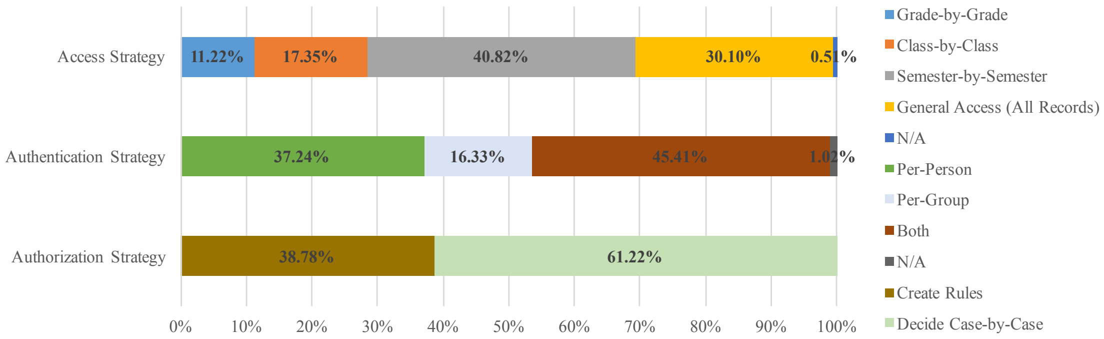


Figure 6.9: Preferences regarding Access Control Mechanisms (Questions III.5, III.6, and III.7).

Participants' preferences regarding authentication strategies is similarly varied. With 45.41% of the sample, the majority of the participants preferred the most flexible choice for authentication, namely a combination of both per-group and per-person based decisions. In fact, the amount of support per authentication strategy follows their degree of flexibility, with individual-based authentication coming in second (37.24%) and group-based authentication coming in last (16.33%). This ordering can also provide developers a prioritization of features in terms of implementation. Thus, given insufficient resources to implement both individual and group-based authentication, priority should go to implement the former rather than the latter.

Finally, participants reveal their preference for 'notice and choice' in their responses regarding authorization strategies. Namely, 61.22% of participants preferred making access decisions case-by-case, compared with 38.8% who preferred specifying rules up-front. This, once again, reveals a preference for flexibility and contextuality over more traditional approaches. With the initial analysis of the data complete, we can now turn to developing the domain model for our application (Step (2) in Figure 3.3).

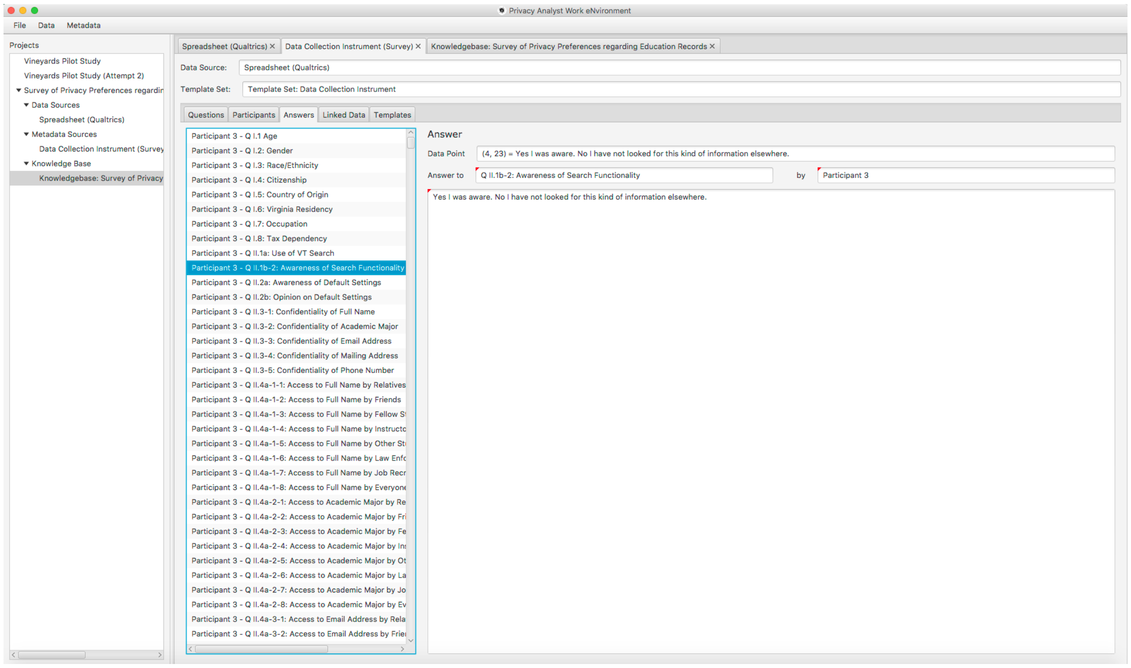
6.5 Domain Modeling

As is often the case, analysis and domain modeling cannot immediately commence as data management issues need to be addressed. Thus, the results of the survey were not in an immediately useful format, but rather occupied 18,897 cells in a comma-separated values (CSV) file. Therefore, the immediate concern is the transformation of the data into a more useful format. As mentioned in Section 6.4.1, contributions of 16 participants (11 graduate students and 5 incomplete submissions) have to be removed. While spreadsheet applications (such as Microsoft Excel) are certainly valid choices for this task, looking ahead at modeling data for our 196 participants within such an application is simply not feasible. Especially considering our requirement of *traceability*, using multiple applications for data management and analysis would make the process significantly more difficult.

For this reason, we have developed an application specifically for the support of analysts employing the PREprocess: the Privacy Analyst's Work eNvironment (PAWN; see Figures 6.10 and 6.12). PAWN allows an analyst to simply import a spreadsheet as well as modify and sanitize its contents within the application. Furthermore, it provides an initial layer of abstraction of the raw data in terms of *participants*, *questions*, and *responses* (or *answers*). In fact, these are exactly the concepts we introduced in Section 5.2.2 as components of the definition of *privacy-related information* (cf. Definition 5.13).

Thus, after sanitizing the raw data within the spreadsheet, the analyst's first task is the initial abstraction of the separate spreadsheet cells into questions, participants, and answers. Since matrix-table questions like Question II.4a are represented as one question per combination of row and column, the number of questions within the abstraction of our survey rises from 30 questions (cf. Appendix B) to a total of 80 questions. Provided these questions and our 196 participants, PAWN automatically populates the survey with the responses, yielding a total of 15,564 responses. Figure 6.10 contains a screenshot showing one of the resulting answers. *Traceability* is established by extracting the value of the spreadsheet cell into the 'value' of the response, as well as by providing a direct reference to the originating spreadsheet cell.

Given our sanitized and abstracted *privacy-related information*, we can proceed with the analysis. We will employ the information modeling process outlined in 3.3.1. The domain modeling process represents Step (2) in Figure 3.3. Furthermore, we will employ the Privacy Domain Modeling


Privacy Analyst Work eNvironment
File
Data
Metadata
Projects
Vineyards Pilot Study
Vineyards Pilot Study (Attempt 2)
Survey of Privacy Preferences regardin
Data Sources
Spreadsheet (Qualtrics)
Metadata Sources
Data Collection Instrument (Survey
Knowledge Base
Knowledgebase: Survey of Privacy
Spreadsheet (Qualtrics) ×
Data Collection Instrument (Survey) ×
Knowledgebase: Survey of Privacy Preferences regarding Education Records ×
Questions
Participants
Answers
Linked Data
Templates
Answer

Data Source: Spreadsheet (Qualtrics)

Template Set: Template Set: Data Collection Instrument

Participant 3 - Q I.1 Age
Participant 3 - Q I.2: Gender
Participant 3 - Q I.3: Race/Ethnicity
Participant 3 - Q I.4: Citizenship
Participant 3 - Q I.5: Country of Origin
Participant 3 - Q I.6: Virginia Residency
Participant 3 - Q I.7: Occupation
Participant 3 - Q I.8: Tax Dependency
Participant 3 - Q II.1a: Use of VT Search
Participant 3 - Q II.1b-2: Awareness of Search Functionality
Participant 3 - Q II.2a: Awareness of Default Settings
Participant 3 - Q II.2b: Opinion on Default Settings
Participant 3 - Q II.3-1: Confidentiality of Full Name
Participant 3 - Q II.3-2: Confidentiality of Academic Major
Participant 3 - Q II.3-3: Confidentiality of Email Address
Participant 3 - Q II.3-4: Confidentiality of Mailing Address
Participant 3 - Q II.3-5: Confidentiality of Phone Number
Participant 3 - Q II.4a-1-1: Access to Full Name by Relatives
Participant 3 - Q II.4a-1-2: Access to Full Name by Friends
Participant 3 - Q II.4a-1-3: Access to Full Name by Fellow St
Participant 3 - Q II.4a-1-4: Access to Full Name by Instructo
Participant 3 - Q II.4a-1-5: Access to Full Name by Other St
Participant 3 - Q II.4a-1-6: Access to Full Name by Law Enfo
Participant 3 - Q II.4a-1-7: Access to Full Name by Job Recr
Participant 3 - Q II.4a-1-8: Access to Full Name by Everyone
Participant 3 - Q II.4a-2-1: Access to Academic Major by Re
Participant 3 - Q II.4a-2-2: Access to Academic Major by Fri
Participant 3 - Q II.4a-2-3: Access to Academic Major by Fe
Participant 3 - Q II.4a-2-4: Access to Academic Major by Ins
Participant 3 - Q II.4a-2-5: Access to Academic Major by Ot
Participant 3 - Q II.4a-2-6: Access to Academic Major by La
Participant 3 - Q II.4a-2-7: Access to Academic Major by Jo
Participant 3 - Q II.4a-2-8: Access to Academic Major by Ev
Participant 3 - Q II.4a-3-1: Access to Email Address by Rela
Participant 3 - Q II.4a-3-2: Access to Email Address by Frie

Data Point (4, 23) = Yes I was aware. No I have not looked for this kind of information elsewhere.

Answer to Q II.1b-2: Awareness of Search Functionality by Participant 3

Yes I was aware. No I have not looked for this kind of information elsewhere.

Figure 6.10: Traceability of Information in the Privacy Analyst's Work eNvironment (PAWN).

Language (PDML) presented in Section 4.2 to represent our domain model. Support for PDML is built into PAWN, which allows the analyst to model directly within the application. Furthermore, an additional benefit of the combination of PDML and PAWN is the ability to perform bracketing of assumptions through creating *templates*.

6.5.1 Bracket Assumptions through Templates

Templates are formal statements about the assumptions of the analyst. As such, creating templates to formalize the analyst's assumptions and predictions of the occurrence of phenomena within the privacy-related information is a *model-driven* process. By using PDML for the domain modeling process, such assumptions can be interpreted as prototypical *assertions*. Thus, we can partition templates, analogous to assertions, into *instance templates* and *relationship templates*. These templates are formulated through a (currently very basic) expression language. Thus, if the analyst expects answers to a question to always contain information about the parents of a participant, the analyst can create an instance template with value 'Parents (@participant.name)', which allows

PAWN's template engine to replace the value with the participant's identifier and create a corresponding instance within the PDML knowledge base. Currently, the expression language supports the following expressions:

- @participant.name
- @participant.value
- @question.name
- @question.value
- @answer.name
- @answer.value
- @domain (relationship templates)
- @range (relationship templates)

This, for example, allows us to specify our expectation for responses to Questions II.1a and II.1b-2 through the template depicted in Figure 6.11. This technique is particularly useful in the case of quantitative choice questions (like Question II.1a), as the response is entirely made up of choices provided by the analyst. For qualitative text questions (like Question II.1b-2) a template can only specify the assumptions of the analyst contained in the question. Manual chunking of the information contained in the actual responses of participants is still required for these types of questions.

Thus, given the large amount of quantitative questions in our survey, we can automate large parts of the chunking process. In fact, creating templates for our questions results in a total of 310 templates. Of those, 48 are instance templates and 262 are relationship templates. A reference of all templates is provided in Appendix C. This reflects the relatively fine granularity of our chunking approach, chunking data at the subsentence level. Moreover, it becomes apparent that using templates to semi-automate the chunking process at this level is vastly beneficial, as manually instantiating the assertions represented by our templates would take a significant amount of time[2].

[2] In fact, manual encoding of all responses of *a single* participant takes between four and six hours. Template-based generation of assertions for *all* participants only takes about eight hours (with vast room for optimization of the current implementation in PAWN).

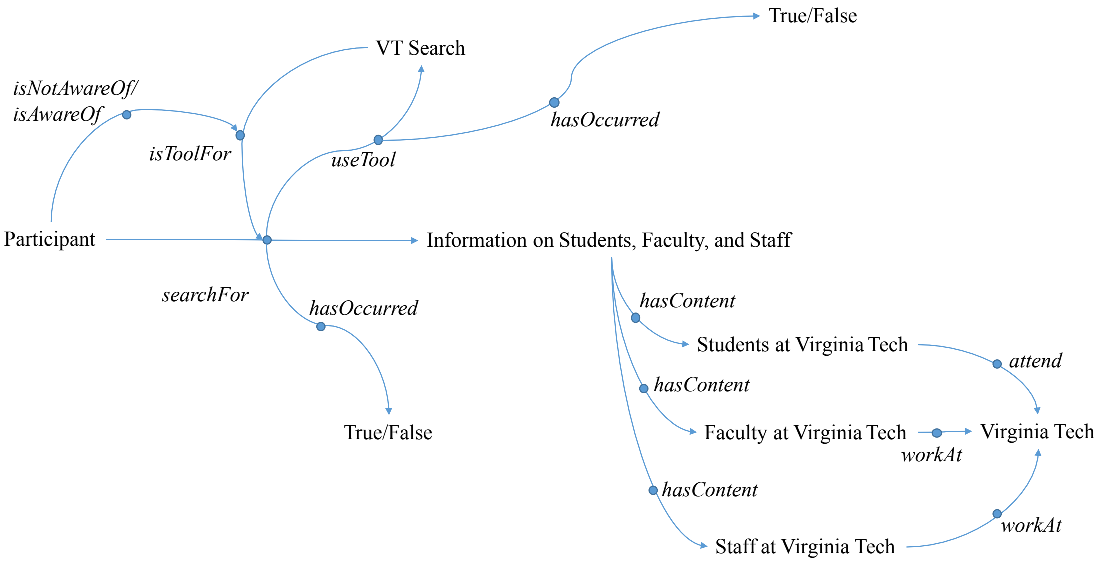


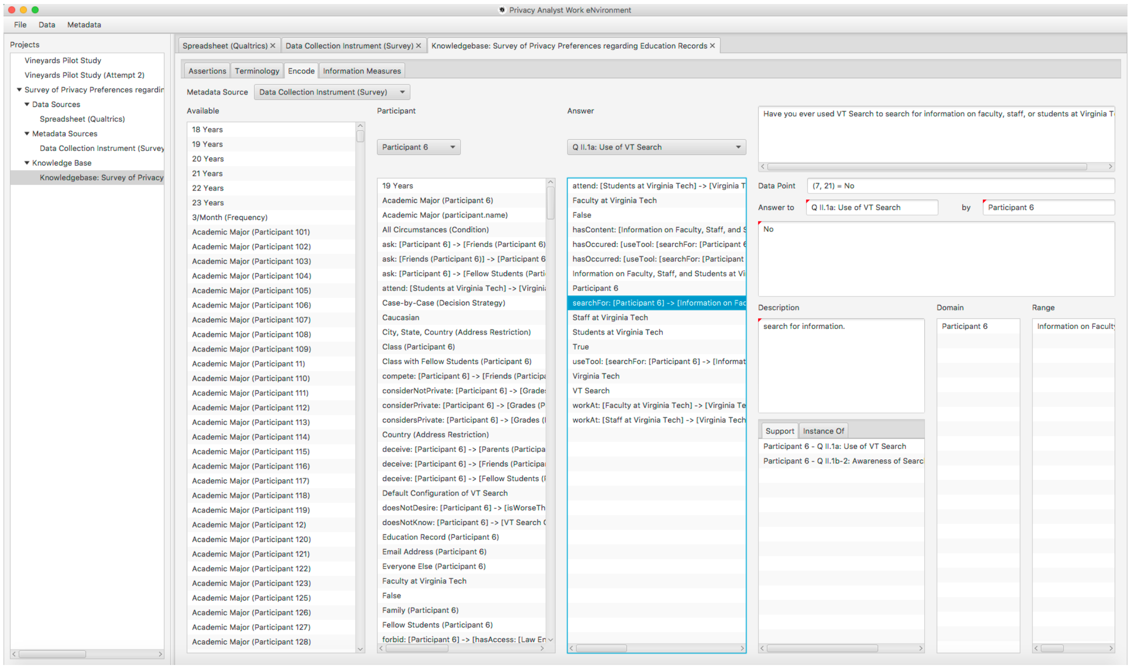
Figure 6.11: Example of a Template representing Question II.1a and Parts of Question II.1b-2.

6.5.2 Chunking of Information to Generate Assertions

While template creation and evaluation automates parts of the chunking process (and thus significantly reducing the time involved in the process) the analyst still has to perform the manual chunking of the free-form questions. These questions are especially important, as they represent the sources of truly unique assertions of the participants.

As shown in Figure 6.12, PAWN provides the analyst with all the information needed to streamline the encoding process. Thus, the encoding view provides lists of all assertions to allow sharing of common assertions (e.g., ‘Virginia Tech’) between participants. Furthermore, two more levels of filtering are provided on assertions, with one list containing all assertions used by the current participant as well as all assertions used to model the current response. Furthermore, the view contains the entire value of the response, as well as information about the currently selected assertion. Finally, to maintain traceability of the decisions back to the raw data, every assertion added to a particular response will receive that response as part of its *support*.

Tool support notwithstanding, chunking information is still a significantly challenging and time-


Privacy Analyst Work eNvironment
File
Data
Metadata
Projects
Spreadsheet (Qualtrics) ×
Data Collection Instrument (Survey) ×
Knowledgebase: Survey of Privacy Preferences regarding Education Records ×
Assertions
Terminology
Encode
Information Measures
Metadata Source
Available
Participant
Answer
Description
Domain
Range
Support
Instance Of

Projects:

- Vineyards Pilot Study
- Vineyards Pilot Study (Attempt 2)
- ▾ Survey of Privacy Preferences regardir
  - ▾ Data Sources
    - Spreadsheet (Qualtrics)
  - ▾ Metadata Sources
    - Data Collection Instrument (Survey
  - ▾ Knowledge Base
    - Knowledgebase: Survey of Privacy

Metadata Source: Data Collection Instrument (Survey)

Available:

18 Years
19 Years
20 Years
21 Years
22 Years
23 Years
3/Month (Frequency)
Academic Major (Participant 101)
Academic Major (Participant 102)
Academic Major (Participant 103)
Academic Major (Participant 104)
Academic Major (Participant 105)
Academic Major (Participant 106)
Academic Major (Participant 107)
Academic Major (Participant 108)
Academic Major (Participant 109)
Academic Major (Participant 11)
Academic Major (Participant 110)
Academic Major (Participant 111)
Academic Major (Participant 112)
Academic Major (Participant 113)
Academic Major (Participant 114)
Academic Major (Participant 115)
Academic Major (Participant 116)
Academic Major (Participant 117)
Academic Major (Participant 118)
Academic Major (Participant 119)
Academic Major (Participant 12)
Academic Major (Participant 120)
Academic Major (Participant 121)
Academic Major (Participant 122)
Academic Major (Participant 123)
Academic Major (Participant 125)
Academic Major (Participant 126)
Academic Major (Participant 127)
Academic Major (Participant 128)

Participant: Participant 6

19 Years
Academic Major (Participant 6)
Academic Major (participant.name)
All Circumstances (Condition)
ask: [Participant 6] -> [Friends (Participant 6)
ask: [Friends (Participant 6)] -> [Participant 6
ask: [Participant 6] -> [Fellow Students (Parti
attend: [Students at Virginia Tech] -> [Virgini
Case-by-Case (Decision Strategy)
Caucasian
City, State, Country (Address Restriction)
Class (Participant 6)
Class with Fellow Students (Participant 6)
compete: [Participant 6] -> [Friends (Participa
considerNotPrivate: [Participant 6] -> [Grade
considerPrivate: [Participant 6] -> [Grades (P
considersPrivate: [Participant 6] -> [Grades (
Country (Address Restriction)
deceive: [Participant 6] -> [Parents (Participa
deceive: [Participant 6] -> [Friends (Participa
deceive: [Participant 6] -> [Fellow Students (
Default Configuration of VT Search
doesNotDesire: [Participant 6] -> [isWorseTh
doesNotKnow: [Participant 6] -> [VT Search (
Education Record (Participant 6)
Email Address (Participant 6)
Everyone Else (Participant 6)
Faculty at Virginia Tech
False
Family (Participant 6)
Fellow Students (Participant 6)
forbid: [Participant 6] -> [hasAccess: [Law En

Answer: Q II.1a: Use of VT Search

attend: [Students at Virginia Tech] -> [Virginia T
Faculty at Virginia Tech
False
hasContent: [Information on Faculty, Staff, and S
hasOccured: [useTool: [searchFor: [Participant 6
hasOccurred: [useTool: [searchFor: [Participant
Information on Faculty, Staff, and Students at Vi
Participant 6
searchFor: [Participant 6] -> [Information on Fac
Staff at Virginia Tech
Students at Virginia Tech
True
useTool: [searchFor: [Participant 6] -> [Informat
Virginia Tech
VT Search
workAt: [Faculty at Virginia Tech] -> [Virginia Te
workAt: [Staff at Virginia Tech] -> [Virginia Tech

Have you ever used VT Search to search for information on faculty, staff, or students at Virginia T

Data Point: (7, 21) = No

Answer to: Q II.1a: Use of VT Search by: Participant 6

No

Description: search for information.

Domain: Participant 6

Range: Information on Faculty

Support:

Participant 6 - Q II.1a: Use of VT Search
Participant 6 - Q II.1b-2: Awareness of Searc

Figure 6.12: Chunking of Information in the Privacy Analyst's Work eNvironment (PAWN).

intensive process. One of the most challenging aspects of the modeling process is the fact that the analyst has almost infinite freedom in terms of modeling choices. This can be demonstrated quite simply with a sentence that is part of Question III.2a:

> "The participant talks to his/her parents about grades".

The problem, here, arises through the intransitive use of the verb 'talk'. Namely, we can remove parts of the above sentence in two different ways and still maintain a valid sentence. Thus, "The participant talks to his/her parents." as well as "The participant talks about grades." can both be represented as triads, with 'participant', 'parents', and 'grades' representing instances and 'talkTo' or 'talkAbout', respectively, representing relationships. However, combining the two sentence parts, we are left with two equivalent choices, shown in Figure 6.13. Similarly, the analyst has the choice of explicitly modeling the possessive pronouns ('his' or 'her'), or implicitly represent this relationship through naming of the instance ('parents of participant x').

