An Individual’s Views of the Right to Privacy of Other Individuals, Companies, and Governments: A Theoretical Perspective

Justin Scott Giboney  
University of Arizona  
jgiboney@cmi.arizona.edu

David W. Wilson  
University of Arizona  
davidwilsonphd@gmail.com

Alexandra Durcikova  
University of Oklahoma  
alex@ou.edu

Abstract

This paper develops a theoretical model to help answer the following question—what influences an individual’s opinions regarding the right to privacy of others (individuals, organizations, and governments)? This question is particularly relevant for organizations and governments, for whom insider threats to corporate or government privacy present a dangerous risk. We draw from three bases of literature (human rights, privacy, and transparency) to theorize several constructs that should account for individual attributions of another’s right to privacy. In addition, we differentiate between individual, company, and government right to privacy, justify different origins of these entity types’ right to privacy, and propose different effects on these entity types from predictors in our model. The model presented here is the first of its kind in the IS literature, and lays the groundwork for future contributions in academic research and greater understanding relevant to practitioners.
Introduction

Who is entitled to privacy? The answer to this question has generated substantial debate for decades, and has received particular attention in light of recent events such as Edward Snowden’s leak of documents detailing NSA surveillance practices. Privacy is typically defined as the “ability to control information about oneself” (Bélanger & Crossler, 2011). This internal, individual-centric view has been studied extensively within the information systems (IS) discipline. In this paper, we argue that given these recent events it is also important to address an externally focused view—one that examines individuals’ perceptions of another person’s or organization’s right to privacy.

An externally focused view allows us to expand our focus beyond the individual to other entities such as companies or governments, a shift that has been called for in recent literature (Smith, Dinev, & Xu, 2011). Individuals typically desire a right to privacy to keep some information hidden from others. Likewise, companies also like to keep some of their information (e.g., technological or process advancements) private to retain an advantage over competitors. Governments also desire to maintain some level of control over the information that they release to the public, especially military, espionage, and national security operations. This paper will examine individuals’ underlying beliefs about why or why not other individuals, companies, or governments have a right to privacy.

Just like individuals, organizations and governments are at significant risk for privacy invasions in the form of insider threats—trusted members of an organization who compromise security—and such threats are often regarded as the greatest cyber security threat to organizations (Holmlund, Mucisko, Kimberland, & Freyre, 2010; Holmlund, Mucisko, Lynch, & Freyre, 2011). The insider threat problem presents an important motivation for understanding
differences in individual beliefs regarding others’ right to privacy. Edward Snowden, for example, was able to leverage his considerable expertise to develop rapport and gain access to classified information within the NSA. One can see how his actions may have been motivated by a belief in the necessity of information transparency, i.e., the public’s “right to know,” and that he may have decided against the NSA’s right to maintain privacy regarding its surveillance operations. There is clearly an opportunity for academics and organizations to better understand why individuals decide that others do or do not deserve a right to privacy. Further, organizations may be able to create controls to prevent future privacy violations. To explore issues related to privacy rights of others’, we seek to answer the following question:

What influences an individual’s opinions regarding the right to privacy of others (e.g., individuals, companies, governments)?

In answering this research question, we expand the concept of individual right to privacy to company and government rights to privacy, as perceived by an individual. Accordingly, we make two important contributions. First, we build on the IS privacy literature to include an individual’s evaluations of another’s privacy, focusing specifically on differences in evaluations of other individuals, organizations, or governments. Second, in order to adequately account for differences in human rights attributions, we incorporate the perspectives of other disciplines to provide a unique and more holistic theoretical model.

We will continue the paper by introducing our theoretical model and providing propositions. We will then conclude by discussing implications for research and practice.
Theoretical Model

Because the concept of privacy is complex, it is useful to study it via several lenses. To guide our theorizing about an entity’s rights to privacy, we draw on three literatures that inform us about human rights, privacy, and corporate and government transparency. The human rights literature is an essential perspective to incorporate because it provides understanding regarding why an individual supports or opposes freedoms for another individual. The privacy literature (which is predominantly focused on evaluations of one’s own privacy) provides a foundation for evaluating privacy of others. The transparency literature provides relevant understanding regarding why and whether individuals believe governments should be open and accessible. Incorporating these three lenses, we introduce a theoretical model to study the antecedents of other entities’ right to privacy (see Figure 1). We will begin our theoretical discussion on the right side of the model—an entity’s right to privacy—and then discuss each of the antecedents in turn.