Further challenges lie in the modeling of hypothetical situations, disjunctions, and negations. Thus,

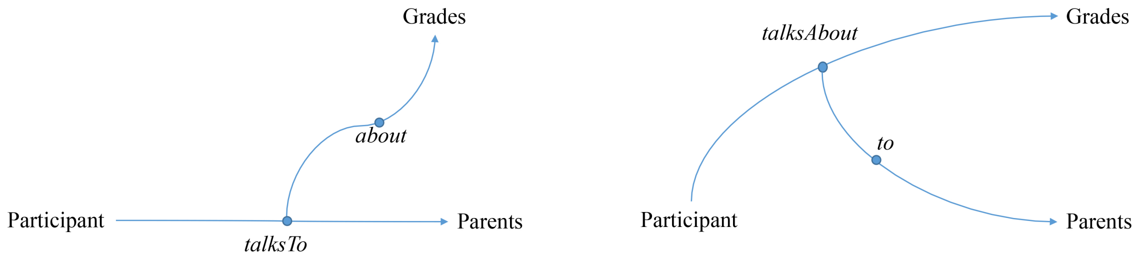


Figure 6.13: Equivalent Choices during Modeling.

modeling that VT Search *could* list a participant's mailing address requires either a convention of simply instantiating the relationship ('lists') and implying its hypothetical nature, use a separate notation for hypotheticals ('canList'), or even annotate the relationship with a meta attribute ('lists isHypothetical true'). Similarly, with the lack of disjunctions and enumerations on a language-level in the current version of PDML, the analyst could define and instantiate a relationship to represent this situation ('disjointWith'), or simply use naming conventions ('Everyone Else'). Finally, negations (or the absence of something) provide another challenge due to the open-world assumption implied in PDML. Thus, to negate an action or property, an analyst currently has to define specific negated versions of the action or property ('doesNotKnow') or use another meta attribute ('knows hasValue false').

The exact decision as to which approach to use to address each of the challenges is up to the analyst. The choices are *fully equivalent*, yet affect *query* of and *reasoning* about the data. Thus, the analyst needs to apply the approach chosen at modeling time consistently throughout the entire analysis process. In our encoding of responses, we strived to follow the structure of the data while preferring simpler variants over more complex ones. Thus, in the example presented in Figure 6.13, we used the first variant, since the flow of the sentence puts more emphasis on the parents than the grades. In the case of hypotheticals, we opted to imply the hypothetical nature of scenarios. This is the simplest choice and allows, if desired, to add annotations with meta attributes. Finally, we used naming conventions in case of negations (like 'Everyone Else'; cf. Appendix C).

As a result of these challenges, manual encoding of all remaining responses (not covered through template evaluation) can still take in excess of an hour. Furthermore, the analyst has to keep track of any decisions made regarding the conventions chosen, starting as early as during template creation. The latter factor is somewhat mitigated through the support of the process in PAWN, especially through the design of the encoding view. A side-effect of the fine granularity of the chunking used is an expansion of the data in terms of the number of assertions created. Thus, through template evaluation and chunking of five participants, the number of assertions reached 58,500 assertions. These assertions are supported through a total of 126,482 support statements backed by 14,748 supporting responses.

6.5.3 Open Coding to Generate Terms

One of the advantages of using PDML and PAWN for the domain modeling process reveals itself when one attempts the open coding of assertions to generate terms. Namely, despite the vast amount of assertions present in the knowledge base (either generated through template evaluation or encoded by the analyst), open coding of these assertions into terms is relatively simple. This has two reasons. First, by creating templates for the bracketing of assumptions the analyst implicitly identifies candidates for leaf terms. For example, by creating the 'hasAge' relationship template for Question I.1, in order to automatically generate appropriate relationships between the participant and his or her age, the analyst establishes a common *label* for this *category* of relationships. Thus, in this example, 'hasAge' can serve as a leaf role for all instantiated relationships with name 'hasAge'. Furthermore, while currently not implemented in PAWN, such relationship templates could be associated with roles in the knowledge base, as both relationship templates and roles are prototypes of relationship instances. Thus, the 'isA' relation could be automatically established during template evaluation.

Second, for manually created assertions, the necessity to abide by one's own conventions (as mentioned above) results in consistent naming and modeling of assertions. Given the same (or similar) names, these groups of assertions can be easily identified and an appropriate term created. Overall, this leads to a significant reduction of the number of terms compared to the number of assertions and oftentimes results in categories with a large amount of members in the terminology. In fact, the

58,384 categorized assertions are members of only 131 distinct terms. This relatively low number, furthermore, reflects the relatively high number of quantitative questions within our survey, as they explicitly define the terms being used. Moreover, at the time of writing, there are only five fully encoded participants. Given further encoding, it can be assumed that more terms will be added.

Provided the current state of the domain model, there are three venues of action the analyst can take. First, the analyst can continue to iterate over the chunking and open coding processes to complete the base layer of the domain model, followed by building the taxonomic hierarchy of terms through *axial coding* (i.e., iterate over Step (2) in Figure 3.3). Alternatively, the analyst can commence further in the design process and attempt to develop privacy requirements corresponding with the current state of the domain model (Step (3) in Figure 3.3). Finally, the analyst can commence with the evaluation of the current state of the domain model (Step (9) in Figure 3.3). We are going to do the latter of the three.

6.6 Evaluation of the Domain Model

As specified in Section 3.3.1, the evaluation of the domain model has two parts: *verification* of the *consistency* of the model as well as *validation* of its *completeness*. Had we not used PDML and PAWN, we would also have to establish or confirm the *traceability* of our encoding to the data source. However, traceability — as we have seen in Figures 6.10 and 6.12 — is achieved directly through architectural support within PAWN, which obviates this step.

6.6.1 Verification of Consistency

We have identified threats to the consistency of the domain model as *incompleteness*, *meaninglessness*, and *ambiguity*. Incompleteness refers to leaf terms without any support within the assertions. Assertions are deemed meaningless if they are not categorized. Finally, assertions are ambiguous if they are members of two or more different terms. The structure of knowledge bases in PDML combined with tools support through PAWN allows verification to be automated.

In our case, initial verification revealed three incomplete terms, 116 meaningless assertions, and no ambiguous or incomplete assertions. The meaningless assertions were simply a side-effect of incomplete encoding and have since been categorized. Once encoding is completed, however, no meaningless assertions should remain. Investigating the incomplete terms revealed three different causes for the incompleteness. The first term, the instance 'Authentication Strategy', was lacking support due to mis-classification of assertions. Namely, 'Per-Person Authentication' and 'Per-Group Authentication' (cf. Question III.6) were accidentally classified as 'Access Strategy'. The second term, the role 'hasFunctionality', could be matched to a meaningless relationship of the same name, linking the instance 'VT Search' to its functionality. Finally, the last term, namely the instance 'Information Source', has since been replaced by the instance 'Study Resource' and has therefore been removed. Correcting the above issues allows us to pass verification, and we can now move on to the validation of completeness.

6.6.2 Validation of Completeness

As we have discussed in Section 5.2, *conceptual saturation* is a prerequisite for *completeness*. Since open coding of the assertions is not yet complete, it is highly unlikely that this state has been achieved at this point in time. However, since all participants are at least partially encoded and a number of participants are fully encoded, we can nevertheless apply the information theoretical measures from Section 5.2.2 to our domain model. Should our predictions be correct, each partially encoded participant should be interpreted as non-contributor with respect to terms, and thus simulate achieving conceptual saturation, as no new terms are introduced starting with the first partially encoded participant. Furthermore, since PAWN provides an implementation for the calculation of the various forms of entropy, we have the opportunity to not only examine the entropy of the current state of the knowledge base, but rather calculate the values one participant at a time. The result of these calculations is shown in Figure 6.14.

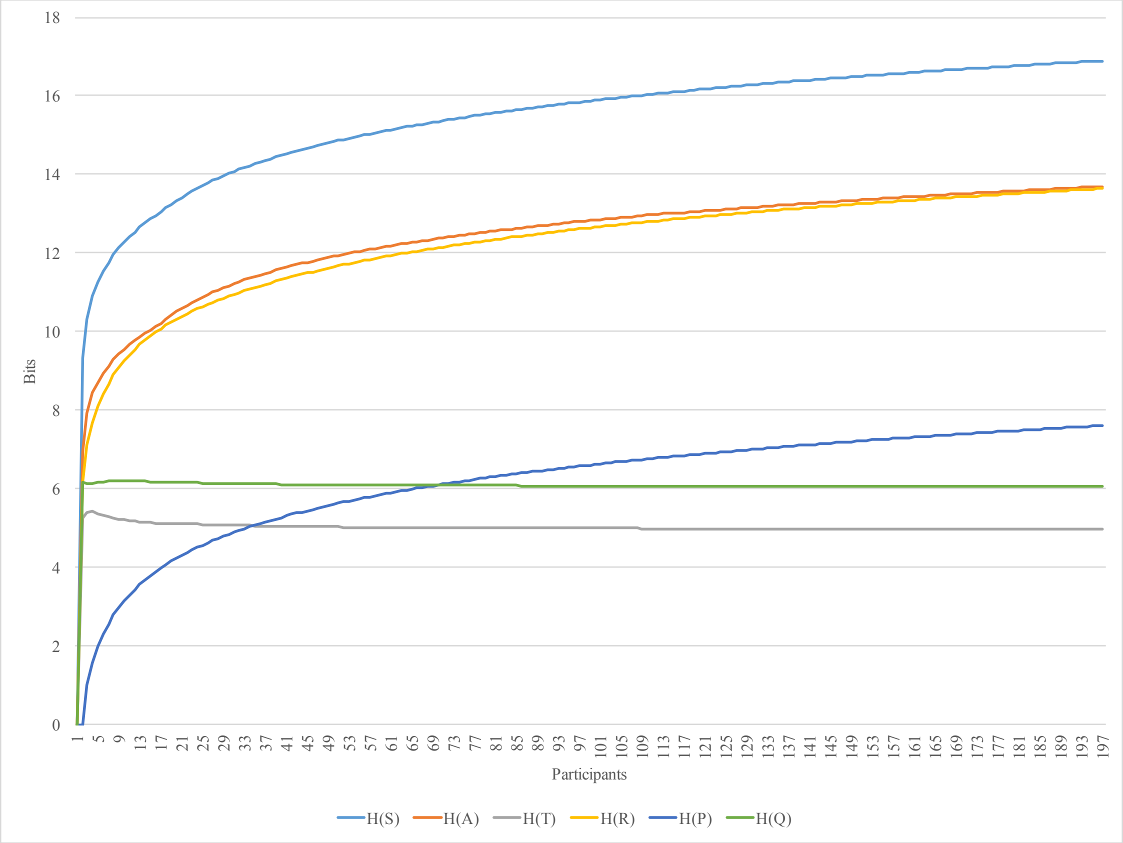


Figure 6.14: Support Entropy $H(S)$, Assertion Entropy $H(A)$, Term Entropy $H(T)$, Response Entropy $H(R)$, Participant Entropy $H(P)$, and Question Entropy $H(Q)$ over Time.

The chart shows that the predictions we made based on the growth of entropies of our example study (cf. Table 5.12) were, to a big part, accurate. However, it is worthwhile to examine and reflect on the graph of each of the various entropies. As discussed in Section 5.2.2, the entropy of the support set $H(S)$ shows the largest growth over time, reflecting the immense size of this set. It is worth noting that its value immediately jumps to 9.69 bits with the first participant (revealing the set to contain 827 support statements). Considering the relative simplicity of the assertions stemming from the demographic questions and other quantitative questions compared to the complexity found within the qualitative questions, it may be possible to take the size of the initial growth of this graph as an indicator for the 'depth' of the data collection instrument. Thus, we would expect a quantitative survey to yield a significantly lesser initial growth than an interview or a focus group.

Similarly, comparing the values of both response entropy $H(R)$ and assertion entropy $H(A)$ raises an interesting question. While both entropies, as predicted, exhibit consistent growth, their values are within 2 bits of each other (the assertion entropy being consistently higher, as expected). Thus, once again, the question is whether the relatively small difference between these two entropies is an indicator of limited depth of the responses. One would expect the difference to be larger, should the chunking of a response lead to a large number of assertions. Conversely, if the number of assertions generated through encoding is low, these values can be expected to be close together.

Examining the participant entropy $H(P)$ reveals the effect of the template-based generation of assertions combined with the lack of manual chunking. To be precise, the evaluation of templates for each participant results in the same number of assertions for each participant. This results in a close to uniform distribution of assertions supported by participants. Thus, the value of the participant entropy is virtually indistinguishable from the maximum entropy.

We did not directly make a prediction about the values of the question entropy $H(Q)$ when observing changes based on participants. However, examining the graph of this function reinforces the uniform nature of the template evaluation process. Namely, the same amount of assertions are introduced not only per participant, but rather also per question. Yet since we are only varying participants over time and not questions, the overall distribution of assertions per question does not change significantly. Ordering entropies based on the variation of questions, however, should reveal a curve similar to the one exhibited by the participant entropy. Moreover, the question entropy exhibits the steady decline we predicted of the term entropy once conceptual saturation is reached, as the term representing 'Human' increasingly dominates the distribution of assertions. Unfortunately, the decline of its value is immediate, thus making the question entropy useless to determine conceptual saturation.

Due to its importance for the prediction of conceptual saturation, Figure 6.15 provides a more detailed view of the values of the term entropy over time.

Recall our prediction regarding the term entropy $H(T)$ in Section 5.2.2. According to our reasoning, we expected the value of the term entropy to grow up until conceptual saturation was reached (i.e., no new terms were added to the knowledge base). After that point, we expected the value of

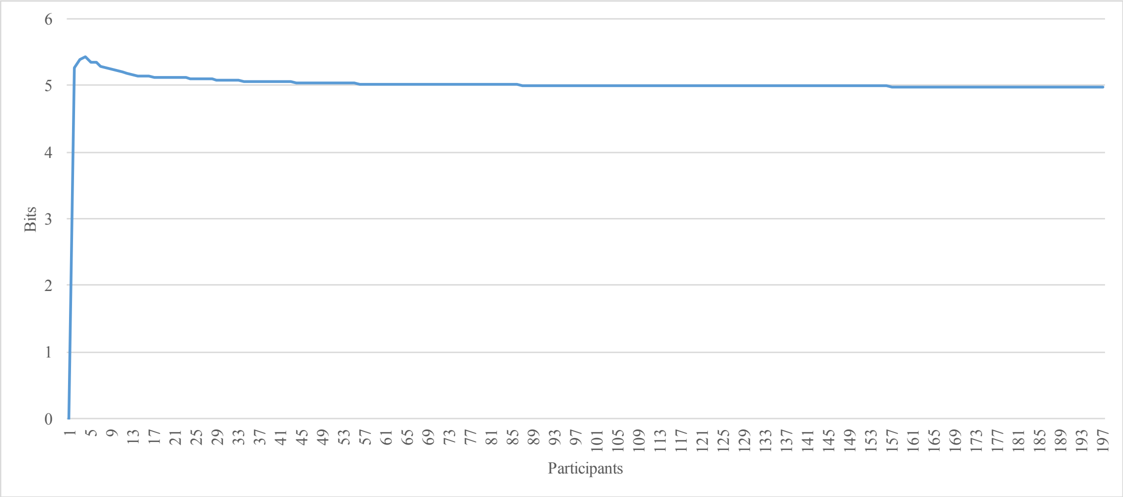


Figure 6.15: Term Entropy $H(T)$ over Time.

the entropy to stabilize around a value reflecting the actual distribution of the terms within the target population, eventually oscillating around that value. Finally, we predicted an eventual decline, as the probability of the term 'Human' begins to dominate the probability distribution.

Comparing these predictions with the graph in Figure 6.15 we can see that our predictions hold up within our domain model at this point. First, we can observe a strong initial growth of the entropy, followed by a brief period of continued growth. This part of the curve represents exactly the few fully encoded participants, revealing that each participant contributes additional terms to the knowledge base. Following these few participants, we can see a somewhat sharp decline in the entropy and its approximation of a value around 4.938 bits. This represents the adjustment of the probability distribution to the actual distribution of the phenomena within the population. In our case, this is achieved by the uniform addition of assertions through the evaluation of templates, essentially negating the individual contributions of the initial participants. Furthermore, close examination of the values reveals that, around participant 53, the value starts to oscillate around 4.938 bits, while still maintaining a slight downward trend. However, this comes with the added caveat that the differences between values are so small that they may be influenced by the precision and numerical stability of the underlying implementation.

This allows us to make the following observations. First (and not surprisingly), conceptual saturation is reached early on with the last fully-encoded participant. After that participant, the probability distribution starts initial oscillation at around participant 53, and reaches a fully stable probability distribution around participant 163. Taking into consideration the limited number of fully encoded results, we can nevertheless assert that employing the term entropy of the knowledge base as a basis for asserting conceptual saturation is indeed feasible. Realistically, however, this state is likely to be reached much later than participant 10. Moreover, term entropy offers the additional benefit of revealing when the probability distribution of the terms achieves its actual value within the population. We will refer to this as the *stability* of the entropy. As we have seen, full stability of the distribution can be reached significantly later than conceptual saturation. However, the large delay between conceptual saturation and distribution stability can be attributed to the large difference between fully and partially encoded responses. Namely, the fully encoded responses often add new terms to the support of the distribution, which are not supported by the partially encoded responses. Thus, the terms that are supported by automatically generated assertions eventually dominate the distribution, counteracting the increase of entropy by the few new terms supported by the fully encoded responses. Furthermore, considering how little the entropy values differ between participants past participant 53 (i.e., approximately 10^{-4}), a specific threshold value could be chosen to indicate sufficient stability of the entropy.

6.7 Further Steps

Once validation of the domain model is complete, the analyst, once again, has the choice between two courses of action. The first choice is continuing on to the formulation of privacy requirements (Step (3) in Figure 3.3). The second is sampling additional data to improve the coverage of the domain model (Step (10) in Figure 3.3). However, as these steps are not the focus of our evaluation, we will only cover each of the steps briefly.

6.7.1 Synthesizing Requirements

The synthesis of privacy requirements is the goal of the privacy design frameworks we reviewed in Section 1.3. Thus, we can show how our domain model provides the necessary domain knowledge to be able to address specific concerns of different frameworks. This demonstrates the integration of the PREprocess with existing practice, while the privacy design frameworks provide the analyst with guidance on how to synthesize requirements.

For example, the Privacy Engineering Guidelines [Spiekermann and Cranor 2009] provide different recommendations depending on the type of the system to (re-)design. In our case, since the users of our system are fully identified through their directory information, we are dealing with a system requiring *privacy-by-policy*. Thus, as the guidelines assign us with the responsibility of providing users with control over access to their data through *notice and choice* in order to minimize future privacy risks. However, to be able to do so, we need information on whether users fully understand how their data is currently used and controlled and what their expectations of privacy are. Additionally, the guidelines suggest either providing users with ad-hoc choices or allowing users to provide rules for their preferences as the mechanism for notice and choice, raising the question which method is appropriate in our case.

We can answer each of these questions by examining our domain model. As we have stated in Section 6.4.2, 37.24% of our participants were not aware of their data being available in VT Search. Furthermore, Figure 6.6 shows participants' expectation of privacy. Finally, Figure 6.9 reveals that providing ad-hoc choices is preferred by 61.22% of participants.

Similar to the Privacy Engineering Guidelines, the PriS Method [Kalloniatis et al. 2008] tasks analysts to identify the privacy goals of the users of the system. The method categorizes these goals into *authentication*, *authorization*, *identification*, *data protection*, *anonymity*, *pseudonymity*, *unlinkability*, and *unobservability*. Relevant for us are the first five categories. We have already covered the preferred authorization strategy based on questions raised by the Privacy Engineering Guidelines. For the remaining goals, we can once again retrieve our participants' preferences from our domain model. Figure 6.9 reveals that a hybrid authentication strategy is preferred over both per-person and per-group authentication. Identification and anonymity are not large concerns, as 94.39% of participants would leave their full name accessible (cf. Figure 6.6). In contrast, participants show very nuanced preferences regarding the protection of their information depending on different groups (cf. Figure 6.7).

These expressions of varying trust also factor into decisions required by the Quality-of-Service (QoS) approach of Chakraborty et al. [2011]. In addition, however, QoS relies on adapting *accuracy*, *precision*, *currency*, and *completeness* based on variations in trust. Figure 6.8 reveals our participants' preferences regarding the provided precision of address information based on varying groups. Furthermore, we can establish that a total of 69.39% of participants prefer providing only partial access to their education record (cf. Figure 6.9), varying both currency and completeness. Moreover, participants' responses to Questions III.3a, III.3b, and III.3c reveal varying circumstances in which participants' adjust the accuracy of information they disseminate (i.e., circumstances in which they may lie about their grades).

All these reflections, furthermore, can be interpreted as part of the *privacy risk analysis* of the Privacy Risk Model [Hong et al. 2004]. The elicited preferences, moreover, allow us to prioritize the different requirements mentioned above for *privacy risk management*. More so, the fact that the term entropy of our domain model stabilizes provides us with *confidence* that the preferences found in our data reflect the preferences of the population as a whole. Thus, we can define our priorities for the redesign of VT Search as follows:

Prioritized Requirements *(VT Search)*

Redesign should prioritize:

1. Change of default settings (supported by >90%; cf. Figure 6.6)
2. Adding support for groups (varying support; cf. Figure 6.7)

Similarly, the priorities for the redesign of Hokie Spa are given as:

Prioritized Requirements *(Hokie Spa)*

Redesign should prioritize (cf. Figure 6.9):

1. Adding support for case-by-case decisions (supported by 61.22%)
2. Adding support for finer-grained access (supported by 69.39%)
    1. per-semester access (supported by 40.82%)
    2. per-class access (supported by 17.35%)
    3. per-grade access (supported by 11.22%)
3. Adding support for groups (supported by 16.33%; 45.41% for hybrid)
4. Adding support for rule-based access control (supported by 11.22%)

Ideally, while these requirements can serve as basis for technical specifications and allow developers to start implementing features, the requirements should be fleshed out into *use cases* [McDonald 2015] or *scenarios* [Rosson and Carroll 2002]. However, examining our domain model reveals that we lack contextual information on how some of the strategies within our requirements would be used by our stakeholders. To acquire this information, we would need to sample additional data.

6.7.2 Sampling Additional Data

In general, there are two reasons for sampling additional data (Step (10) in Figure 3.3). As we have seen in the previous section, the first reason is the presence of *open questions* arising from the analysis of the data which our current collection of privacy-related information cannot answer. The second and more fundamental reason is having concerns regarding the *validity* of the collected data (or the data collection process in general). In the latter case, sampling additional data is only appropriate should it allow for the mitigation of perceived threats to validity. If previous data collection suffered from inherent flaws, that data — and any analysis artifact solely dependent on said data — would need to be discarded. As validity concerns are potentially more impactful than questions arising from the data, we will examine these concerns first.

Evaluating Validity Concerns

As we have seen in Section 2.2, validity with respect to data collection is commonly evaluated through examining *external* and *internal validity* (or, in other terms, measurement and causal validity as well as generalizability). In our case, this translates into the question whether our survey questions produced accurate measures and whether our results, as a whole, can be generalized from our sample to our target population.

The first part of the question is more difficult to answer than the second part, as it is in part subjective and, furthermore, reliant on the reactivity of the responses provided. Section 6.3.3 provides our reasoning that lead to the design of our survey questions, and the results we have discussed so far have to be interpreted in that context. Thus, the valuation of the measurement validity of our data collection instrument really hinges on the question of whether it produced descriptions of behavior that are consistent with the actual behavior of our target population (i.e., its *predictive validity*). This, however, can be interpreted as one of the 'open questions' arising from our data. We will address this issue along with the other open questions in the next section.

In terms of generalizability, our data (and thus our domain model and requirements) face two threats. First, our sample only covered a single stakeholder group: undergraduate students. Thus, it is impossible to claim that the requirements we have elicited so far are representative of the preferences of *all* stakeholders. This issue can be addressed by sampling other stakeholder groups. Second, while we can get a general notion about the preferences of undergraduate students, our sample is heavily skewed towards female participants. Thus, in order to have strong confidence in the generalizability, we would need to sample more male participants from the participant pool to either achieve parity or achieve the actual distribution of males versus females in the undergraduate population as a whole (i.e., using *quota sampling*). As an alternative, we could calculate the development of the term entropy over time based solely on the contributions of male participants to determine whether the entropy reaches conceptual saturation as well as stability[3]. Both threats, however, can — and should — be addressed through additional sampling, which is encouraged

[3] This functionality is not yet implemented in PAWN and will be added in a later release.

by the iterative structure of the PREprocess. This sampling could be done with either our current survey (cf. Appendix B) or through a different data collection instrument or methodology.

Addressing Open Questions

In contrast, addressing the open questions which arise from the analysis of our data cannot be achieved through our current survey. We can be confident of this fact, as we have shown that the term entropy achieves conceptual saturation and stability (cf. Figure 6.15). Thus, we have to perform the *theoretical sampling* of our population through a different data collection instrument or methodology. The choice of methodology, however, closely depends on the questions.

As we have discussed above, the first question that arises is motivated by concerns about the predictive validity of our data. However, simply asking whether our data predicts actual behavior is a very vague question. Furthermore, the question implies the need for the observation of stakeholders, which is both costly and heavily influenced by reactivity (cf. Table 2.3). Thus, it makes sense to narrow the scope of the question to not *if* stakeholders act in a certain way, but rather *under what circumstances* they act in a certain way.

Reflecting on the contents of the domain model allows us to come up with more concrete questions:

Open Questions

Questions arising from the data are:

- What motivates the high level of trust in job recruiters?
- What motivates distrust in instructors and TAs?
- What circumstances are implied in the displayed trust of law enforcement officials?
- Why are mailing addresses considered more sensitive than phone numbers?
- Under what circumstances are phone numbers or mailing addresses shared?
- What mechanisms are used to share phone numbers or mailing addresses?
- What circumstances lead to the use of per-group versus per-person authentication?
- What are examples of access rules for education records?

- Are there potential group-dynamics in sharing grades?
- Do group dynamics influence the likelihood of deception?

Answers to these questions would allow to address the concerns regarding the measurement validity of our data as well as provide sufficient information for use cases and scenarios. However, the questions also show the need for more depth than what could be reasonably expected from survey responses. Thus, our data collection needs are better addressed by an interview or focus group study. The choice between the methodologies largely depends on how much importance we assign to potential group dynamics. The ideal scenario would be a two-phase design: a focus group for collaboratively eliciting answers to the above questions as first phase and follow-up interviews with the individual participants of the groups to clarify or validate responses as second phase. Regardless of the actual choice, the design and application of the data collection strategy and the subsequent analysis of collected data would follow the same steps as our initial data collection and analysis.

6.8 Summary

At the beginning of this chapter, we set out to evaluate our Privacy Requirements Engineering process (PREprocess) and Privacy Domain Modeling Language (PDML) using the evaluation methodology described in Chapter 5 in order to provide support for Hypothesis 1. In that regard, we have determined that showing support for the **data collection**, **process**, **artifact**, and **representational requirements** provides sufficient evidence for bridging the gap between the complexity of privacy behavior and preferences on the one hand (cf. Q 1) and the concrete, structured domain knowledge required by privacy design frameworks on the other (cf. Q 2). Our evaluation centers around an application for the management of *directory information* (VT Search) and *education records* (HokieSpa) at Virginia Tech (cf. Section 6.2), which is heavily influenced by the Federal Education Rights and Privacy Act of 1974 (FERPA; cf. Section 6.1).

Based on this target application, we showed the development of a matching research design in

Section 6.3, showcasing how the PREprocess addresses the **data collection requirements**, allowing for the capture of the complexity of the privacy domain . We discussed the results of the data collection in Section 6.4. Consequently, in Section 6.5 we used PDML and the Privacy Analyst's Work eNvironment (PAWN) to create a domain model from the collected data. Furthermore, we demonstrated how creating **templates** allows for automation of parts of the chunking process (cf. Section 6.5.1). The templates also highlight the **expressiveness** of PDML, allowing to capture the complex semantic, temporal information within the privacy-related information (demonstrating its match with the **representational requirements**). In Sections 6.5.2 and 6.5.3 we show how chunking and open coding lead to **incremental structuring** of information. We demonstrated PAWN's support for **traceability** through linking assertions to points in the data and terms to their supporting assertions. This built-in traceability allows the automation of the **verification** process, as PAWN provides queries for incompleteness, meaninglessness, and ambiguity.

PAWN also allows to calculate all entropies discussed in Section 5.2.2 'over time' (i.e., as it develops participant by participant), automating the **validation** process. Figures 6.14 and 6.15, furthermore, confirm our predictions in Section 5.2.2 and show how the term entropy allows to identify both the moment of **conceptual saturation** and **stability**. Thus, applying term entropy to PDML domain models not only provides us with a measure of **completeness**, but even allows us to achieve **confidence** in the fact that adding more participants — barring outliers — will not significantly change the distribution of measured phenomena.

Finally, in Section 6.7 we have shown how the PREprocess seamlessly **integrates** with the privacy design frameworks discussed in Section 1.3, allowing to both synthesize and prioritize privacy requirements. Moreover, we demonstrated how the PREprocess encourages and guides the **iterative refinement** of the domain model through evaluating validity concerns and addressing open questions arising from the analysis (cf. Section 6.7.2). Thus, in conclusion, we have met each of our requirements, showing how the PREprocess, PDML, and PAWN provide an analyst with both the methodology and the tools to develop application-specific domain models that capture the contextual privacy preference and practice of the application's stakeholders.

Chapter 7

Conclusion

With every new wave of new innovations, information technology is changing the ways we live our lives, reshaping our everyday interactions as it permeates more and more aspects of our existence. These changes are not without growing pains, as we learn to adapt to the presence of a new, parallel, and intangible world of ever-present information. Part of these changes involve how we, as individuals and as a society, perceive and experience privacy. Thus, as we gain access to more and more information about the world around us, the world gains access to more and more information about ourselves — to an extent that some claim that expectations of confidentiality are a thing of the past [Hubaux and Juels 2016]. Still, there are pushes to counter the growing threat of pervasive surveillance, be it through 'the right to be forgotten' [European Parliament and Council of the European Union 2016] or the call for 'privacy by design' [Federal Trade Commission 2012]. This provides developers who wish to create 'privacy-aware' applications with the challenge of having to determine the requirements needed to support stakeholder privacy preference and practice with little tangible information about said preference and practice.

In this work, we have hypothesized that it is possible to leverage domain-knowledge and requirements gathering approaches to construct application-specific privacy domain models (Hypothesis 1). The initial challenge of this hypothesis arises from the complex nature of privacy (cf. Section 1.2): Every problem domain can potentially change the expression and perception of privacy (P 1).

In Chapter 2 we addressed the considerations that have to go into capturing this complex social behavior, eliciting a set of **data collection requirements**. Faced with the potentially large amount of unstructured, qualitative data (P 3) generated through data collection, we surveyed existing analysis approaches (cf. Section3.1) and extracted a set of **process** and **artifact requirements** a privacy data analysis process has to meet (cf. Section 3.2.3).

To address the procedural aspects of these requirements, we developed the Privacy Requirements Engineering process (PREprocess; cf. Figure 3.3) that provides an analyst with guidance in the development of application-specific privacy domain models. Such domain models need to take on a form that meets the artifact requirements (traceability, consistency, and completeness) and adequately captures the complexity of the captured data, while at the same time providing appropriate structure for the management of the model (P 4). Thus, we elicited a set of **representational requirements** for privacy domain models (cf. Chapter 4) and evaluated current representations based on these requirements (cf. Section 4.1). As none of the reviewed representations fully met our needs, we developed the Privacy Domain Modeling Language (PDML) (cf. Section 4.2).

Armed with the PREprocess and PDML, we set out to determine the methodology required to show that the resulting domain model would provide sufficiently concrete domain knowledge for the application of existing privacy design frameworks (P 2) — and thus, also show support for Hypothesis 1. As addressing each problem we faced led to specific requirements that allowed to address them, we determined that evaluation should focus on the **data collection**, **process**, **artifact**, and **representational requirements** (cf. Chapter 5). During the evaluation, specific care needs to be taken in the **verification of consistency** and **validation of completeness** of the domain model created. Thus, we adopted the metrics of *incompleteness*, *meaninglessness*, and *ambiguity* for the evaluation of model consistency (cf. Section 5.1). Furthermore, we showed how the information theoretical concept of **entropy** can be applied to PDML domain models to not only demonstrate **conceptual saturation**, but also to gauge the **stability** of the underlying distribution of phenomena within the model (cf. Section 5.2). Finally, in Chapter 6, we systematically demonstrate how the PREprocess and PDML, with the tool support of the Privacy Analyst's Work eNvironment (PAWN) fulfills each evaluation criterion, and allows seamless integration with existing practice.

7.1 Contributions

This research has provided several valuable contributions to the research community. First, this work features a thorough evaluation of both motivations for and expressions of privacy behavior (cf. Section 1.2) and the resulting challenges for the design of privacy-aware applications (cf. Section 1.3.1). Furthermore, we provide a detailed analysis of the considerations an analyst has to address when attempting to capture the complexity of privacy behavior within a given domain (cf. Chapter 2), developing a set of succinct requirements for data collection and highlighting the trade-offs involved in such a process.

Moreover, we have designed the Privacy Requirements Engineering process (PREprocess; cf. Section 3.3) that provides an analyst with guidance in the development of application-specific privacy domain models. The PREprocess leverages existing best practice from qualitative data analysis and software engineering, providing the scaffolding required for repeatable results. Moreover, through the incorporation of verification, validation, traceability, and validity evaluation, the process allows for the assessment and justification of outcomes. Furthermore, the PREprocess is tailored to seamlessly integrate with existing engineering and analysis processes, lowering the threshold for its adoption into practice.

A further contribution of this work is the Privacy Domain Modeling Language (PDML; cf. Section 4.2). The key aspect of PDML is its expressivity, allowing it to represent complex semantic contexts as well as intricate temporal relationships — even in the case of missing or incomplete information. This makes it singularly suitable to represent privacy-related information. However, its expressivity is not specific to the privacy domain, and thus its use may benefit other domains with similar representational requirements.

Tying into the value of PDML is our systematic evaluation of the applicability of entropy to establish conceptual saturation of PDML domain models in Section 5.2. Besides providing a quantitative metric for completeness, observing the term entropy over time furthermore allows to determine the point in time at which the distribution of the concepts represented in the model reaches *sta-*

bility. Thus, it provides a quantitative measure of *confidence* in the accuracy of the data and the representativeness of the concepts within the model. Furthermore, entropy and related information theoretical measures may allow to identify outliers in the data as well as provide evidence for the validity of the data based on only parts of the sampled data.

Finally, with the Privacy Analyst's Work eNvironment (PAWN), we have contributed a powerful open-source data analysis platform to the set of tools available to the research community (available for download at https://bitbucket.org/aftenkap/pawn). Not only does PAWN provide invaluable support in the application of the PREprocess and the creation of PDML domain models, it also allows the automation of parts of the process, reducing the amount of work required of the analyst. Furthermore, it provides built-in support for the traceability of information across different levels of abstraction and for the calculation of entropies. PAWN also addresses the data management needs of analysis processes and can serve as repository of organizational memory.

7.2 Remaining Challenges

Unfortunately, despite our contributions, one of the primary challenges that Shapiro [2010] identifies for the design of privacy-aware technology remains. Namely, while providing a lot of guidance, successfully applying the PREprocess still requires a large amount of expertise. As mentioned in Chapter 2, the determining the appropriate sampling method and data collection strategy, designing good data collection instruments, and applying data collection methods correctly requires a significant amount of training. Furthermore, distinguishing relevant patterns within the data from 'noise', as well as creating and maintaining an adequate encoding convention require both practice in modeling and knowledge of the privacy field. However, these requirements are already met by members of many User Experience teams, namely *User Researchers*.

A similar remaining challenge is the significant amount of time that the process requires. As mentioned in Section 6.5.2, the manual chunking of assertions on a sub-sentence takes between four and six hours per participant. This establishes a relatively high threshold for the adoption of the PREprocess, especially in the context of agile software development — at least at a very fine granularity of chunking.

While this issue can be addressed through adding more analysts to the team, multiple analysts lead to separate issues. Namely, while analysts can tackle the modeling task in parallel, the flexibility of modeling in PDML is likely to yield different modeling choices by different analysts (cf. Figure 6.13). Thus, additional time needs to be invested in either developing a common modeling convention, or aligning the conflicting parts of the domain model into a consistent whole.

7.3 Future Work

Many of the remaining challenges can be addressed through future work. For example, the large amount of time required by the PREprocess indicates the need for further automation of parts of the process. As we have seen in Section 6.5.1, creating templates of the questions allows for the automation of parts of the chunking. Reflecting on the template in Figure 6.11 in combination with the need for conventions mentioned before reveals a possible venue of additional automation. Namely, we plan to investigate whether **Natural Language Processing** can be used to automate chunking of assertions based on the decomposition of sentences based on their function. A similar approach for the generation of access control policies has been developed by Slankas and Williams [2013].

Furthermore, as PDML is based on an extension of Description Logics with temporal properties and the expansion of predicates of arbitrary length, we intend to explore the the possibility of logical **reasoning**. Automated reasoning may allow to automatically identify modeling mismatches between different analysts, as well as the automatic classification of assertions. It would, furthermore, provide an additional means of verifying the consistency of the domain model. Moreover, we will examine whether extending PDML with additional concepts from description logics, such as *cardinality restrictions*, *enumerated terms*, etc. would increase its value.

As the PDML domain models are meant to serve as organizational memory, such domain models would see significant growth over the lifetime of a project. This may lead to a model size that does not yield itself to exploration through querying an opaque database. Thus, the **visualization** of the semantic temporal networks would allow analysts to visually explore the domain models. We therefore plan to integrate the visualization capabilities of the Open Semantic Network Analysis Platform (OSNAP; [Radics et al. 2015]) into PAWN.

Finally, as the utility of PDML is not bound strictly to the privacy domain, we intend to examine whether other domains may benefit from its expressivity. Moreover, we plan on evaluating whether the conceptual saturation and stability of domain models in such domains can also be determined through a notion of entropy.

Bibliography

20 U.S. Code §1232g. 1974. Family educational and privacy rights. (February 1974). Retrieved July 07, 2016 from http://uscode.house.gov/browse/prelim@title20/chapter31/subchapter3/part4&edition=prelim

Mark S. Ackerman. 2000. The Intellectual Challenge of CSCW: The Gap Between Social Requirements and Technical Feasibility. *Human-Computer Interaction* 15, 2 (June 2000), 179–203. DOI:http://dx.doi.org/10.1207/S15327051HCI1523_5

Alessandro Acquisti and Jens Grossklags. 2004. Privacy Attitudes and Privacy Behavior. In *Economics of Information Security*, L. Jean Camp and Stephen Lewis (Eds.). Advances in Information Security, Vol. 12. Springer US, Boston, MA, 165–178. DOI:http://dx.doi.org/10.1007/1-4020-8090-5_13

Ryan Aipperspach, Ben Hooker, and Allison Woodruff. 2009. The Heterogeneous Home. *interactions* 16, 1 (January 2009), 35–38. DOI:http://dx.doi.org/10.1145/1456202.1456211

James F. Allen. 1983. Maintaining Knowledge about Temporal Intervals. *Commun. ACM* 26, 11 (November 1983), 832–843. Issue 11. DOI:http://dx.doi.org/10.1145/182.358434

Irwin Altman. 1975. *Environment and Social Behaviour* (1st ed.). Brooks/Cole Publishing Co., Monterey, CA.

Abdullahi Arabo, Ian Brown, and Fadi El-Moussa. 2012. Privacy in the Age of Mobility and Smart Devices in Smart Homes. In *Proceedings of the 2012 ASE/IEEE International*

Conference on Privacy, Security, Risk and Trust and 2012 ASE/IEEE International Conference on Social Computing (PASSAT/SocialCom '12). IEEE, Piscataway, NJ, USA, 819–826. DOI: http://dx.doi.org/10.1109/SocialCom-PASSAT.2012.108

Alessandro Artale and Enrico Franconi. 2000. A Survey of Temporal Extensions of Description Logics. *Annals of Mathematics and Artificial Intelligence (AMAI)* 30, 1 (June 2000), 171–210. DOI: http://dx.doi.org/10.1023/A:1016636131405

Judy Attfield. 1999. Bringing Modernity Home: Open Plan in the British Domestic Interior. In *At Home: An Anthropology of Domestic Space* (1st ed.), Irene Cieraad (Ed.). Syracuse University Press, Syracuse, NY, Chapter 6, 73–82.

Prashanth Ayyavu and Carlos Jensen. 2011. Integrating User Feedback with Heuristic Security and Privacy Management Systems. In *Proceedings of the 2011 Annual Conference on Human Factors in Computing Systems (CHI '11)*. ACM, New York, NY, USA, 2305–2314. DOI: http://dx.doi.org/10.1145/1978942.1979281

Franz Baader and Werner Nutt. 2003. Basic Description Logics. In *The Description Logic Handbook: Theory, Implementation, and Applications* (1st ed.), Franz Baader, Diego Calvanese, Deborah L. McGuinness, Daniele Nardi, and Peter Patel-Schneider (Eds.). Cambridge University Press, New York, NY, USA, Chapter 2, 47–100.

Aubrey Baker, Laurian Vega, Tom DeHart, and Steve Harrison. 2011. Medical Record Privacy: Is It a Facade?. In *CHI '11 Extended Abstracts on Human Factors in Computing Systems (CHI EA '11)*. ACM, New York, NY, USA, 2203–2208. DOI: http://dx.doi.org/10.1145/1979742.1979918

Ayan Banerjee and Sandeep K. S. Gupta. 2012. Your Mobility Can Be Injurious to Your Health: Analyzing Pervasive Health Monitoring Systems under Dynamic Context Changes. In *Proceedings of the 2012 IEEE International Conference on Pervasive Computing and Communications (PerCom '12)*. IEEE, Piscataway, NJ, USA, 39–47. DOI: http://dx.doi.org/10.1109/PerCom.2012.6199847

Kristian Beckers. 2012. Comparing Privacy Requirements Engineering Approaches. In *Proceedings of the 2012 Seventh International Conference on Availability, Reliability and Security (ARES '12)*. IEEE, Piscataway, NJ, USA, 574–581. DOI: http://dx.doi.org/10.1109/ARES.2012.29

Jacob A. Benfield. 2009. *Longitudinal assessment of privacy and territory establishment in a college residence hall setting*. Ph.D. dissertation. Colorado State University, Fort Collins, CO.

Bettina Berendt, Oliver Günther, and Sarah Spiekermann. 2005. Privacy in E-Commerce: Stated Preferences vs. Actual Behavior. *Commun. ACM* 48, 4 (April 2005), 101–106. DOI: http://dx.doi.org/10.1145/1053291.1053295

Regina Bernhaupt, Marianna Obrist, Astrid Weiss, Elke Beck, and Manfred Tscheligi. 2008. Trends in the living room and beyond: results from ethnographic studies using creative and playful probing. *ACM Computers in Entertainment* 6, 1, Article 5 (May 2008), 23 pages. Issue 1. DOI: http://dx.doi.org/10.1145/1350843.1350848

Giulia Biamino. 2011. Modeling Social Contexts for Pervasive Computing Environments. In *Proceedings of the 2011 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Wksp '11)*. IEEE, Piscataway, NJ, USA, 415–420. DOI: http://dx.doi.org/10.1109/PERCOMW.2011.5766925

Dines Bjørner. 2006. *Software Engineering 3: Domains, Requirements, and Software Design*. Springer, Berlin Heidelberg. DOI: http://dx.doi.org/10.1007/3-540-33653-2

Jan Oliver Borchers. 2000. A Pattern Approach to Interaction Design. In *Proceedings of the 3rd Conference on Designing Interactive Systems (DIS '00)*. ACM, New York, NY, USA, 369–378. DOI: http://dx.doi.org/10.1145/347642.347795

Jennifer K. Bosson, Jennifer L. Prewitt-Freilino, and Jenel N. Taylor. 2005. Role Rigidity: A Problem of Identity Misclassification? *Journal of Personality and Social Psychology* 89, 4 (October 2005), 552–565. http://dx.doi.org/10.1037/0022-3514.89.4.552

Ronald J. Brachman and James G. Schmolze. 1985. An Overview of the KL-ONE Knowledge Representation System. *Cognitive Science* 9, 2 (April 1985), 171–216. DOI:http://dx.doi.org/10.1207/s15516709cog0902_1

A.J. Bernheim Brush, Bongshin Lee, Ratul Mahajan, Sharad Agarwal, Stefan Saroiu, and Colin Dixon. 2011. Home Automation in the Wild: Challenges and Opportunities. In *Proceedings of the 2011 Annual Conference on Human Factors in Computing Systems (CHI '11)*. ACM, New York, NY, USA, 2115–2124. DOI:http://dx.doi.org/10.1145/1978942.1979249

Akiko Busch. 1999. *Geography of Home: Writings on Where We Live* (1st ed.). Princeton Architectural Press, New York, NY, USA.

Anne Buttimer and David Seamon (Eds.). 1980. *The Human Experience of Space and Place*. Croom Helm, London, UK.

Kelly E. Caine, Arthur D. Fisk, and Wendy A. Rogers. 2006a. Benefits and Privacy Concerns of a Home Equipped with a Visual Sensing System: Perspective from Older Adults. In *Proceedings of the Human Factors and Ergonomics Society 50th Annual Meeting*, Vol. 50. Sage Publications, Inc., Thousand Oaks, CA, USA, 180–184. DOI:http://dx.doi.org/10.1177/154193120605000203

Kelly E. Caine, Marita A. O'Brien, Sung Park, Wendy A. Rogers, Arthur D. Fisk, Koert Van Ittersum, Muge Capar, and Leonard J. Parsons. 2006b. Understanding Acceptance of High Technology Products: 50 Years of Research. In *Proceedings of the Human Factors and Ergonomics Society 50th Annual Meeting*, Vol. 50. Sage Publications, Inc., Thousand Oaks, CA, USA, 2148–2152. DOI:http://dx.doi.org/10.1177/154193120605001807

Donald T. Campbell. 1957. Factors relevant to the validity of experiments in social settings. *Psychological Bulletin* 54, 4 (July 1957), 297–312. DOI:http://dx.doi.org/10.1037/h0040950

Supriyo Chakraborty, Haksoo Choi, and Mani B. Srivastava. 2011. Demystifying Privacy in Sensory Data: A QoI Based Approach. In *Proceedings of the 2011 IEEE International Conference* *on Pervasive Computing and Communications Workshops (PerCom Wksp '11)*. IEEE, Piscataway, NJ, USA, 38–43. DOI: http://dx.doi.org/10.1109/PERCOMW.2011.5766914

Suranjan Chakraborty, Christoph Rosenkranz, and Josh Dehlinger. 2015. Getting to the Shalls: Facilitating Sensemaking in Requirements Engineering. *ACM Transactions on Management Information Systems* 5, 3, Article 14 (January 2015), 30 pages. DOI: http://dx.doi.org/10.1145/2629351

Sophie Chevalier. 1999. The French Two-Home Project: Materialization of Family Identity. In *At Home: An Anthropology of Domestic Space* (1st ed.), Irene Cieraad (Ed.). Syracuse University Press, Syracuse, NY, Chapter 7, 83–94.