Right to Privacy

People have long had the desire to be left alone if desired, and laws have been established to give people a right to privacy (Dawes, 2014). There are many legal nuances regarding what it means to have a “right” to privacy, but we will adapt an academic definition (Bélanger & Crossler, 2011) and define privacy as an entity’s right to control information about itself. Recent events, such as the Edward Snowden case, have forced us to look at privacy from the standpoint of not only the individual but also companies and governments. While the concept of privacy within the IS literature is generally studied at the individual level (Bélanger & Crossler, 2011; Smith et al., 2011), we expand our focus to include other entities, such as a company or a
government. We thus leverage the literature related to individual privacy to better understand privacy as it relates to companies and governments. As we are interested in the individual perceptions about other entities’ rights, we define our dependent variable as an individual’s belief that another entity has the legal or moral protection to control information about itself. As discussed below, we argue that, compared to individuals, companies or governments will be perceived as having different rights regarding privacy.

Culturally and legally, society makes distinctions between individuals, organizations, and governments regarding their privacy-related rights (see Table 1). The rights to privacy for these three different entity types are rooted in different concepts. Individual privacy is essentially derived from the individual’s inherent right, freedom, or privilege to privacy (similar to freedom of speech or religion). In contrast, corporate privacy is derived from legal protections of free market competition (e.g., a company maintaining competitive advantage by not sharing their detailed product designs) (Grossman, 1982). Government privacy is derived from the desire to ensure national security (e.g., CNN Staff, 2013).
Following the arguments in the preceding paragraphs, we argue that individuals will report different opinions regarding individual vs. other entities’ rights to privacy, and that these
different entities have to be investigated separately. We further argue that antecedents to these dependent variables will be different depending on the type of entity being considered. Accordingly, the relationships discussed within the model are presented as separately influencing opinions regarding individuals’ vs. companies’ vs. governments’ rights to privacy.

\[ P1. \text{Individuals perceive the rights of an individual differently than the rights of an organization and differently than the rights of a government.} \]

In the next section, we will explore how these perceptions about rights to privacy play out given a set of beliefs and individual might have about human rights, privacy, and transparency.

**Human Rights Literature**

Since we are theorizing about an individual’s perceptions about other entities’ (including other individuals) right to privacy, we draw upon the human rights literature that has explored some antecedents to general human rights perceptions, of which rights to privacy are a part. Within the human rights literature we are focusing on one major antecedent to the perception of human rights: political conservatism. Political conservatism is typically connected with, and significantly associated as a predictor of, the restriction of human rights (Crowson & DeBacker, 2008; Crowson, 2004). Political conservatism, with two sub-dimensions of right-wing authoritarianism and social dominance orientation, are important predictors of one’s perceptions about another human’s rights (Crowson & DeBacker, 2008; Crowson, 2004). The first element of political conservatism is the amount that an individual opposes change or desires to maintain social or political order (i.e., orthodoxy) (Jost, Glaser, Kruglanski, & Sulloway, 2003; Narvaez, Getz, Rest, & Thoma, 1999). This element is typically captured by right-wing authoritarianism (Jost et al., 2003). The second element is the extent to which an individual believes that societies
will be unequal, typically involving economic inequality (Jost et al., 2003). We will now provide background on both of these elements.