Eun Kyoung Choe, Sunny Consolvo, Jaeyeon Jung, Beverly Harrison, and Julie A. Kientz. 2011. Living in a Glass House: A Survey of Private Moments in the Home. In *Proceedings of the 13th International Conference on Ubiquitous Computing (UbiComp '11)*. ACM, New York, NY, USA, 41–44. DOI: http://dx.doi.org/10.1145/2030112.2030118

Eun Kyoung Choe, Sunny Consolvo, Jaeyeon Jung, Beverly Harrison, Shwetak N. Patel, and Julie A. Kientz. 2012. Investigating receptiveness to sensing and inference in the home using sensor proxies. In *Proceedings of the 2012 ACM Conference on Ubiquitous Computing (UbiComp '12)*. ACM, New York, NY, USA, 61–70. DOI: http://dx.doi.org/10.1145/2370216.2370226

Delphine Christin, Christian Roßkopf, Matthias Hollick, Leonardo A. Martucci, and Salil S. Kanhere. 2012b. IncogniSense: An Anonymity-Preserving Reputation Framework for Participatory Sensing Applications. In *Proceedings of the 2012 IEEE International Conference on Pervasive Computing and Communications (PerCom '12)*. IEEE, Piscataway, NJ, USA, 135–143. DOI: http://dx.doi.org/10.1109/PerCom.2012.6199860

Nicolas Christin, Serge Egelman, Timothy Vidas, and Jens Grossklags. 2012a. It's All About The Benjamins: An Empirical Study on Incentivizing Users to Ignore Security Advice. In *Financial Cryptography and Data Security: 15th International Conference, FC 2011 (Lecture Notes* *in Computer Science)*, George Danezis (Ed.), Vol. 7035. Springer, Berlin, Heidelberg, 16–30. DOI: http://dx.doi.org/10.1007/978-3-642-27576-0_2

Irene Cieraad. 1999. Introduction: Anthropology at Home. In *At Home: An Anthropology of Domestic Space* (1st ed.), Irene Cieraad (Ed.). Syracuse University Press, Syracuse, NY, Chapter 1, 1–12.

Sherley Codio, Dennis Kafura, Manuel Pérez-Quiñones, Andrea Kavanaugh, and Denis Gračanin. 2012. Identifying Critical Factors of Community Privacy. In *Proceedings of the 2012 ASE/IEEE International Conference on Privacy, Security, Risk and Trust and 2012 ASE/IEEE International Conference on Social Computing (PASSAT/SocialCom '12)*. IEEE, Piscataway, NJ, USA, 666–675. DOI: http://dx.doi.org/10.1109/SocialCom-PASSAT.2012.74

Amanda Coffey. 2014. Analysing Documents. In *The SAGE Handbook of Qualitative Data Analysis* (1st ed.), Uwe Flick (Ed.). SAGE Publications Ltd, Thousand Oaks, CA, USA, Chapter 25, 367–380. DOI: http://dx.doi.org/10.4135/9781446282243

Pietro Colombo and Elena Ferrari. 2012. Towards a Modeling and Analysis Framework for Privacy-Aware Systems. In *Proceedings of the 2012 ASE/IEEE International Conference on Privacy, Security, Risk and Trust and 2012 ASE/IEEE International Conference on Social Computing (PASSAT/SocialCom '12)*. IEEE, Piscataway, NJ, USA, 81–90. DOI: http://dx.doi.org/10.1109/SocialCom-PASSAT.2012.12

Juliet M. Corbin and Anselm L. Strauss. 2008. *Basics of Qualitative Research: Techniques and Procedures for Developing Frounded Theory* (3rd ed.). Sage Publications, Inc., Thousand Oaks, CA, USA. DOI: http://dx.doi.org/10.4135/9781452230153

Imelda T. Coyne. 1997. Sampling in qualitative research. Purposeful and theoretical sampling; merging or clear boundaries? *Journal of Advanced Nursing* 26, 3 (September 1997), 623–630. DOI: http://dx.doi.org/10.1046/j.1365-2648.1997.t01-25-00999.x

Andy Crabtree, Terry Hemmings, and Tom Rodden. 2002. Pattern-Based Support for Interactive Design in Domestic Settings. In *Proceedings of the 4th conference on Designing interactive* *systems: processes, practices, methods, and techniques (DIS '02)*. ACM, New York, NY, USA, 265–276. DOI:http://dx.doi.org/10.1145/778712.778749

Andy Crabtree and Tom Rodden. 2004. Domestic Routines and Design for the Home. *Computer Supported Cooperative Work (CSCW)* 13, 2 (April 2004), 191–220. DOI:http://dx.doi.org/10.1023/B:COSU.0000045712.26840.a4

Emiliano De Cristofaro, Anthony Durussel, and Imad Aad. 2011. Reclaiming Privacy for Smartphone Applications. In *Proceedings of the 2011 IEEE International Conference on Pervasive Computing and Communications (PerCom '11)*. IEEE, Piscataway, NJ, USA, 84–92. DOI:http://dx.doi.org/10.1109/PERCOM.2011.5767598

Tom DeHart. 2013. *Design and Usability Evaluation of a Community Enabled Email System*. Master's Thesis. Virginia Tech, Blacksburg, VA, USA.

Mina Deng, Kim Wuyts, Riccardo Scandariato, Bart Preneel, and Wouter Joosen. 2011. A Privacy Threat Analysis Framework: Supporting the Elicitation and Fulfillment of Privacy Requirements. *Requirements Engineering* 16, 1 (March 2011), 3–32. DOI:http://dx.doi.org/10.1007/s00766-010-0115-7

Paul Dourish. 2006. Implications for design. In *Proceedings of the 2006 SIGCHI Conference on Human Factors in Computing Systems (CHI '06)*. ACM, New York, NY, USA, 541–550. DOI:http://dx.doi.org/10.1145/1124772.1124855

John Duncan, L. Jean Camp, and William R. Hazelwood. 2009. The Portal Monitor: A Privacy-Enhanced Event-Driven System for Elder Care. In *Proceedings of the 4th International Conference on Persuasive Technology (Persuasive '09)*. ACM, New York, NY, USA, Article 36, 9 pages. DOI:http://dx.doi.org/10.1145/1541948.1541995

Ellucian. 2016. Student Information System for Higher Education: Banner by Ellucian. (July 2016). Retrieved July 07, 2016 from http://www.ellucian.com/student-information-system/

Markus Endler, Alexandre Skyrme, Daniel Schuster, and Thomas Springer. 2011. Defining Situated Social Context for pervasive social computing. In *Proceedings of the 2011 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Wksp '11)*. IEEE, Piscataway, NJ, USA, 519–524. DOI: http://dx.doi.org/10.1109/PERCOMW.2011.5766945

European Parliament and Council of the European Union. 2016. Regulation (EU) 2016/679: General Data Protection Regulation. *Official Journal of the European Union* 59, L119 (April 2016), 1–88. http://eur-lex.europa.eu/eli/reg/2016/679/oj

Michael W. Eysenck and Mark T. Keane. 2010. *Cognitive Psychology: A Student's Handbook* (6th ed.). Psychology Press, New York, NY, USA.

Véronique Faucounau, Ya-Huei Wu, Mélodie Boulay, Marina Maestrutti, and Anne-Sophie Rigaud. 2009. Caregivers' Requirements for In-Home Robotic Agent for Supporting Community-Living Elderly Subjects with Cognitive Impairment. *Technology and Health Care* 17, 1 (January 2009), 33–40. Issue 1. DOI: http://dx.doi.org/10.3233/THC-2009-0537

Federal Trade Commission. 2000. *Privacy Online: Fair Information Practices in the Electronic Marketplace*. Report to Congress. Federal Trade Commission, Washington, D.C., USA. Retrieved February 04, 2016 from https://www.ftc.gov/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission

Federal Trade Commission. 2012. *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*. Federal Trade Commission, Washington, D.C., USA. Retrieved February 04, 2016 from http://ftc.gov/os/2012/03/120326privacyreport.pdf

David M. Fetterman. 2009. Ethnography. In *The SAGE Handbook of Applied Social Research Methods* (1st ed.), Leonard Bickman and Debra J. Rog (Eds.). SAGE Publications, Inc., Thousand Oaks, CA, USA, Chapter 17, 543–589. DOI: http://dx.doi.org/10.4135/9781483348858

Uwe Flick. 2014. Mapping the Field. In *The SAGE Handbook of Qualitative Data Analysis* (1st ed.), Uwe Flick (Ed.). SAGE Publications Ltd, Thousand Oaks, CA, USA, Chapter 1, 3–19. DOI:http://dx.doi.org/10.4135/9781446282243

Uwe Flick (Ed.). 2014. *The SAGE Handbook of Qualitative Data Analysis* (1st ed.). SAGE Publications Ltd, Thousand Oaks, CA, USA. DOI:http://dx.doi.org/10.4135/9781446282243

Martin Fowler. 2002. *Patterns of Enterprise Application Architecture* (1st ed.). Addison-Wesley Professional, Upper Saddle River, NJ, USA.

Christian Freksa. 1992. Temporal Reasoning Based on Semi-Intervals. *Artificial Intelligence* 54, 1-2 (March 1992), 199–227. DOI:http://dx.doi.org/10.1016/0004-3702(92)90090-K

Erich Gamma, Richard Helm, Ralph Johnson, and John M. Vlissides. 1994. *Design Patterns: Elements of Reusable Object-Oriented Software* (1st ed.). Addison-Wesley Professional, Upper Saddle River, NJ, USA.

Katrin Gaßner and Michael Conrad. 2010. *ICT Enabled Independent Living for Elderly: A Status-Quo Analysis on Products and the Research Landscape in the Field of Ambient Assisted Living (AAL) in EU-27.* Institute for Innovation and Technology, Berlin, Germany. http://www.vdivde-it.de/publications/studies/

Alastair J. Gill, Asimina Vasalou, Chrysanthi Papoutsi, and Adam N. Joinson. 2011. Privacy Dictionary: A Linguistic Taxonomy of Privacy for Content Analysis. In *Proceedings of the 2011 Annual Conference on Human Factors in Computing Systems (CHI '11).* ACM, New York, NY, USA, 3227–3236. DOI:http://dx.doi.org/10.1145/1978942.1979421

Leah Glass and Robin Gresko. 2012. Legislation and Privacy Across Borders. In *Proceedings of the 2012 ASE/IEEE International Conference on Privacy, Security, Risk and Trust and 2012 ASE/IEEE International Conference on Social ComputingInternational Conference on Privacy, Security, Risk and Trust (PASSAT) and 2012 International Confernece on Social Computing (SocialCom) (PASSAT/SocialCom '12).* IEEE, Piscataway, NJ, USA, 807–808. DOI:http://dx.doi.org/10.1109/SocialCom-PASSAT.2012.135

Denis Gračanin, D. Scott McCrickard, Arthur Billingsley, Roosevelt Cooper, Tavon Gatling, Erik J. Irvin-Williams, Felicia Osborne, and Felicia Doswell. 2011. Mobile Interfaces for Better Living: Supporting Awareness in a Smart Home Environment. In *Proceedings of the HCI International 2011: Universal Access in Human-Computer Interaction: Context Diversity (Lecture Notes in Computer Science)*, Constantine Stephanidis (Ed.), Vol. 6767. Springer, Berlin, Heidelberg, 163–172. DOI:http://dx.doi.org/10.1007/978-3-642-21666-4_19

Glenn Greenwald. 2013a. Boundless Informant: the NSA's secret tool to track global surveillance data. The Guardian. (June 2013). Retrieved February 04, 2016 from http://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining

Glenn Greenwald. 2013b. NSA Prism program taps in to user data of Apple, Google and others. The Guardian. (June 2013). Retrieved February 04, 2016 from http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

Michael M. Groat, Benjamin Edwards, James Horey, Wenbo He, and Stephanie Forrest. 2012. Enhancing Privacy in Participatory Sensing Applications with Multidimensional Data. In *Proceedings of the 2012 IEEE International Conference on Pervasive Computing and Communications (PerCom '12)*. IEEE, Piscataway, NJ, USA, 144–152. DOI:http://dx.doi.org/10.1109/PerCom.2012.6199861

Jaber F. Gubrium and James A. Holstein. 2014. Analytic Inspiration in Ethnographic Fieldwork. In *The SAGE Handbook of Qualitative Data Analysis* (1st ed.), Uwe Flick (Ed.). SAGE Publications Ltd, Thousand Oaks, CA, USA, Chapter 3, 35–49. DOI:http://dx.doi.org/10.4135/9781446282243

Antal Haans, Florian G. Kaiser, and Yvonne A. W. de Kort. 2007. Privacy Needs in Office Environments: Development of Two Behavior-Based Scales. *European Psychologist* 12, 2 (July 2007), 93–102. DOI:http://dx.doi.org/10.1027/1016-9040.12.2.93

Martyn Hammersley. 2008. Assessing Validity in Social Research. In *The SAGE Handbook of Social Research Methods* (1st ed.), Julia Brannen Pertti Alasuutari, Leonard Bickman (Ed.). SAGE Publications Ltd., Thousand Oaks, CA, USA, Chapter 4, 42–54. DOI:http://dx.doi.org/10.4135/9781848608429

Earl Harris, Jr. 2001. *Information Gain Versus Gain Ratio: A Study of Split Method Biases*. Technical paper. The MITRE Corporation, McLean, VA, USA.

Chris Harrison, Jason Wiese, and Anind K. Dey. 2010. Achieving Ubiquity: The New Third Wave. *IEEE Multimedia* 17, 3 (July 2010), 8–12. DOI:http://dx.doi.org/10.1109/MMUL.2010.53

Steve Harrison and Paul Dourish. 1996. Re-Place-ing Space: The Roles of Place and Space in Collaborative Systems. In *Proceedings of the 1996 ACM Conference on Computer Supported Cooperative Work (CSCW '96)*. ACM, New York, NY, USA, 67–76. DOI:http://dx.doi.org/10.1145/240080.240193

Steve Harrison and Deborah Tatar. 2008. Places: People, Events, Loci – The Relation of Semantic Frames in the Construction of Place. *Computer Supported Cooperative Work (CSCW)* 17, 2 (April 2008), 97–133. DOI:http://dx.doi.org/10.1007/s10606-007-9073-0

Ralph Vinton Lyon Hartley. 1928. Transmission of Information. *The Bell System Technical Journal* 7, 3 (July 1928), 535–563. DOI:http://dx.doi.org/10.1002/j.1538-7305.1928.tb01236.x

Rex Hartson and Partha Pyla. 2012. *The UX Book: Process and Guidelines for Ensuring Quality User Experience* (1st ed.). Morgan Kaufmann Publishers Inc., Waltham, MA.

Nick Heath. 2015. Windows 10 now lets you turn off tracking – but only if you're a business. TechRepublic. (November 2015). Retrieved February 04, 2016 from http://www.techrepublic.com/article/windows-10-now-lets-you-turn-off-tracking-but-only-if-youre-a-business/

P. Paul Heppner, Bruce E. Wampold, and Dennis M. Kivlinghan, Jr. 2008. *Research Design in Counseling* (3rd ed.). Brooks/Cole Publishing Co., Belmont, CA, USA.

Jason I. Hong, Jennifer D. Ng, Scott Lederer, and James A. Landay. 2004. Privacy Risk Models for Designing Privacy-Sensitive Ubiquitous Computing Systems. In *Proceedings of the 5th Con-*

ference on Designing Interactive Systems: Processes, Practices, Methods, and Techniques (DIS '04). ACM, New York, NY, USA, 91–100. DOI:http://dx.doi.org/10.1145/1013115.1013129

Bijit Hore, Jehan Wickramasuriya, Sharad Mehrotra, Nalini Venkatasubramanian, and Daniel Massaguer. 2009. Privacy-Preserving Event Detection in Pervasive Spaces. In *Proceedings of the 2009 IEEE International Conference on Pervasive Computing and Communications (PerCom '09)*. IEEE, Piscataway, NJ, USA, 1–10. DOI:http://dx.doi.org/10.1109/PERCOM.2009.4912772

Jean-Pierre Hubaux and Ari Juels. 2016. Privacy is Dead, Long Live Privacy. *Commun. ACM* 59, 6 (May 2016), 39–41. DOI:http://dx.doi.org/10.1145/2834114

Giovanni Iachello, Ian Smith, Sunny Consolvo, Gregory D. Abowd, Jeff Hughes, James Howard, Fred Potter, James Scott, Tim Sohn, Jeffrey Hightower, and Anthony LaMarca. 2005. Control, Deception, and Communication: Evaluating the Deployment of a Location-Enhanced Messaging Service. In *Ubicomp 2005: Ubiquitous Computing: 7th International Conference (Lecture Notes in Computer Science)*, Vol. 3660. Springer, Berlin, Heidelberg, 213–231. DOI:http://dx.doi.org/10.1007/11551201_13

Heba Ezzat Ibrahim, Sherif M. Badr, and Mohamed A. Shaheen. 2012. Adaptive Layered Approach using Machine Learning Techniques with Gain Ratio for Intrusion Detection Systems. *International Journal of Computer Applications* 56, 7 (October 2012), 10–16. DOI:http://dx.doi.org/10.5120/8901-2928

Tejinder K. Judge, Carman Neustaedter, Steve Harrison, and Andrew Blose. 2011. Family Portals: Connecting Families through a Multifamily Media Space. In *Proceedings of the 2011 Annual Conference on Human Factors in Computing Systems (CHI '11)*. ACM, New York, NY, USA, 1205–1214. DOI:http://dx.doi.org/10.1145/1978942.1979122

Tejinder K. Judge, Carman Neustaedter, and Andrew F. Kurtz. 2010. The Family Window: The Design and Evaluation of a Domestic Media Space. In *Proceedings of the 28th International*

Conference on Human Factors in Computing Systems (CHI '10). ACM, New York, NY, USA, 2361–2370. DOI:http://dx.doi.org/10.1145/1753326.1753682

Dennis Kafura, Denis Gračanin, Manuel Pérez-Quiñones, Tom DeHart, and Sherley Codio. 2011. An Approach to Community-Oriented Email Privacy. In *Proceedings of the 2011 IEEE Third International Conference on Privacy, Security, Risk and Trust and 2011 IEEE Third International Conference on Social Computing (PASSAT/SocialCom '11)*. IEEE, Piscataway, NJ, USA, 966–973. DOI:http://dx.doi.org/10.1109/PASSAT/SocialCom.2011.96

Christos Kalloniatis, Evangelia Kavakli, and Stefanos Gritzalis. 2008. Addressing Privacy Requirements in System Design: The PriS Method. *Requirements Engineering* 13, 3 (September 2008), 241–255. DOI:http://dx.doi.org/10.1007/s00766-008-0067-3

Rachel Kaplan and Stephen Kaplan. 1989. *The Experience of Nature: A Psychological Perspective* (1st ed.). Cambridge University Press, Cambridge, UK.

Clare-Marie Karat, John Karat, and Carolyn Brodie. 2005. Why HCI Research in Privacy and Security is Critical Now. *International Journal of Human-Computer Studies* 63, 1–2 (July 2005), 1–4. DOI:http://dx.doi.org/10.1016/j.ijhcs.2005.04.016

Mohamad Kassab, Colin Neill, and Phillip Laplante. 2014. State of Practice in Requirements Engineering: Contemporary Data. *Innovations in Systems and Software Engineering* 10, 4 (April 2014), 235–241. DOI:http://dx.doi.org/10.1007/s11334-014-0232-4

Patrick Gage Kelley, Michael Benisch, Lorrie Faith Cranor, and Norman Sadeh. 2011. When Are Users Comfortable Sharing Locations with Advertisers?. In *Proceedings of the 2011 Annual Conference on Human Factors in Computing Systems (CHI '11)*. ACM, New York, NY, USA, 2449–2452. DOI:http://dx.doi.org/10.1145/1978942.1979299

Julie A. Kientz, Shwetak N. Patel, Brian Jones, Ed Price, Elizabeth D. Mynatt, and Gregory D. Abowd. 2008. The Georgia Tech Aware Home. In *CHI '08 Extended Abstracts on Human Factors in Computing Systems (CHI EA '08)*. ACM, New York, NY, USA, 3675–3680. DOI:http://dx.doi.org/10.1145/1358628.1358911

Hubert Knoblauch, René Tuma, and Bernt Schnettler. 2014. Video Analysis and Videography. In *The SAGE Handbook of Qualitative Data Analysis* (1st ed.), Uwe Flick (Ed.). SAGE Publications Ltd, Thousand Oaks, CA, USA, Chapter 30, 435–450. DOI:http://dx.doi.org/10.4135/9781446282243

Orestis Kostakis, Panagiotis Papapetrou, and Jaakko Hollmén. 2011. Distance Measure for Querying Sequences of Temporal Intervals. In *Proceedings of the 4th International Conference on Pervasive Technologies Related to Assistive Environments (PETRA '11)*. ACM, New York, NY, USA, Article 40, 8 pages. DOI:http://dx.doi.org/10.1145/2141622.2141669

Vassilis Kostakos, Jayant Venkatanathan, Bernardo Reynolds, Norman Sadeh, Eran Toch, Siraj A. Shaikh, and Simon Jones. 2011. Who's Your Best Friend?: Targeted Privacy Attacks in Location-Sharing Social Networks. In *Proceedings of the 13th International Conference on Ubiquitous Computing (UbiComp '11)*. ACM, New York, NY, USA, 177–186. DOI:http://dx.doi.org/10.1145/2030112.2030138

Hans-Ulrich Krieger. 2010. A General Methodology for Equipping Ontologies With Time. In *Proceedings of the Seventh International Conference on Language Resources and Evaluation (LREC'10)*, Nicoletta Calzolari, Khalid Choukri, Bente Maegaard, Joseph Mariani, Jan Odijk, Stelios Piperidis, Mike Rosner, and Daniel Tapias (Eds.). European Language Resources Association (ELRA), Valletta, Malta, 3165–3172. http://www.lrec-conf.org/proceedings/lrec2010/summaries/29

Airi Lampinen, Vilma Lehtinen, Asko Lehmuskallio, and Sakari Tamminen. 2011. We're in It Together: Interpersonal Management of Disclosure in Social Network Services. In *Proceedings of the 2011 Annual Conference on Human Factors in Computing Systems (CHI '11)*. ACM, New York, NY, USA, 3217–3226. DOI:http://dx.doi.org/10.1145/1978942.1979420

Mark R. Leary and Robin M. Kowalski. 1990. Impression Management: A Literature Review and Two-Component Model. *Psychological Bulletin* 107, 1 (January 1990), 34–47. DOI:http://dx.doi.org/10.1037/0033-2909.107.1.34

Ki Jung Lee and Il-Yeol Song. 2011. Modeling and Analyzing User Behavior of Privacy Management on Online Social Network: Research in Progress. In *Proceedings of the 2011 IEEE Third International Conference on Privacy, Security, Risk and Trust and 2011 IEEE Third International Conference on Social Computing (PASSAT/SocialCom '11)*. IEEE, Piscataway, NJ, USA, 1344–1351. DOI:http://dx.doi.org/10.1109/PASSAT/SocialCom.2011.80

Chiara Leonardi, Claudio Mennecozzi, Elena Not, Fabio Pianesi, Massimo Zancanaro, Francesca Gennai, and Antonio Cristoforetti. 2009. Knocking on Elders' Door: Investigating the Functional and Emotional Geography of Their Domestic Space. In *Proceedings of the 27th International Conference on Human Factors in Computing Systems (CHI '09)*. ACM, New York, NY, USA, 1703–1712. DOI:http://dx.doi.org/10.1145/1518701.1518963

Lawrence Lessig. 1999. The Architecture of Privacy. *Vanderbilt Journal of Entertainment Law & Practice* 1, 1 (Spring 1999), 56–65. http://www.jetlaw.org/journal-archives/volume-1/volume-1-issue-1/

Dan Levine and Joseph Menn. 2016. Apple calls FBI iPhone request 'unprecedented' in court filing. Reuters. (February 2016). Retrieved April 14, 2016 from http://www.reuters.com/article/us-apple-encryption-lawsuit-idUSKCN0VY2PI

Linda Little and Pam Briggs. 2009. Pervasive Healthcare: The Elderly Perspective. In *Proceedings of the 2nd International Conference on Pervasive Technologies Related to Assistive Environments (PETRA '09)*. ACM, New York, NY, USA, Article 71, 5 pages. DOI:http://dx.doi.org/10.1145/1579114.1579185

Clara Mancini, Yvonne Rogers, Keerthi Thomas, Adam N. Joinson, Blaine A. Price, Arosha K. Bandara, Lukasz Jedrzejczyk, and Bashar Nuseibeh. 2011. In the Best Families: Tracking and Relationships. In *Proceedings of the 2011 Annual Conference on Human Factors in Computing Systems (CHI '11)*. ACM, New York, NY, USA, 2419–2428. DOI:http://dx.doi.org/10.1145/1978942.1979296

Winfried Marotzki, Jens Holze, and Dan Verständig. 2014. Analysing Virtual Data. In *The SAGE Handbook of Qualitative Data Analysis* (1st ed.), Uwe Flick (Ed.). SAGE Publications Ltd, Thousand Oaks, CA, USA, Chapter 31, 450–465. DOI:http://dx.doi.org/10.4135/9781446282243

John McCarthy and Patrick J. Hayes. 1969. Some Philosophical Problems from the Standpoint of Artificial Intelligence. In *Machine Intelligence 4*, Bernard Meltzer and Donald Michie (Eds.). Edinburgh University Press, Edinburgh, UK, 463–502.

Kent McDonald. 2015. *Beyond Requirements: Analysis with an Agile Mindset* (1st ed.). Addison-Wesley Professional, Upper Saddle River, NJ, USA.

H. Mehdi, Kh. S. Karimov, and A. A. Kavokin. 2010. Information Gain Ratio Based Clustering for Investigation of Environmental Parameters Effects on Human Mental Performance. *International Journal of Social, Behavioral, Educational, Economic, Business and Industrial Engineering* 4, 2 (2010), 54–58. http://the-internationalacademy.org/publication/11422

Fabian Mörchen. 2006. Algorithms for time series knowledge mining. In *Proceedings of the 12th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD '06)*. ACM, New York, NY, USA, 668–673. DOI:http://dx.doi.org/10.1145/1150402.1150485

Fabian Mörchen. 2007. Unsupervised Pattern Mining from Symbolic Temporal Data. *ACM SIGKDD Explorations Newsletter* 9, 1 (June 2007), 41–55. Issue 1. DOI:http://dx.doi.org/10.1145/1294301.1294302

Fabian Mörchen and Dmitriy Fradkin. 2010. Robust Mining of Time Intervals with Semi-Interval Partial Order Patterns. In *Proceedings of the 2010 SIAM International Conference on Data Mining (SDM '10)*. SIAM, Philadelphia, PA, USA, 315–326. DOI:http://dx.doi.org/10.1137/1.9781611972801.28

Anthony Morton. 2013. Measuring Inherent Privacy Concern and Desire for Privacy: A Pilot Survey Study of an Instrument to Measure Dispositional Privacy Concern. In *Proceedings of* *the 2013 ASE/IEEE International Conference on Privacy, Security, Risk and Trust and 2013 ASE/IEEE International Conference on Social Computing (PASSAT/SocialCom '13)*. IEEE, Piscataway, NJ, USA, 468–477. DOI: http://dx.doi.org/10.1109/SocialCom.2013.73

Moira Munro and Ruth Madigan. 1999. Negotiating Space in the Family Home. In *At Home: An Anthropology of Domestic Space* (1st ed.), Irene Cieraad (Ed.). Syracuse University Press, Syracuse, NY, Chapter 9, 107–117.

John Mylopoulos, Lawrence Chung, and Eric Yu. 1999. From Object-Oriented to Goal-Oriented Requirements Analysis. *Commun. ACM* 42, 1 (January 1999), 31–37. DOI: http://dx.doi.org/10.1145/291469.293165

Daniele Nardi and Ronald J. Brachmann. 2003. An Introduction to Description Logic. In *The Description Logic Handbook: Theory, Implementation, and Applications* (1st ed.), Franz Baader, Diego Calvanese, Deborah L. McGuinness, Daniele Nardi, and Peter Patel-Schneider (Eds.). Cambridge University Press, Cambridge, UK, Chapter 1, 5–44.

Patricia Brierley Newell. 1994. A Systems Model of Privacy. *Journal of Environmental Psychology* 14, 1 (March 1994), 65–78. DOI: http://dx.doi.org/10.1016/S0272-4944(05)80199-9

David H. Nguyen, Aurora Bedford, Alexander Gerard Bretana, and Gillian R. Hayes. 2011. Situating the Concern for Information Privacy through an Empirical Study of Responses to Video Recording. In *Proceedings of the 2011 Annual Conference on Human Factors in Computing Systems (CHI '11)*. ACM, New York, NY, USA, 3207–3216. DOI: http://dx.doi.org/10.1145/1978942.1979419

Helen Nissenbaum. 2004. Privacy as Contextual Integrity. *Washington Law Review* 79, 1 (February 2004), 119–158. http://hdl.handle.net/1773.1/61

Shawn C. O'Connor and Lorne K. Rosenblood. 1996. Affiliation Motivation in Everyday Experience: A Theoretical Comparison. *Journal of Personality and Social Psychology* 70, 3 (March 1996), 513–522. DOI: http://dx.doi.org/10.1037/0022-3514.70.3.513

Leysia Palen and Paul Dourish. 2003. Unpacking “Privacy” for a Networked World. In *Proceedings of the 2003 SIGCHI Conference on Human Factors in Computing Systems (CHI ’03)*. ACM, New York, NY, USA, 129–136. DOI: http://dx.doi.org/10.1145/642611.642635

Themis Panayiotopoulos. 2000. Temporal Reasoning with TRL. In *Intensional Programming II: Based on the Papers at ISLIP ’99 (ISLIP ’99)*, Manolis Gergatsoulis and Panos Rondogiannis (Eds.). World Scientific Publishing Company, Hackensack, NJ, USA, 133–148.

Kyungseo Park, Yong Lin, Vangelis Metsis, Zhengyi Le, and Fillia Makedon. 2010. Abnormal Human Behavioral Pattern Detection in Assisted Living Environments. In *Proceedings of the 3rd International Conference on Pervasive Technologies Related to Assistive Environments (PETRA ’10)*. ACM, New York, NY, USA, Article 9, 8 pages. DOI: http://dx.doi.org/10.1145/1839294.1839305

Sameer Patil, Natalia Romero, and John Karat. 2006. Privacy and HCI: Methodologies for Studying Privacy Issues. In *CHI ’06 Extended Abstracts on Human Factors in Computing Systems (CHI EA ’06)*. ACM, New York, NY, USA, 1719–1722. DOI: http://dx.doi.org/10.1145/1125451.1125771

Debprakash Patnaik, P. S. Sastry, and K. P. Unnikrishnan. 2008. Inferring Neuronal Network Connectivity from Spike Data: A Temporal Data Mining Approach. *Scientific Programming* 16, 1 (January 2008), 49–77. DOI: http://dx.doi.org/10.3233/SPR-2008-0242

Michael Quinn Patton. 1990. *Qualitative Evaluation and Research Methods* (2nd ed.). SAGE Publications, Inc., Thousand Oaks, CA, USA.

Sai Teja Peddinti and Nitesh Saxena. 2011. On the Limitations of Query Obfuscation Techniques for Location Privacy. In *Proceedings of the 13th International Conference on Ubiquitous Computing (UbiComp ’11)*. ACM, New York, NY, USA, 187–196. DOI: http://dx.doi.org/10.1145/2030112.2030139

Darhl M. Pedersen. 1979. Dimensions of Privacy. *Perceptual and Motor Skills* 48, 3c (June 1979), 1291–1297. DOI: http://dx.doi.org/10.2466/pms.1979.48.3c.1291

Darhl M. Pedersen. 1982. Personality Correlates of Privacy. *Journal of Psychology* 112, 1 (September 1982), 11. DOI:http://dx.doi.org/10.1080/00223980.1982.9923528

Darhl M. Pedersen. 1987. Sex Differences in Privacy Preferences. *Perceptual and Motor Skills* 64, 3c (June 1987), 1239–1242. DOI:http://dx.doi.org/10.2466/pms.1987.64.3c.1239

Darhl M. Pedersen. 1997. Psychological Functions of Privacy. *Journal of Environmental Psychology* 17, 2 (June 1997), 147–156. DOI:http://dx.doi.org/10.1006/jevp.1997.0049

Darhl M. Pedersen. 1999. Model for Types of Privacy by Privacy Functions. *Journal of Environmental Psychology* 19, 4 (December 1999), 397–405. DOI:http://dx.doi.org/10.1006/jevp.1999.0140

Darhl M. Pedersen and Shelia Frances. 1990. Regional Differences in Privacy Preferences. *Psychological Reports* 66, 3 (August 1990), 731–736. DOI:http://dx.doi.org/10.2466/pr0.1990.66.3.731

Hanchuan Peng, Fuhui Long, and C. Ding. 2005. Feature selection based on mutual information criteria of max-dependency, max-relevance, and min-redundancy. *IEEE Transactions on Pattern Analysis and Machine Intelligence* 27, 8 (August 2005), 1226–1238. DOI:http://dx.doi.org/10.1109/TPAMI.2005.159

Paul J. J. Pennartz. 1999. Home: The Experience of Atmosphere. In *At Home: An Anthropology of Domestic Space* (1st ed.), Irene Cieraad (Ed.). Syracuse University Press, Syracuse, NY, Chapter 8, 95–106.

Peter Pirolli and Stuart Card. 2005. The Sensemaking Process and Leverage Points for Analyst Technology as Identified through Cognitive Task Analysis. In *Proceedings of the 2005 International Conference on Intelligence Analysis*. The MITRE Corporation, Bedford, MA, USA, 2–4. https://analysis.mitre.org/proceedings/Final_Papers_Files/206_Camera_Ready_Paper.pdf

Inmaculada Plaza, Lourdes Martín, Sergio Martin, and Carlos Medrano. 2011. Mobile Applications in an Aging Society: Status and Trends. *Journal of Systems and Software* 84, 11 (November 2011), 1977–1988. DOI:http://dx.doi.org/10.1016/j.jss.2011.05.035

Nayot Poolsappasit and Indrakshi Ray. 2008. Towards a Scalable Model for Location Privacy. In *Proceedings of the ACM SIGSPATIAL GIS 2008 International Workshop on Security and Privacy in GIS and LBS (SPRINGL '08)*. ACM, New York, NY, USA, 46–51. DOI:http://dx.doi.org/10.1145/1503402.1503412

William H. Press, Brian P. Flannery, Saul A. Teukolsky, and William T. Vetterling. 2007. *Numerical Recipes: the Art of Scientific Computing* (3rd ed.). Cambridge University Press, Cambridge, UK.

Tim Putnam. 1999. "Postmodern" Home Life. In *At Home: An Anthropology of Domestic Space* (1st ed.), Irene Cieraad (Ed.). Syracuse University Press, Syracuse, NY, Chapter 12, 144–152.

Hongwu Qin, Xiuqin Ma, Tutut Herawan, and Jasni Mohamad Zain. 2014. MGR: An Information Theory Based Hierarchical Divisive Clustering Algorithm for Categorical Data. *Knowledge-Based Systems* 67 (September 2014), 401–411. DOI:http://dx.doi.org/10.1016/j.knosys.2014.03.013

John Ross Quinlan. 1986. Induction of Decision Trees. *Machine Learning* 1, 1 (March 1986), 81–106. DOI:http://dx.doi.org/10.1007/BF00116251

Peter Jozsef Radics and Denis Gračanin. 2011. Privacy in Domestic Environments. In *CHI '11 Extended Abstracts on Human Factors in Computing Systems (CHI EA '11)*. ACM, New York, NY, USA, 1735–1740. DOI:http://dx.doi.org/10.1145/1979742.1979837

Peter Jozsef Radics, Denis Gračanin, and Dennis Kafura. 2013. PREprocess Before You Build: Introducing a Framework for Privacy Requirements Engineering. In *Proceedings of the 2013 ASE/IEEE International Conference on Privacy, Security, Risk and Trust and 2013 ASE/IEEE International Conference on Social Computing (PASSAT/SocialCom '13)*. IEEE, Piscataway, NJ, USA, 564–569. DOI:http://dx.doi.org/10.1109/SocialCom.2013.85

Peter J. Radics, Nicholas F. Polys, Shawn P. Neuman, and William H. Lund. 2015. OSNAP! Introducing the Open Semantic Network Analysis Platform. In *Proceedings of the IS&T/SPIE Visualization and Data Analysis Conference*, Vol. 9397. SPIE, Bellingham, WA, USA, 939707–1–939707–15. DOI:http://dx.doi.org/10.1117/12.2077834

Andrew Raij, Animikh Ghosh, Santosh Kumar, and Mani Srivastava. 2011. Privacy Risks Emerging from the Adoption of Innocuous Wearable Sensors in the Mobile Environment. In *Proceedings of the 2011 Annual Conference on Human Factors in Computing Systems (CHI '11)*. ACM, New York, NY, USA, 11–20. DOI:http://dx.doi.org/10.1145/1978942.1978945

Tim Rapley. 2014. Sampling Strategies in Qualitative Research. In *The SAGE Handbook of Qualitative Data Analysis* (1st ed.), Uwe Flick (Ed.). SAGE Publications Ltd, Thousand Oaks, CA, USA, Chapter 4, 49–64. DOI:http://dx.doi.org/10.4135/9781446282243

Joseph Reagle and Lorrie Faith Cranor. 1999. The Platform for Privacy Preferences. *Commun. ACM* 42, 2 (February 1999), 48–55. DOI:http://dx.doi.org/10.1145/293411.293455

Alfréd Rényi. 1961. On Measures of Entropy and Information. In *Proceedings of the Fourth Berkeley Symposium on Mathematical Statistics and Probability, Volume 1: Contributions to the Theory of Statistics*. University of California Press, Berkeley, CA, USA, 547–561. http://projecteuclid.org/euclid.bsmsp/1200512181

Suzanne Robertson and James C. Robertson. 2006. *Mastering the Requirements Process* (2nd ed.). Addison-Wesley Professional, Upper Saddle River, NJ, USA. 592 pages.

Tom Rodden and Steve Benford. 2003. The evolution of buildings and implications for the design of ubiquitous domestic environments. In *Proceedings of the 2003 Annual Conference on Human Factors in Computing Systems (CHI '03)*. ACM, New York, NY, USA, 9–16. DOI:http://dx.doi.org/10.1145/642611.642615

Christoph Rosenkranz, Marianne Corvera Charaf, and Roland Holten. 2013. Language Quality in Requirements Development: Tracing Communication in the Process of Information Systems Development. *Journal of Information Technology* 28, 3 (September 2013), 198–223. DOI:http://dx.doi.org/10.1057/jit.2012.33

Mary Beth Rosson and John M. Carroll. 2002. *Usability Engineering: Scenario-Based Development of Human-Computer Interaction* (1st ed.). Morgan Kaufmann Publishers Inc., San Francisco, CA, USA.

Kathryn Roulston. 2014. Analysing Interviews. In *The SAGE Handbook of Qualitative Data Analysis* (1st ed.), Uwe Flick (Ed.). SAGE Publications Ltd, Thousand Oaks, CA, USA, Chapter 20, 297–313. DOI:http://dx.doi.org/10.4135/9781446282243

Stuart Russell and Peter Norvig. 2003. *Artificial Intelligenc: A Modern Approach* (2nd ed.). Prentice Hall, Upper Saddle River, New Jersey, USA.

Tony Salvador, Genevieve Bell, and Ken Anderson. 1999. Design Ethnography. *Design Management Journal (Former Series)* 10, 4 (October 1999), 35–41. DOI:http://dx.doi.org/10.1111/j.1948-7169.1999.tb00274.x

Florian Schaub, Bastian Könings, Stefan Dietzel, Michael Weber, and Frank Kargl. 2012a. Privacy Context Model for Dynamic Privacy Adaptation in Ubiquitous Computing. In *Proceedings of the 2012 ACM Conference on Ubiquitous Computing (UbiComp '12)*. ACM, New York, NY, USA, 752–757. DOI:http://dx.doi.org/10.1145/2370216.2370383

Florian Schaub, Bastian Könings, Michael Weber, and Frank Kargl. 2012b. Towards Context Adaptive Privacy Decisions in Ubiquitous Computing. In *Proceedings of the 2012 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Wksp '12)*. IEEE, Piscataway, NJ, USA, 407–410. DOI:http://dx.doi.org/10.1109/PerComW.2012.6197521

Claude E. Shannon. 1948. A Mathematical Theory of Communication. *The Bell System Technical Journal* 27, 3 (July 1948), 379–423. DOI:http://dx.doi.org/10.1002/j.1538-7305.1948.tb01338.x

Stuart S. Shapiro. 2010. Privacy by Design: Moving from Art to Practice. *Commun. ACM* 53, 6 (June 2010), 27–29. Issue 6. DOI:http://dx.doi.org/10.1145/1743546.1743559

John Rennie Short. 1999. Foreword. In *At Home: An Anthropology of Domestic Space* (1st ed.), Irene Cieraad (Ed.). Syracuse University Press, Syracuse, NY, ix–x.

John Slankas and Laurie Williams. 2013. Access Control Policy Extraction from Unconstrained Natural Language Text. In *Proceedings of the 2013 ASE/IEEE International Conference on Privacy, Security, Risk and Trust and 2013 ASE/IEEE International Conference on Social Computing (PASSAT/SocialCom '13)*. IEEE, Piscataway, NJ, USA, 435–440. DOI:http://dx.doi.org/10.1109/SocialCom.2013.68

Paul Slovic. 1987. Perception of Risk. *Science* 236, 4799 (April 1987), 280–285. DOI:http://dx.doi.org/10.1126/science.3563507

Paul Slovic and Ellen Peters. 2006. Risk Perception and Affect. *Current Directions in Psychological Science (Wiley-Blackwell)* 15, 6 (December 2006), 322–325. DOI:http://dx.doi.org/10.1111/j.1467-8721.2006.00461.x

Paul Slovic, Ellen Peters, Melissa L. Finucane, and Donald G. MacGregor. 2005. Affect, Risk, and Decision Making. *Health Psychology* 24, 4, Suppl (July 2005), 35–40. DOI:http://dx.doi.org/10.1037/0278-6133.24.4.S35

Daniel J. Solove. 2006. A Taxonomy of Privacy. *University of Pennsylvania Law Review* 154, 3 (January 2006), 477–560. DOI:http://dx.doi.org/10.2307/40041279

Sarah Spiekermann and Lorrie Faith Cranor. 2009. Engineering Privacy. *IEEE Transactions on Software Engineering* 35, 1 (January 2009), 67–82. DOI:http://dx.doi.org/10.1109/TSE.2008.88

Anna Cinzia Squicciarini and Cristopher Griffin. 2012. An Informed Model of Personal Information Release in Social Networking Sites. In *Proceedings of the 2012 ASE/IEEE International*

Conference on Privacy, Security, Risk and Trust and 2012 ASE/IEEE International Confernece on Social Computing (PASSAT/SocialCom '12). IEEE, Piscataway, NJ, USA, 636–645. DOI:http://dx.doi.org/10.1109/SocialCom-PASSAT.2012.137

David W. Stewart, Prem N. Shamdasani, and Dennis W. Rook. 2009. Group Depth Interviews: Focus Group Research. In *The SAGE Handbook of Applied Social Research Methods* (2nd ed.), Leonard Bickman and Debra J. Rog (Eds.). SAGE Publications, Inc., Thousand Oaks, CA, USA, Chapter 18, 589–617. DOI:http://dx.doi.org/10.4135/9781483348858.n18

Lucy A. Suchman. 2007. *Human-Machine Reconfigurations: Plans and Situated Actions* (2nd ed.). Cambridge University Press, New York, NY, USA.

Alistair G. Sutcliffe. 2002. *The Domain Theory: Patterns for Knowledge and Software Reuse* (1st ed.). Lawrence Erlbaum Associates, Inc., Mahwah, NJ.

Alistair G. Sutcliffe and John M. Carroll. 1999. Designing Claims for Reuse in Interactive Systems Design. *International Journal of Human-Computer Studies* 50, 3 (March 1999), 213–241. DOI:http://dx.doi.org/10.1006/ijhc.1999.0245

Joseph Tan, Patrick C. K. Hung, Michael Dohan, Thomas Trojer, Matthias Farwick, and Jayshiro Toshiro. 2010. Gateway to Quality Living for the Elderly: Charting an Innovative Approach to Evidence-Based E-Health Technologies for Serving the Chronically Ill. In *Proceedings of the 2010 13th IEEE International Conference on Computational Science and Engineering (CSE '10)*. IEEE, Piscataway, NJ, USA, 146–159. DOI:http://dx.doi.org/10.1109/CSE.2010.27

Eran Toch, Justin Cranshaw, Paul Hankes Drielsma, Janice Y. Tsai, Patrick Gage Kelley, James Springfield, Lorrie Cranor, Jason Hong, and Norman Sadeh. 2010. Empirical Models of Privacy in Location Sharing. In *Proceedings of the 12th ACM International Conference on Ubiquitous Computing (Ubicomp '10)*. ACM, New York, NY, USA, 129–138. DOI:http://dx.doi.org/10.1145/1864349.1864364

Myron Tribus. 1961. *Thermostatics and Thermodynamics: An Introduction to Energy, Information and States of Matter, with Engineering Applications* (2nd ed.). D. Van Nostrand Company, Inc., Princeton, NJ, USA.

Alfred Ultsch. 2004. *Unification-Based Temporal Grammar.* Technical Report 37. Philips-Universität, Marburg, Germany.

Va. Code §231.1-1303. 2016. Governing boards; duties. (October 2016). Retrieved July 07, 2016 from http://law.lis.virginia.gov/vacode/title23.1/chapter13/section23.1-1303

Peter-Paul Verbeek. 2005. *What Things Do: Philosophical Reflection on Technology, Agency, and Design* (1st ed.). The Pennsylvania State University Press, University Park, PA, USA.

Virginia Tech. 2016. Factbook: About the University. (June 2016). Retrieved July 08, 2016 from http://www.vt.edu/about/factbook.html

Ron Wakkary and Karen Tanenbaum. 2009. A Sustainable Identity: The Creativity of an Everyday Designer. In *Proceedings of the 27th International Conference on Human Factors in Computing Systems (CHI '09).* ACM, New York, NY, USA, 365–374. DOI: http://dx.doi.org/10.1145/1518701.1518761

Jinjun Wang and Ying Yan. 2012. The Interview Question. In *The SAGE Handbook of Interview Research: The Complexity of the Craft* (1st ed.), Jaber F. Gubrium, James A. Holstein, Amir B. Marvasti, and Karyn D. McKinney (Eds.). SAGE Publications, Inc., Thousand Oaks, CA, USA, Chapter 15, 231–243. DOI: http://dx.doi.org/10.4135/9781452218403

Karl E. Weick. 2000. *Making Sense of the Organization* (1st ed.). Wiley-Blackwell, Malden, MA, USA.

Marius Wernke, Frank Dürr, and Kurt Rothermel. 2012. PShare: Position sharing for location privacy based on multi-secret sharing. In *Proceedings of the 2012 IEEE International Conference on Pervasive Computing and Communications (PerCom '12).* IEEE, Piscataway, NJ, USA, 153–161. DOI: http://dx.doi.org/10.1109/PerCom.2012.6199862

Alan F. Westin. 1967. *Privacy and Freedom* (1st ed.). Atheneum, New York, NY, USA.

Jason Wiese, Patrick Gage Kelley, Lorrie Faith Cranor, Laura Dabbish, Jason I. Hong, and John Zimmerman. 2011. Are you close with me? are you nearby?: investigating social groups, closeness, and willingness to share. In *Proceedings of the 13th international conference on Ubiquitous computing (UbiComp '11)*. ACM, New York, NY, USA, 197–206. DOI: http://dx.doi.org/10.1145/2030112.2030140

Ian H. Witten, Eibe Frank, and Mark A. Hall. 2011. *Data Mining: Practical Machine Learning Tools and Techniques* (3rd ed.). Morgan Kaufmann Publishers Inc., Boston, MA, USA.

World Wide Web Consortium (W3C). 2004a. OWL Web Ontology Language Overview. (February 2004). Retrieved February 04, 2016 from http://www.w3.org/TR/owl-features/

World Wide Web Consortium (W3C). 2004b. XML Schema Part 2: Datatypes Second Edition. (October 2004). Retrieved July 25, 2016 from http://www.w3.org/TR/xmlschema-2/

Chien-Ping Wu, Chen-Che Huang, Jiun-Long Huang, and Chih-Lin Hu. 2011. On Preserving Location Privacy in Mobile Environments. In *Proceedings of the 2011 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Wksp '11)*. IEEE, Piscataway, NJ, USA, 490–495. DOI: http://dx.doi.org/10.1109/PERCOMW.2011.5766939

Sarita Yardi and Amy Bruckman. 2011. Social and technical challenges in parenting teens' social media use. In *Proceedings of the 2011 annual conference on Human factors in computing systems (CHI '11)*. ACM, New York, NY, USA, 3237–3246. DOI: http://dx.doi.org/10.1145/1978942.1979422

Eric Yu, Paolo Giorgini, Neil Maiden, and John Mylopoulos (Eds.). 2010. *Social Modeling for Requirements Engineering* (1st ed.). The MIT Press, Cambridge, MA, USA.

Eric Yu, Paolo Giorgini, Neil Maiden, and John Mylopoulos. 2010. Social Modeling for Requirements Engineering: An Introduction. In *Social Modeling for Requirements Engineering* (1st ed.), Eric Yu, Paolo Giorgini, Neil Maiden, and John Mylopoulos (Eds.). MIT Press, Cambridge, MA, USA, Chapter 1, 3–10.

Jinyan Zang, Krysta Dummit, James Graves, Paul Lisker, and Latanya Sweeney. 2015. Who Knows What About Me? A Survey of Behind the Scenes Personal Data Sharing to Third Parties by Mobile Apps. *Technology Science* 2015103001 (October 2015). http://techscience.org/a/2015103001

Ge Zhong and Urs Hengartner. 2009. A Distributed k-Anonymity Protocol for Location Privacy. In *Proceedings of the 2009 IEEE International Conference on Pervasive Computing and Communications (PerCom '09)*. IEEE, Piscataway, NJ, USA, 1–10. DOI : http://dx.doi.org/10.1109/PERCOM.2009.4912774

Appendix A

The Privacy Domain Modeling Language Abstract Syntax

The syntax of the Privacy Domain Modeling Language (PDML) is provided in the Extended Backus-Naur Form used for the definition of the abstract syntax of the Web Ontology Language (OWL) [World Wide Web Consortium (W3C) 2004a]. Datatypes correspond to the XML Schema Datatypes [World Wide Web Consortium (W3C) 2004b], referenced through the namespace *xsd* and given in italics. Furthermore, terminal symbols are quoted ('. . . '), whereas non-terminal symbols are bold and not quoted. Alternatives are either separated by a vertical bar (|) or given in separate rules. Components that can occur zero or one time are enclosed in square brackets ([. . .]). Conversely, components that can occur zero or any other number of times are enclosed in braces ({. . . }). Whitespace is ignored in the production rules.

A.1 Knowledge Base

A knowledge base in PDML consists of a unique identifier, a human-readable label, and a sequence of statements. The main content of a PDML knowledge base is carried in these statements, which provide assertions about instances and relationships, terminology in the shape of concepts and roles, and information about the temporal order of assertions.

knowledgeBase ::= 'KnowledgeBase(' **knowledgeBaseID** **label** { **statement** } ')'

statement ::= **assertion**

| **term**

| **order**

label ::= 'label(' *xsd:string* ')'

Each statement is uniquely identified through an identifier within each category. However, identifiers are not unique across categories (i.e., a term and assertion may have identical identifiers).

knowledgeBaseID ::= *xsd:ID*

instanceID ::= *xsd:ID*

relationshipID ::= *xsd:ID*

conceptID ::= *xsd:ID*

roleID ::= *xsd:ID*

orderID ::= *xsd:ID*

durationID ::= *xsd:ID*

semiIntervalID ::= *xsd:ID*

Assertions form the core of the knowledge base, representing the *extensional knowledge* or 'A-Box' (cf. [Nardi and Brachmann 2003]).

A.2 Assertions

Assertions represent statements about phenomena within a data set. These assertions can take the form of instances, which describe a thing or entity, or relationships between assertions. Each assertion is uniquely identified by an identifier and takes a human-readable label. Furthermore, details about instances and relationships are contained in a mandatory description. This description can also contain the thoughts of the analyst regarding the assertion.

assertion ::= **instance**
| **relationship**
instance ::= 'Instance(' **instanceID** **label** **description** [**duration**]
{ 'type(' **conceptID** ')' } { **support** } ')'
relationship ::= 'Relationship(' **relationshipID** **name** **description** [**duration**]
{ 'type(' **roleID** ')' } { **support** }
domain **range** ')'
domain ::= 'domain(' **assertionId** ')' { **domain** }
range ::= 'range(' **assertionId** ')' { **range** }

assertionID ::= **instanceID** | **relationshipID**
description ::= 'description(' *xsd:string* ')'
support ::= 'support(' *xsd:anyURI* ')'

Furthermore, the validity of both instances and relationships can be restricted by a duration (defined in Section A.4). Thus, the difference between an *endurant* (i.e., an assertion without temporal restriction) and such a *perdurant* or *fluent* is the existence of a duration element. Moreover, all assertions contain support statements, here given as URIs, which provide a link to the underlying data that gave rise to the assertions. This support, in concert with the reasoning provided in the description, establishes a chain of evidence for readers of the knowledge base. A final commonality shared between all assertions is the ability of classifying their type (i.e., the concept or role they instantiate). Instances are classified by concepts, whereas relationships are classified by roles (see Section A.3 for their definitions).

A large part of the expressivity of PDML lies in the definition of the domain and range of relationships. As shown above, both the domain and range of a relationship can contain one or more assertions. Thus, it is not only possible to relate a single instance to another instance, but rather it is possible to relate a single instance to multiple other instances, or vice versa. Furthermore, the definition also allows relating instances and relationships to each other. In other words, it allows arbitrary *n:m* relationships between any two sets of assertions. However, an analyst may choose to represent such relationships with a set of equivalent *1:1* relationships, depending on context and requirements.

A.3 Terms

Terms represent the *intensional knowledge* or ‘T-Box’ of the knowledge base (cf. [Nardi and Brachmann 2003]). Just like assertions, they contain a unique identifier, human-readable label, and a description. Furthermore, they serve two functions: the classification of assertions and the formation of a taxonomy. Classification is established from the side of the assertions (cf. Section A.2). However, terms can specify whether their associated assertions are *endurants* (i.e., not temporally restricted) or *perdurants* (temporally restricted). To establish a taxonomy, each term can contain a set of generalizing ‘super’ terms of the same type (i.e., concepts can have super-concepts, roles can have super-roles).

term ::= **concept**

| **role**

concept ::= ’Concept(’ **conceptID** **label** **description** **validity**

{ ’super(’ **conceptID** ’) } { **support** } ’)’

role ::= ’Role(’ **roleID** **label** **description** **validity**

{ ’super(’ **roleID** ’) } { **support** }

{ ’domain(’ **termID** ’) } { ’range(’ **termID** ’) } ’)’

termID ::= **conceptID** | **roleID**

validity ::= ‘endurant’ |‘perdurant’

Similar to assertions, terms can be supported directly through links into the data. However, while this allows to establish a chain of evidence directly, it is preferable to establish traceability through the associated assertions or sub-terms of a term. This indirect chain of evidence closer corresponds to a data-driven modeling approach, as, this way, a term is derived from its supporting assertions or represents a generalization of its sub-terms. Finally, analogously to relationships, roles can contain an arbitrary number of terms in their domains and ranges.

A.4 Durations and Semi-Intervals

PDML uses the notion of semi-intervals introduced by Freksa [1992] to represent the beginning and end of temporal intervals. Thus, each duration contains two semi-intervals in addition to an optional length. Each semi-interval contains an optional time point. Both the length of durations and the time point of semi-intervals is optional to allow for the representation of incomplete knowledge of the exact timing of events. Thus, if only the beginning, end, or duration of an event is known, it is still possible to capture that information without providing any other details.

duration ::= ’Duration(’ **durationID** ’beginning(’ **semiInterval** ’)’ ’end(’ **semiInterval** ’)’
[**length**] ’)’
semiInterval ::= ’SemiInterval(’ **semiIntervalID** [**timepoint**] ’)’

timepoint ::= ’timepoint (’ *xsd:dateTime* ’)’.
length ::= ’length(’ *xsd:duration* ’)’.

A.5 Temporal Order

The flexibility of representing durations and semi-intervals with optional lengths and time points is reflected in the way temporal orders are defined. Thus, relationships are not instantiated between the data literals, but rather the components themselves. This allows establishing the order of duration lengths without knowing either of the durations. Similarly, it allows us to establish any of the 17 semi-interval relationships defined by Freksa [1992], without knowing exact timing of events.

order ::= ’Order(’**orderID durationID comparator durationID** ’)’

| ’Order(’ **orderID semiIntervalID comparator semiIntervalID** ’)’

comparator::= ’<’ | ’≤’ | ’=’ | ’≥’ | ’>’

Appendix B

Survey of Privacy Preferences regarding Education Records

Hello, and welcome to our survey!

This research is being conducted by Peter Radics (peter.radics@vt.edu), Nicholas Polys (npolys@vt.edu), and Deborah Tatar (tatar@vt.edu) as part of ongoing research at the Department of Computer Science Department at Virginia Tech.

Purpose of the Study

The Family Educational Rights and Privacy Act of 1974 (better known as FERPA) is a law that regulates how information about students is handled by universities and other educational institutions or agencies. The law covers both “directory information” (e.g., your name, address, and major) as well as your education record (e.g., grades and transcripts). You can learn about Virginia Techs policies regarding FERPA at http://www.registrar.vt.edu/privacy/index.html.

We are interested in learning about if/how you are currently managing this information, as well as your preferences regarding how you would like to be able to manage it. We hope this survey will allow us to better understand how to protect these types of information better. Also, we hope to use the results of this study to provide suggestions to university officials on how to improve current systems. Results of this survey will be used in a dissertation and may be published in a peer-reviewed venue.

You need to be at least 18 years old to participate in this study!

Study Details

During this study, we will ask you some questions about your background. **Participation in this survey is confidential** (i.e., none of your answers can be linked to you). The main part of the survey consists of questions about your preferences regarding the management of directory information and your education record. Some of the questions refer to hypothetical situations and do not necessarily reflect Virginia Tech's current policies regarding FERPA. Taking this survey should not take you more than 30–45 minutes.

As a compensation for your time, we will either reward you 1 research credit through the Virginia Tech SONA system (if you used that system to sign up) or give you the chance to enter a raffle for one of two gift cards to the University Bookstore worth $10. The odds of winning a gift card are about 1 in 50 (specific odds vary based on participation and are at most 1 in 100). To allow us to award you research credit or enter you in the raffle, we will ask you for your Virginia Tech PID or a valid email address respectively. Providing this information is voluntary and cannot be linked to your responses!

You can skip any question you do not want to answer!
You can also exit the survey at any time without penalty by skipping all remaining answers!

I am 18 years or older, and I consent to participating in this study.
(Multiple Choice: yes | no)

I am not a robot! (Captcha to make sure responses are not automated or spammed)

Approval of Research

The Virginia Tech Institutional Review Board (IRB) has approved this research in compliance with the US Code of Federal Regulations (CFR) Title 45 Part 46 (http://www.hhs.gov/ohrp/humansubjects/guidance/45cfr46.html).
Virginia Tech IRB Approval Number: 16–343.

Questions or Concerns

Should you have any questions about this research, feel free to contact Peter Radics at peter.radics@vt.edu or Nicholas Polys at npolys@vt.edu or (540) 231–0968 directly.

Should you have any questions or concerns about the studys conduct or your rights as a research subject, or need to report a research-related injury or event, you may contact the Virginia Tech IRB Chair, Dr. David M. Moore at moored@vt.edu or (540) 231–4991.

Part I: Demographic Information

Before we get started with the questions about your privacy preferences, we would like to get to know you a little bit better. This helps us understand better how different backgrounds influence the responses in the other parts of this survey.
Question I.1: How old are you? (Text Box)
Question I.2: What is your gender? (Text Box)
Question I.3: What is your race/ethnicity? (Text Box)
Question I.4: What country or countries are you a citizen of? (Text Box)
Question I.5: What country were you born in? (Text Box)
Question I.6: Is your primary address in Virginia? (Options: Yes | No)
Question I.7: Are you an undergraduate or graduate student? (Options: undergraduate | graduate | other)
Question I.8: Are you a tax dependent of your parents/guardians (i.e., do they claim you as a dependent on their income tax forms)? (Options: yes | no | I don't know)

Part II: Questions regarding “Directory Information”

As you may know, Virginia Tech allows you to search for faculty, staff, and students through VT Search. In this part of the survey, we will ask you about your usage and preferences regarding the information available through VT Search. This information is commonly referred to as Directory Information, and includes[1]:

- Full name
- Academic major
- Email address
- Mailing address
- Phone number

Question II.1a: Have you ever used VT Search to search for information on faculty, staff, or students at Virginia Tech? *(Options: yes | no | I dont remember)*

Question II.1b-1: *(Yes in II.1a)* What kind of person were you looking for the last time you used VT Search? Were you looking to contact that person or find information about them? *(Text Box)*

Question II.1b-2: *(No in II.1a)* Were you aware of this functionality of VT Search? Have you looked for this kind of information in a different place? *(Text Box)*

Question II.2a: Are you aware that, by default, VT Search lists your full name, academic major, mailing address, and phone number? (You can change these settings in myVT) *(Options: Yes | No)*

Question II.2b: What are your opinions / feelings about these default settings? *(Text Box)*

Question II.3: If you only had the choice to make a piece of information available to everyone (“public”) or no one (“confidential”), what would be your preference for the default value for

- Your full name
- Your academic major
- Your email address
- Your mailing address
- Your phone number

(Options: public | confidential)

[1] Directory information also includes personal website and Instant Messaging IDs.

Question II.4a: If you could choose which pre-defined groups had access to different parts of your "directory information", what would be your preferences?

- Relatives
- Friends
- A fellow student in a class
- Instructors or TAs
- Other Students, Faculty, or Staff
- Law Enforcement Officials
- Job Recruiters
- Everyone else

(Options: name (y | n), major (y | n), email (y | n), mailing address (y | n), phone number (y | n))

Question II.4b: Are there any circumstances/situations in which you would answer differently for any of the groups above? *(Text Box)*

Question II.5a: If you could choose how your mailing addressed was displayed for certain groups, what would be your preferences?

- Relatives
- Friends
- A fellow student in a class
- Instructors or TAs
- Other Students, Faculty, or Staff
- Law Enforcement Officials
- Job Recruiters
- Everyone else

(Options: full address | city, state, country | state, country | country | not displayed)

Question II.5b: Are there any circumstances/situations in which you would answer differently for any of the groups above? *(Text Box)*

Part III: Questions regarding "Education Records"

The Family Educational Rights and Privacy Act (FERPA) sets up provisions for how to protect your education records (like grades, transcripts, etc.). We are interested in how you, as a student, manage this information.

Question III.1: Would you consider grades to be private information? *(Options: Yes | No)*

Question III.2a: Under what circumstances do you talk with your parents/guardians about a grade you received or grades in general? How frequently does this happen? *(Text Box)*

Question III.2b: Under what circumstances do you talk with your friends about a grade you received or grades in general? How frequently does this happen? *(Text Box)*

Question III.2c: Under what circumstances do you talk with fellow students you take a class with about a grade you received or grades in general? How frequently does this happen? *(Text Box)*

Question III.2d: Under what circumstances do you talk with any other people (i.e., people not mentioned before) about a grade or grades in general? How frequently does this happen? *(Text Box)*

Question III.3a: Are there any circumstances in which you would or have lied to your parents/guardians about a grade you received? Why/Why not? *(Text Box)*

Question III.3b: Are there any circumstances in which you would or have lied to your friends about a grade you received? Why/Why not? (Text Box)

Question III.3c: Are there any circumstances in which you would or have lied to to fellow students you take a class with about a grade you received? Why/Why not? *(Text Box)*

For the following questions, imagine there was an electronic system that allowed you to manage access to your educational records (i.e., transcripts/grades) to other people.

Question III.4: Who would you consider giving access to those records? Under what circumstances? *(Text Box)*

Question III.5: How coarse/fine would would you like to be able to grant/restrict access to parts/all of your records? *(Options: general access (all records) | semester-by-semester | class-by-class | grade-by-grade)*

Question III.6: Would you like to be able to grant/restrict access to parts/all of your record separately for each person (per-person), collectively to certain groups of people (per group), or both? *(Options: per-group | per-person | both)*

Question III.7: Would you rather create specific rules that regulate access to your education records once, or decide to grant or deny access case-by-case (potentially many times)?

(Options: create rules | decide case-by-case)

Thank You for Participating!

Before you leave, please let us know where you learned about this survey!

Where did you learn about this survey?

(Options: Virginia Tech SONA system (for research credit) | Mailing List | Other)

(If SONA) Please enter your VT PID so we can award you your research credit. *(Text Box)*

(If Mailing List/Other) If you want to enter the raffle for one of two gift cards to the Virginia Tech University Bookstore worth $10 each, please provide us with a valid email address.
Your email will not be linked to your survey responses in any way!
We will contact you by May 20, 2016 should you have won one of the gift cards. *(Text Box)*

Should you have any questions or comments about this survey, feel free to contact Peter Radics at peter.radics@vt.edu or Nicholas Polys at npolys@vt.edu or (540) 231–0968 directly.

You can learn about Virginia Techs policies regarding FERPA at
http://www.registrar.vt.edu/privacy/index.html.

(Displayed should a potential participate answer no to the question for age of 18 years or older/consent)

Sorry!

Unfortunately, you are not eligible to participate in this survey. Thank you for your interest in our survey! We hope you will consider participating in future research at Virginia Tech!

Should you have any questions about why you are not eligible to participate,feel free to contact Peter Radics at peter.radics@vt.edu or Nicholas Polys at npolys@vt.edu or (540) 231–0968 directly.

You can learn about Virginia Techs policies regarding FERPA at
http://www.registrar.vt.edu/privacy/index.html.

Appendix C

Template Reference

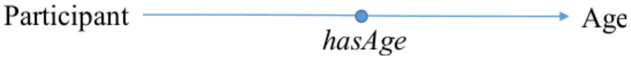


Figure C.1: Template for Question I.1.

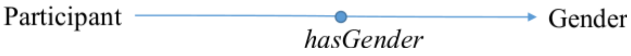


Figure C.2: Template for Question I.2.

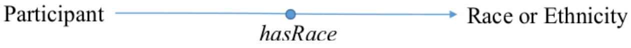


Figure C.3: Template for Question I.3.

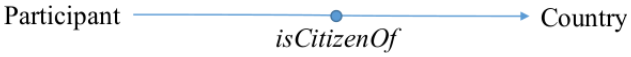


Figure C.4: Template for Question I.4.

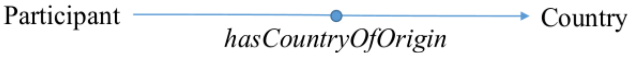


Figure C.5: Template for Question I.5.

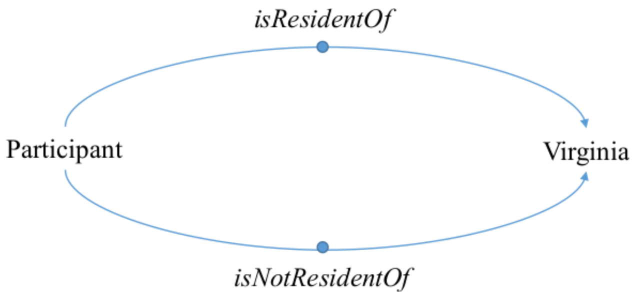


Figure C.6: Template for Question I.6.

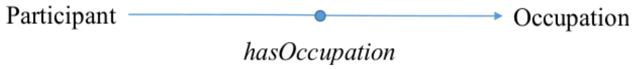


Figure C.7: Template for Question I.7.

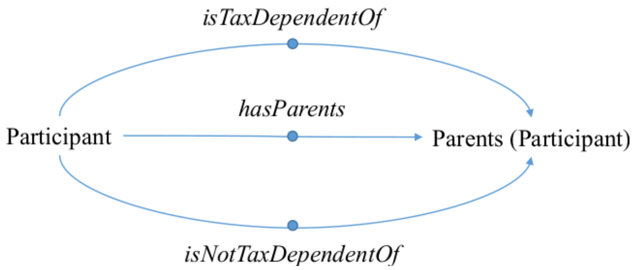


Figure C.8: Template for Question I.8.

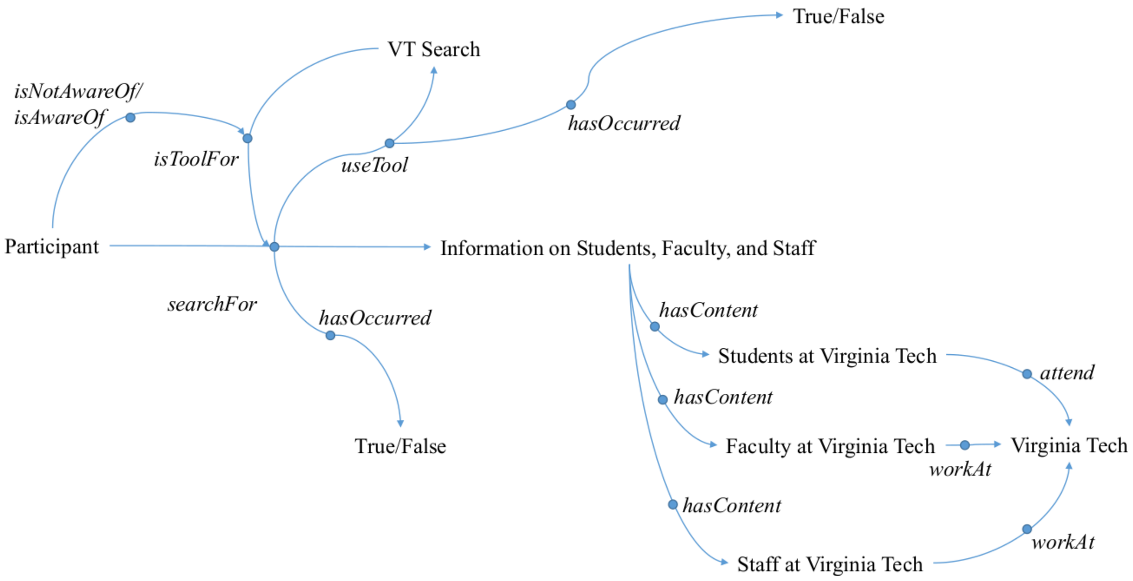


Figure C.9: Template for Questions II.1a and II.1b-2.

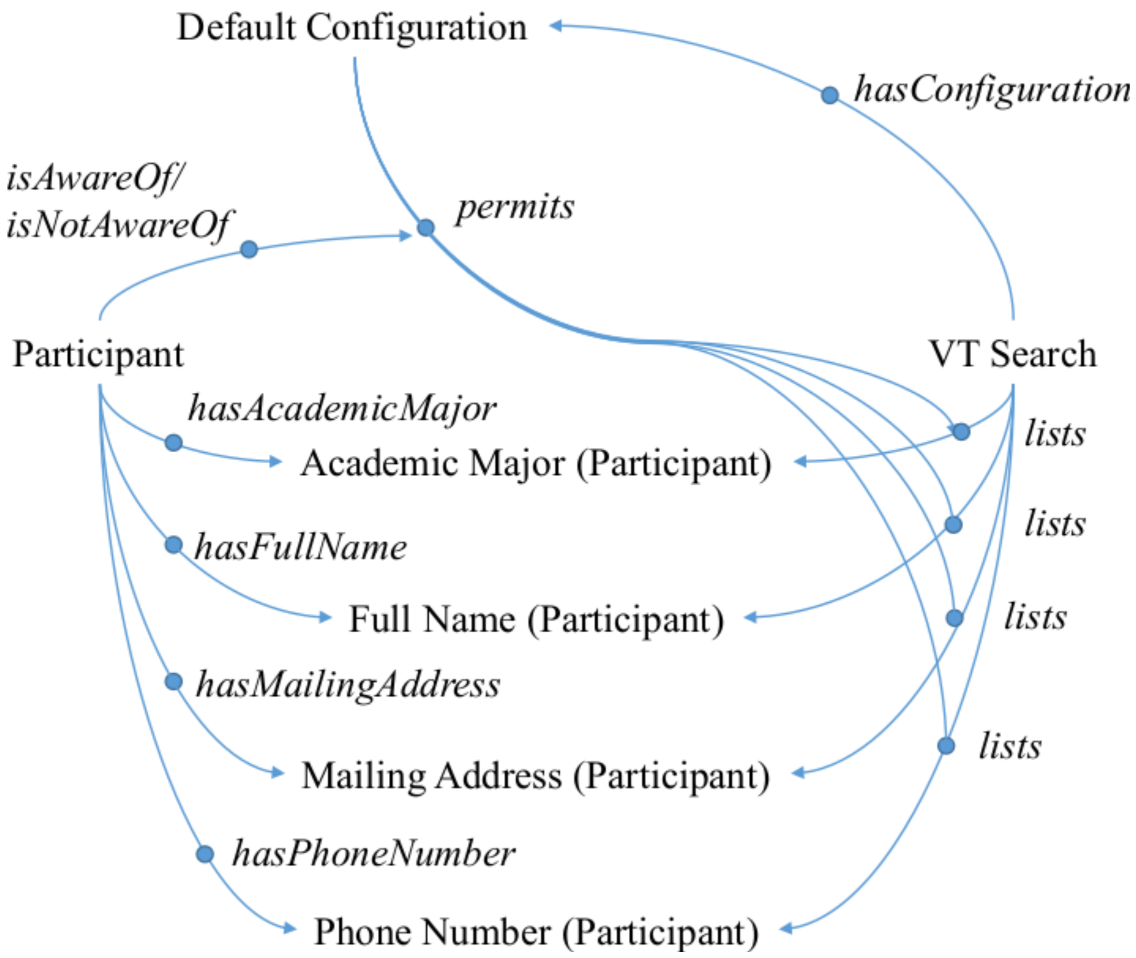


Figure C.10: Template for Question II.2a.

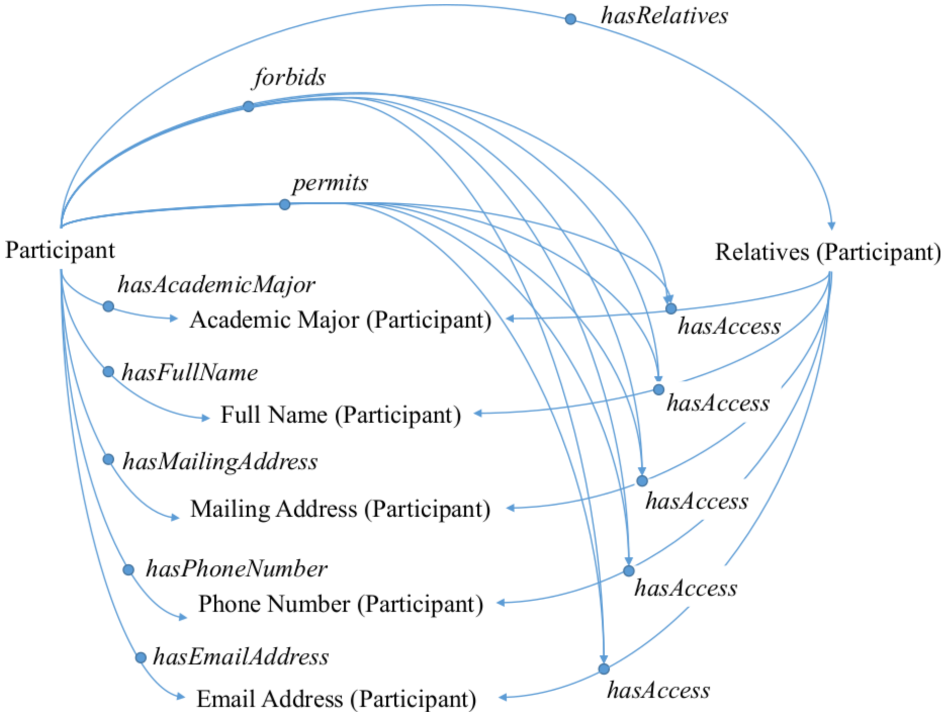


Figure C.11: Template for Question II.4a (Relatives).

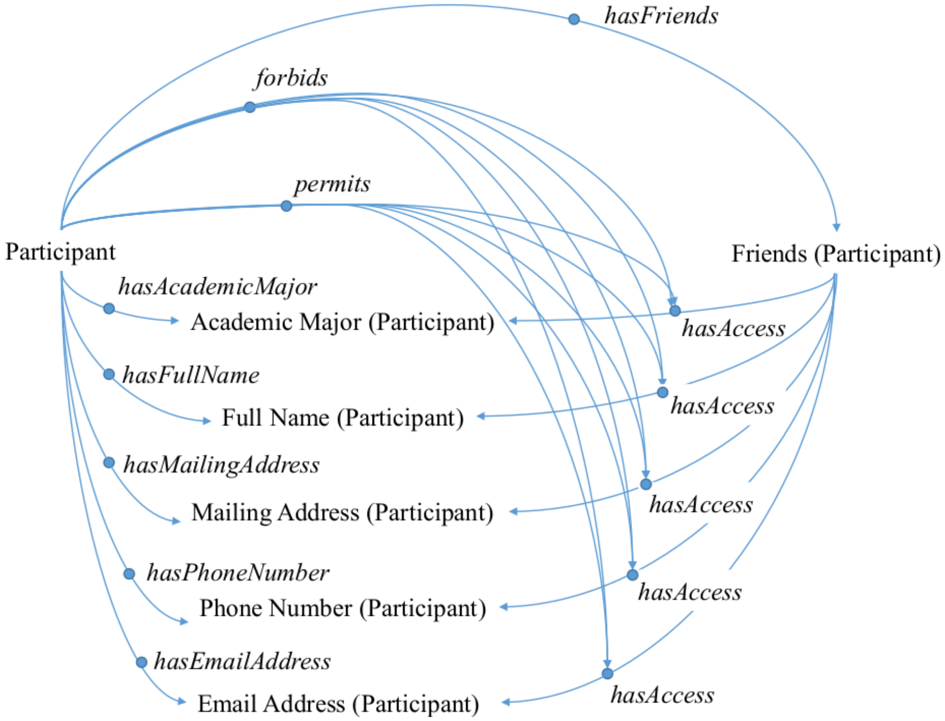


Figure C.12: Template for Question II.4a (Friends).

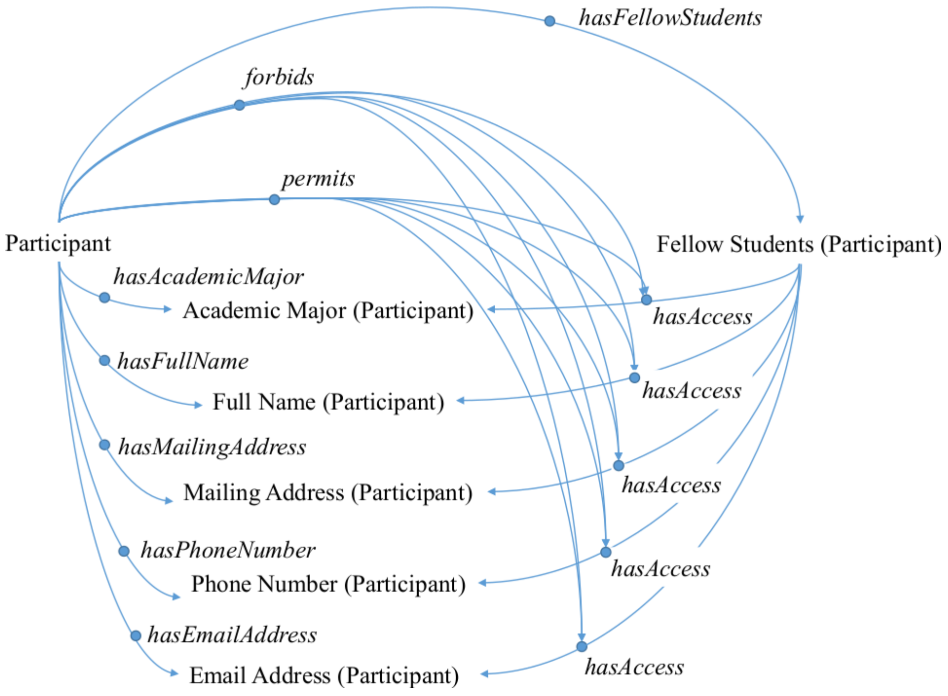


Figure C.13: Template for Question II.4a (Fellow Students).

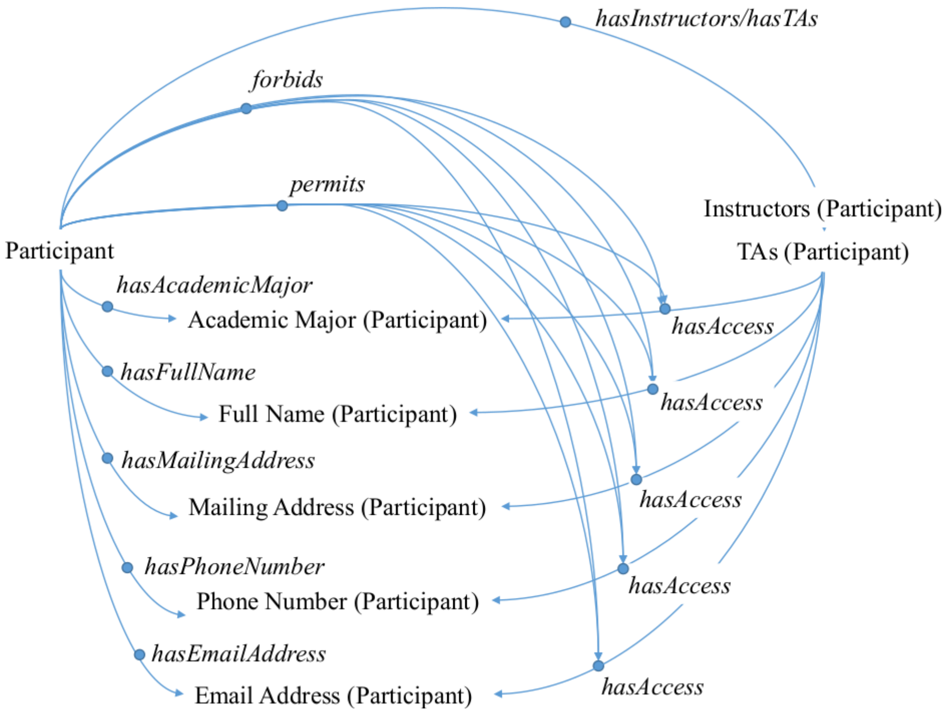


Figure C.14: Template for Question II.4a (Instructors and TAs).

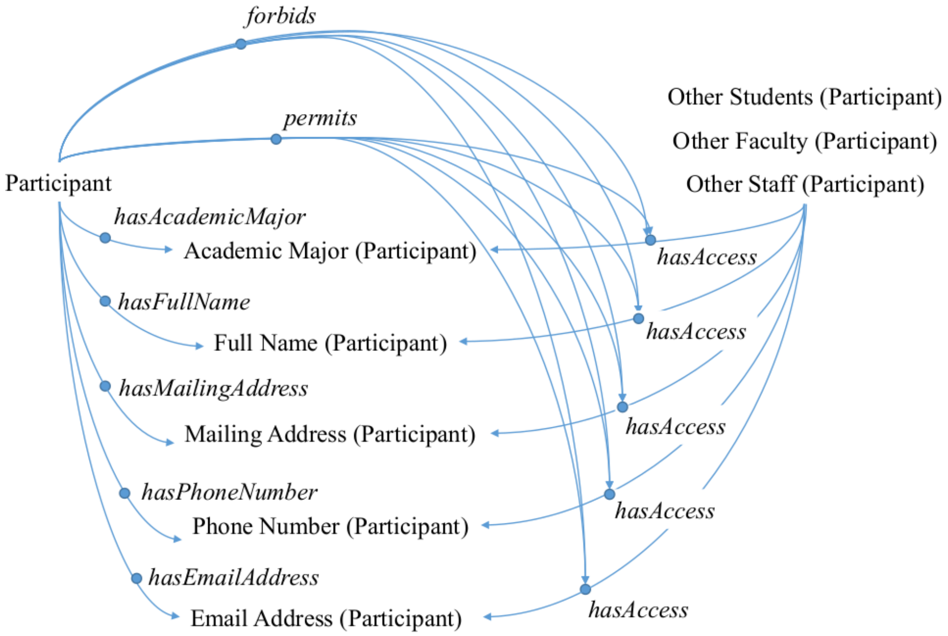

forbids
permits
Participant
Other Students (Participant)
Other Faculty (Participant)
Other Staff (Participant)
hasAcademicMajor
Academic Major (Participant)
hasAccess
hasFullName
Full Name (Participant)
hasAccess
hasMailingAddress
Mailing Address (Participant)
hasAccess
hasPhoneNumber
Phone Number (Participant)
hasAccess
hasEmailAddress
Email Address (Participant)
hasAccess

Figure C.15: Template for Question II.4a (Other Students, Faculty, and Staff).

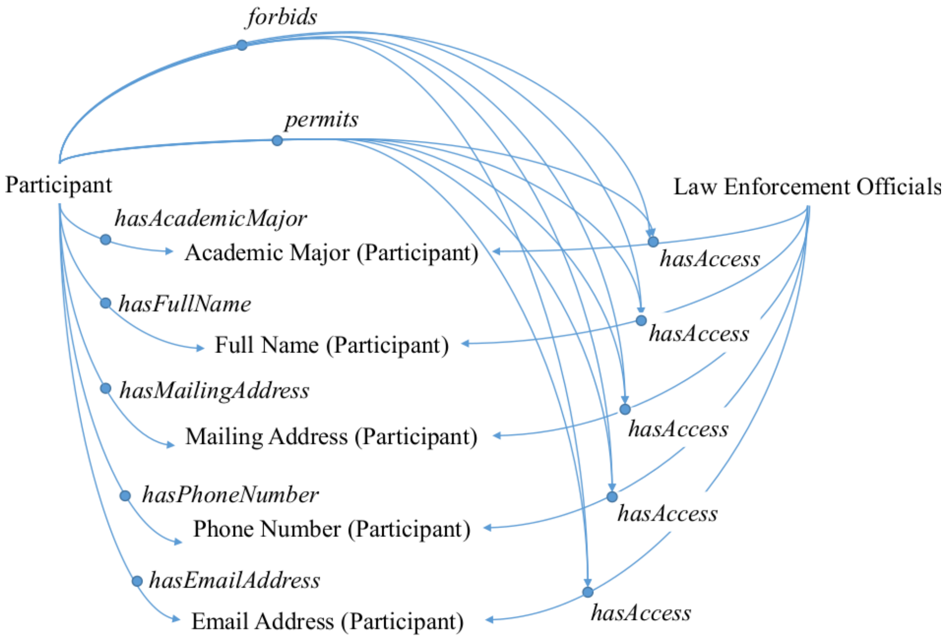


Figure C.16: Template for Question II.4a (Law Enforcement Officials).

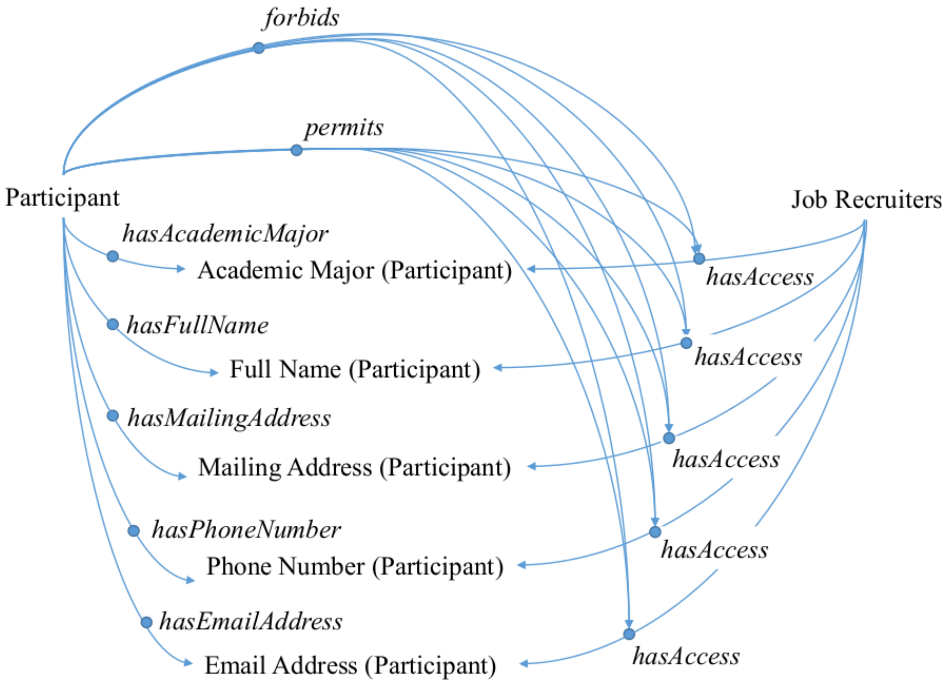


Figure C.17: Template for Question II.4a (Job Recruiters).

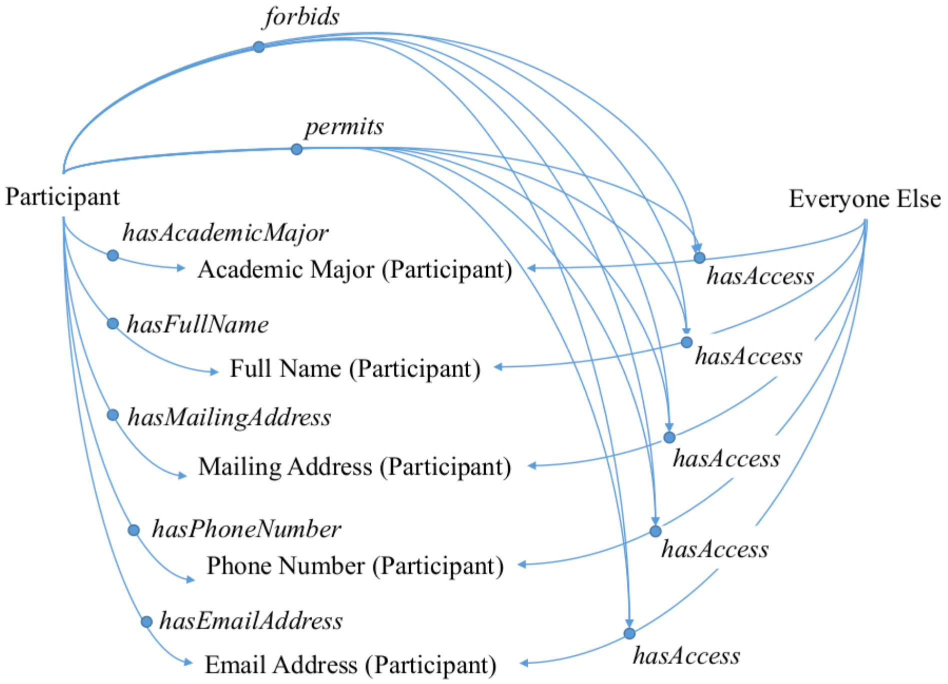


Figure C.18: Template for Question II.4a (Everyone Else).

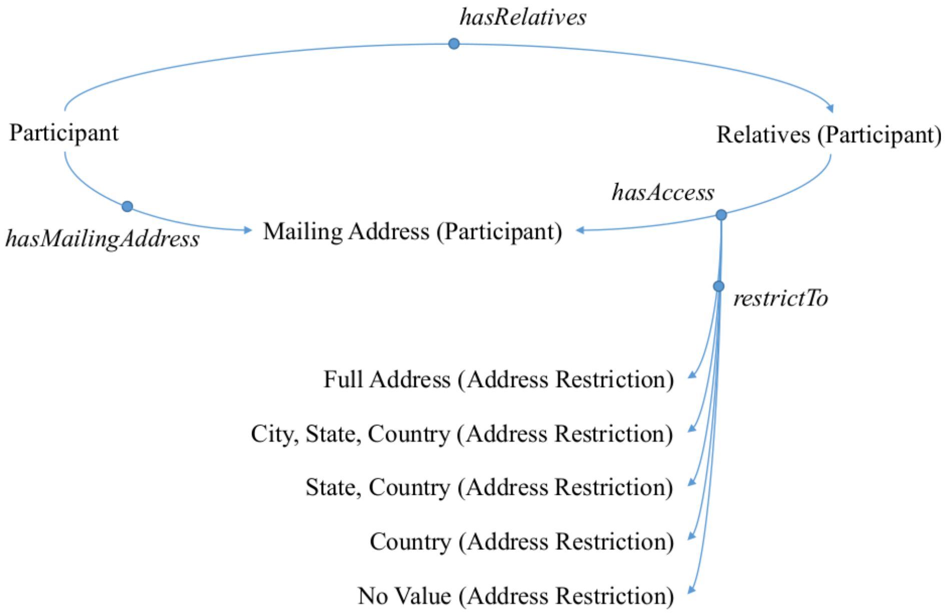

hasRelatives
Participant
Relatives (Participant)
hasAccess
hasMailingAddress
Mailing Address (Participant)
restrictTo
Full Address (Address Restriction)
City, State, Country (Address Restriction)
State, Country (Address Restriction)
Country (Address Restriction)
No Value (Address Restriction)

Figure C.19: Template for Question II.5a (Relatives).

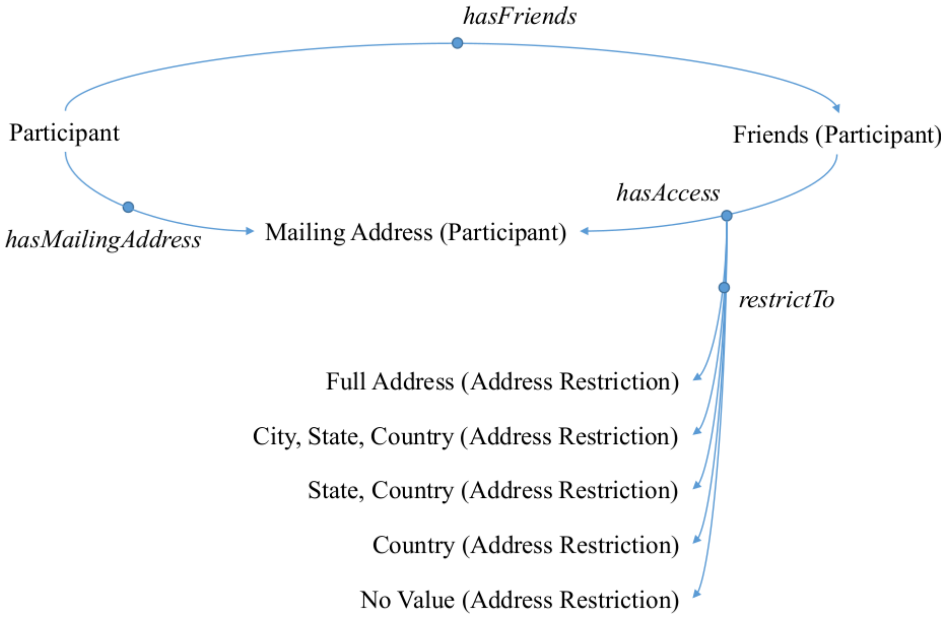

hasFriends
Participant
Friends (Participant)
hasAccess
hasMailingAddress
Mailing Address (Participant)
restrictTo
Full Address (Address Restriction)
City, State, Country (Address Restriction)
State, Country (Address Restriction)
Country (Address Restriction)
No Value (Address Restriction)

Figure C.20: Template for Question II.5a (Friends).

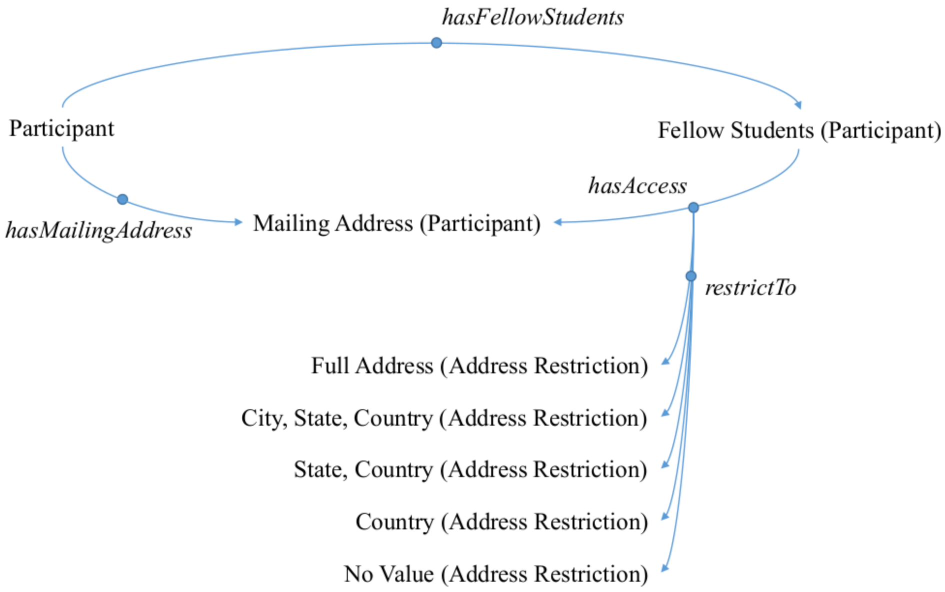

hasFellowStudents
Participant
Fellow Students (Participant)
hasAccess
hasMailingAddress
Mailing Address (Participant)
restrictTo
Full Address (Address Restriction)
City, State, Country (Address Restriction)
State, Country (Address Restriction)
Country (Address Restriction)
No Value (Address Restriction)

Figure C.21: Template for Question II.5a (Fellow Students).

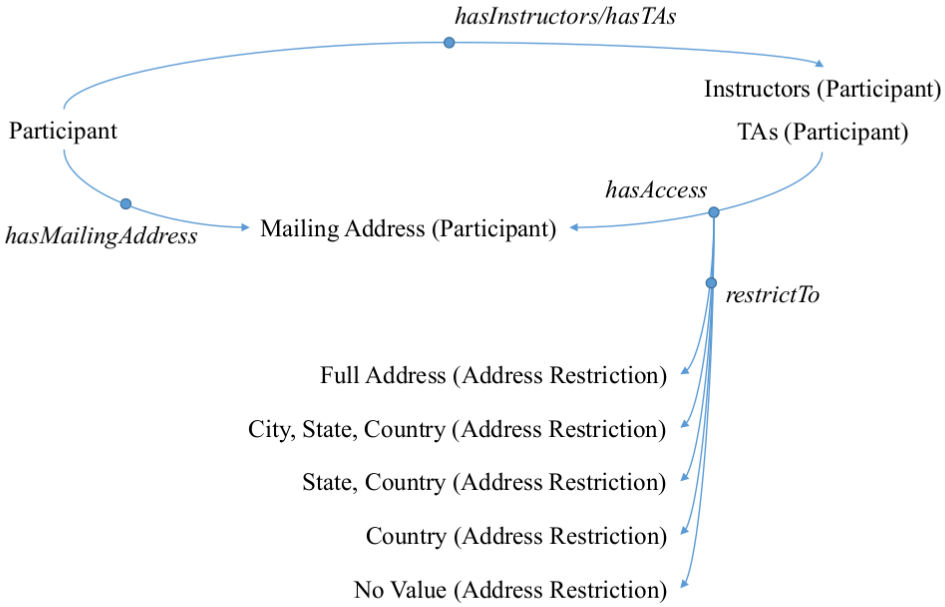

hasInstructors/hasTAs
Instructors (Participant)
Participant
TAs (Participant)
hasAccess
hasMailingAddress
Mailing Address (Participant)
restrictTo
Full Address (Address Restriction)
City, State, Country (Address Restriction)
State, Country (Address Restriction)
Country (Address Restriction)
No Value (Address Restriction)

Figure C.22: Template for Question II.5a (Instructors and TAs).

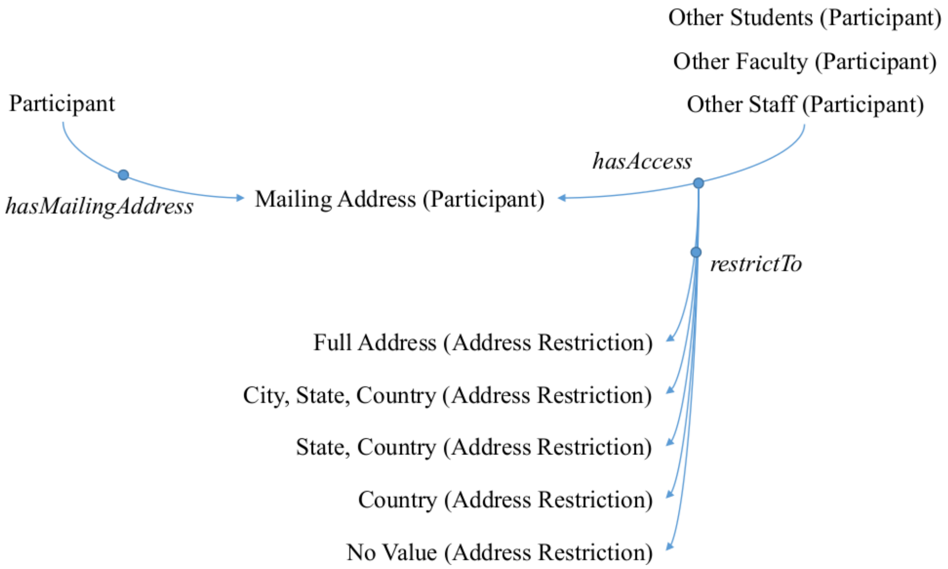

Other Students (Participant)
Other Faculty (Participant)
Other Staff (Participant)
Participant
hasAccess
hasMailingAddress
Mailing Address (Participant)
restrictTo
Full Address (Address Restriction)
City, State, Country (Address Restriction)
State, Country (Address Restriction)
Country (Address Restriction)
No Value (Address Restriction)

Figure C.23: Template for Question II.5a (Other Students, Faculty, and Staff).

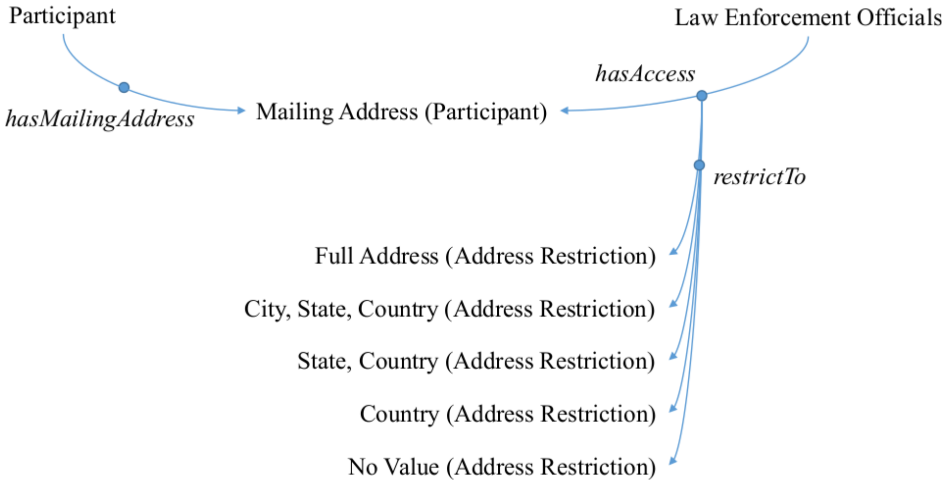

Participant
Law Enforcement Officials
hasAccess
hasMailingAddress
Mailing Address (Participant)
restrictTo
Full Address (Address Restriction)
City, State, Country (Address Restriction)
State, Country (Address Restriction)
Country (Address Restriction)
No Value (Address Restriction)

Figure C.24: Template for Question II.5a (Law Enforcement Officials).

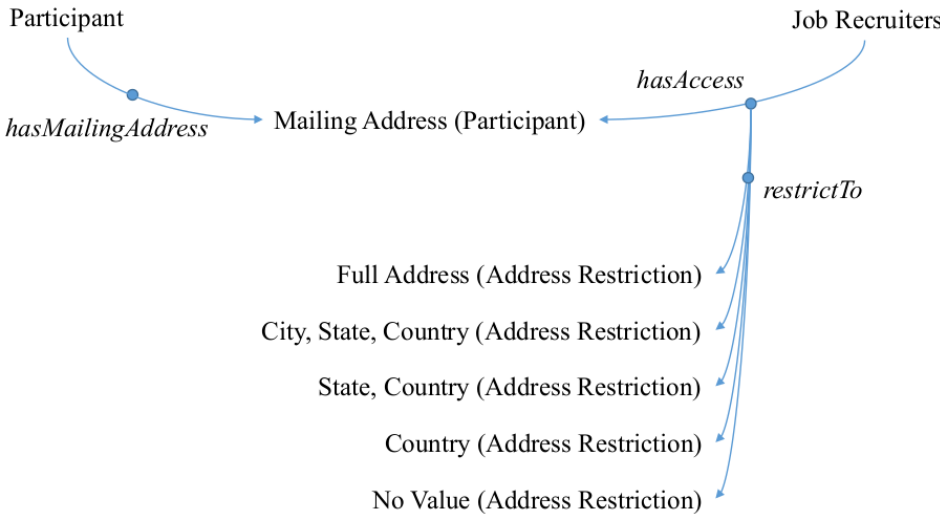

Participant
Job Recruiters
hasAccess
hasMailingAddress
Mailing Address (Participant)
restrictTo
Full Address (Address Restriction)
City, State, Country (Address Restriction)
State, Country (Address Restriction)
Country (Address Restriction)
No Value (Address Restriction)

Figure C.25: Template for Question II.5a (Job Recruiters).

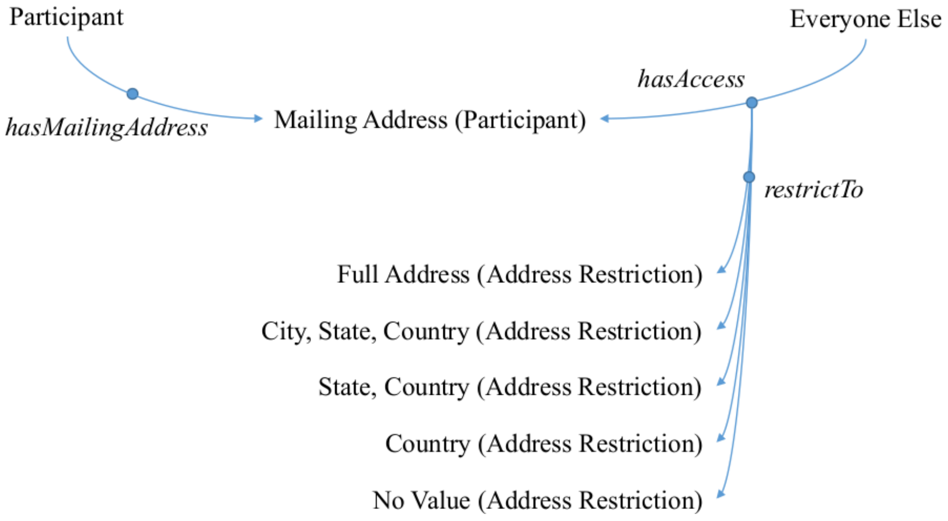

Participant
Everyone Else
hasAccess
hasMailingAddress
Mailing Address (Participant)
restrictTo
Full Address (Address Restriction)
City, State, Country (Address Restriction)
State, Country (Address Restriction)
Country (Address Restriction)
No Value (Address Restriction)

Figure C.26: Template for Question II.5a (Everyone Else).

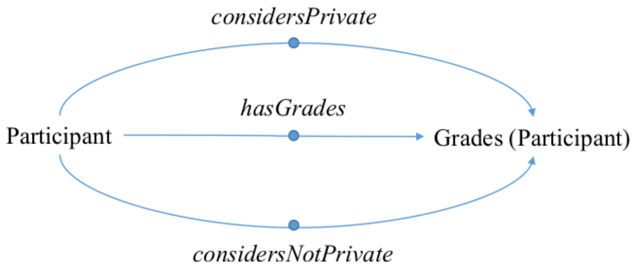


Figure C.27: Template for Question III.1.

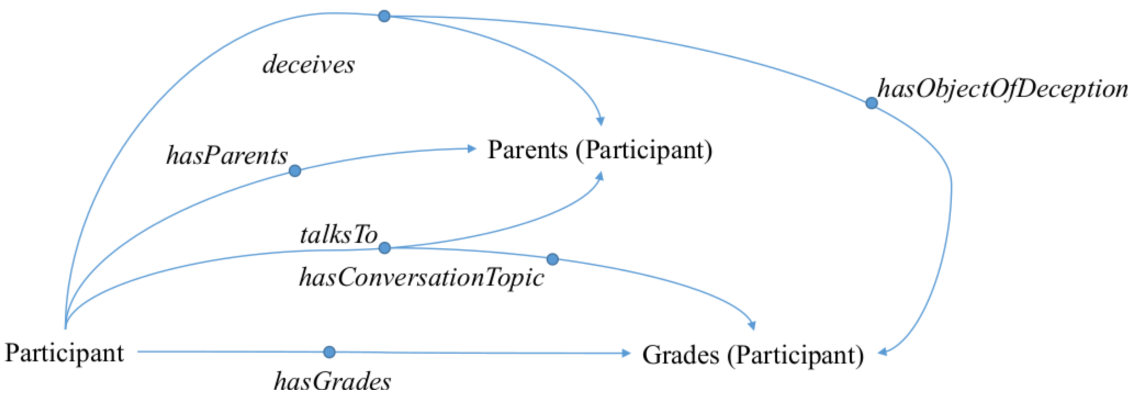


Figure C.28: Template for Questions III.2a and III.3a.

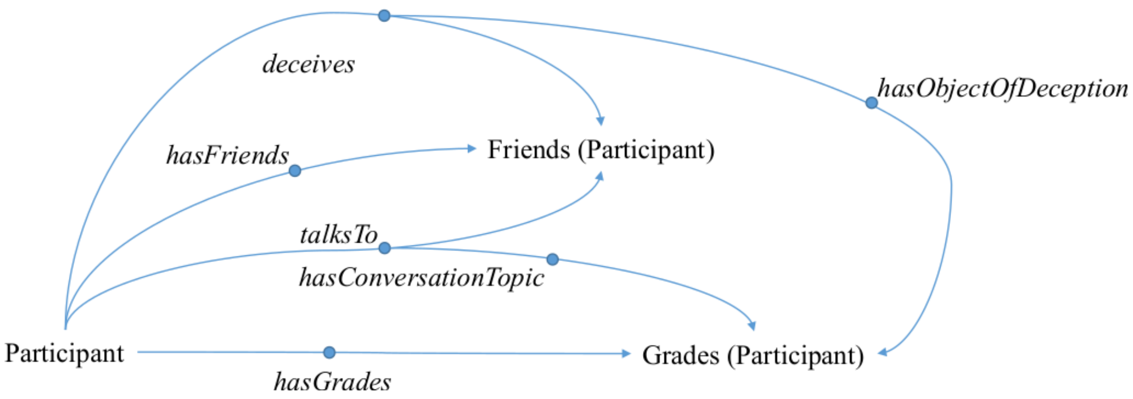


Figure C.29: Template for Questions III.2b and III.3b.

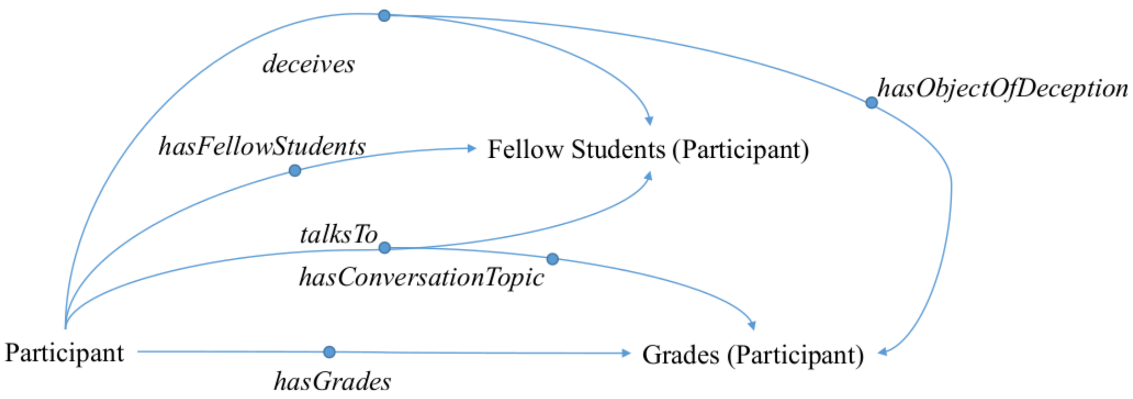


Figure C.30: Template for Questions III.2c and III.3c.

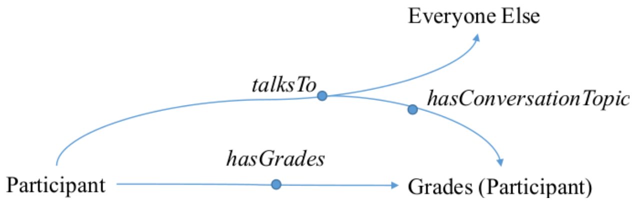


Figure C.31: Template for Question III.2d.

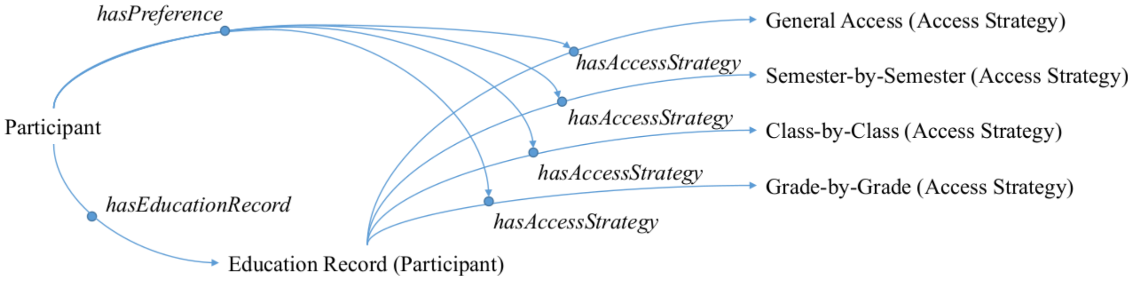

hasPreference
General Access (Access Strategy)
hasAccessStrategy
Semester-by-Semester (Access Strategy)
Participant
hasAccessStrategy
Class-by-Class (Access Strategy)
hasAccessStrategy
Grade-by-Grade (Access Strategy)
hasEducationRecord
hasAccessStrategy
Education Record (Participant)

Figure C.32: Template for Question III.5.

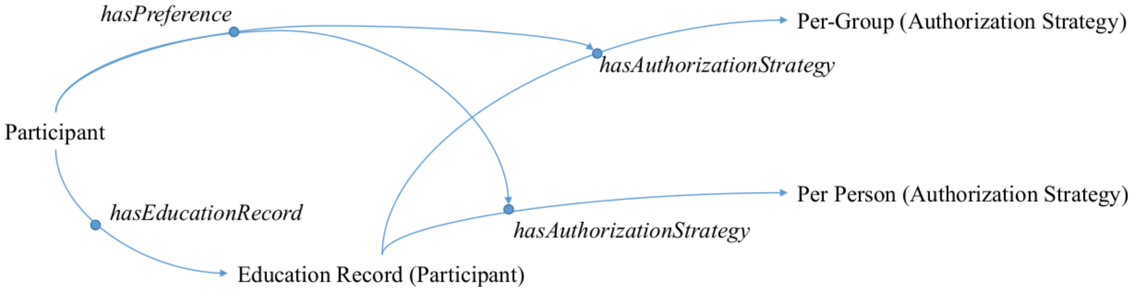

hasPreference
Per-Group (Authorization Strategy)
hasAuthorizationStrategy
Participant
Per Person (Authorization Strategy)
hasEducationRecord
hasAuthorizationStrategy
Education Record (Participant)

Figure C.33: Template for Question III.6.

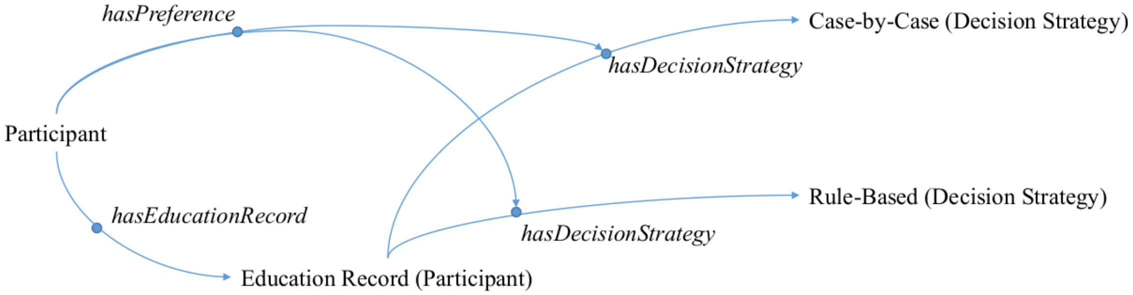

hasPreference
Case-by-Case (Decision Strategy)
hasDecisionStrategy
Participant
Rule-Based (Decision Strategy)
hasEducationRecord
hasDecisionStrategy
Education Record (Participant)

Figure C.34: Template for Question III.7.