Right-wing authoritarianism is typically displayed by individuals reporting political conservatism (Jost et al., 2003). Right-wing authoritarianism is formally defined as the degree to which an individual (a) is submissive to authorities, (b) is aggressive towards those opposed to authorities, and (c) adheres to social conventions (Altemeyer & Hunsberger, 1992; Altemeyer, 1981; Jost et al., 2003). Right-wing authoritarianism has been effective in capturing the submissive crowd (Altemeyer, 1996). Because a more submissive person will obey an authority figure and because of the belief that such obedience is good for society, those with high right-wing authoritarianism are more likely to be accepting of privacy rights restrictions in general. Specifically, an individual with high right-wing authoritarianism will likely believe that those in authority (governments and companies) have the right to privacy, while others (individuals) do not. Formally we state,

\[ P2a. \text{Those scoring high in right-wing authoritarianism will attribute governments and companies higher rights to privacy, while attributing individuals lower rights to privacy.} \]

The second element, social dominance orientation, conceptualizes human rights as being part of a social hierarchy (Cohrs, Maes, Moschner, & Kielmann, 2007; Jost et al., 2003; Pratto, Sidanius, Stallworth, & Malle, 1994). Social dominance orientation is “the extent to which individuals support hierarchy-enhancing or hierarchy-attenuating ideologies” (Cohrs et al., 2007, p. 444). For example, someone high in social dominance orientation believes that some people, such as the upper class, are more worthy than others, such as the working class. Social dominance orientation is associated with the restriction of rights as people high in social dominance orientation believe that social control is necessary to curb deviant behavior (Cohrs et
al., 2007). Specifically, an individual with high social dominance orientation will likely believe that people and companies will need to give up more privacy for the good of society, while governments will have strong rights to privacy.

\[ P2b. \text{ Those scoring high in social dominance orientation will attribute governments higher rights to privacy, while attributing companies and individuals lower rights to privacy.} \]

Privacy Literature

The privacy literature provides a foundation for studying individual perceptions regarding privacy. A majority of the IS privacy literature has focused exclusively on perceptions of privacy at the individual level (Bélanger & Crossler, 2011; Smith et al., 2011). While our externally focused dependent variables (regarding privacy rights of others) deviate from the standard IS privacy perspective, we still focus our model on individual perceptions. Thus, we can leverage several relevant independent variables from within the privacy literature to help account for differences in our dependent variables. These include prior invasions to the individual’s privacy (Smith, Milberg, & Burke, 1996) and the general awareness of the individual to privacy-related practices (Cespedes & Smith, 1993; Malhotra, Kim, & Agarwal, 2004). In addition, we introduce two privacy-related concepts that should have particular relevance to our context—the extent to which the person is able (i.e., has the necessary technical skills) to invade others’ privacy, and the extent to which the individual believes that the target entity has engaged in privacy-invading practices in the past. Each of these factors will be introduced in the section that follows.

Individuals vary in the extent to which they are aware of privacy issues and to which their behavior is affected by concerns regarding privacy (Smith et al., 2011). A common predictor
accounting for these differences in individual concerns about privacy is whether the individual has been the victim of a prior invasion of privacy. These prior invasions of privacy, labeled *privacy experiences* in the literature (Smith et al., 2011, 1996), tend to greatly increase a user’s wariness regarding the collection and use of personal information (Culnan, 1993; Smith et al., 1996; Stone & Stone, 1990; Wilson & Valacich, 2012).

We can also consider the potential impacts of privacy experiences on individual perceptions of other entities’ right to privacy. Prior victims of privacy invasion are more sensitive to privacy issues and should be more likely to desire protection against future invasions. We argue that because victims are more sensitive to privacy issues in general they will additionally produce more positive statements regarding others’ rights to privacy. Further, these effects should be consistent regardless of whether an individual’s, company’s, or government’s right to privacy is being assessed. We explore this conjecture with the following proposition:

*P3a: An individual’s prior experience with privacy violation will positively impact the individual’s attributions of other entities’ rights to privacy.*

In addition to prior invasions to an individual’s privacy, an individual’s awareness of privacy-threatening practices (e.g., company collection of personal data) can increase concerns about privacy (Cespedes & Smith, 1993). Privacy awareness also refers to the extent to which the individual is apprised of recent privacy violations or privacy news in general (Malhotra et al., 2004). Such privacy awareness would mean the individual is more aware of the potential dangers of privacy invasion. We argue that this awareness would also cause the individual to defend other entities’ rights to privacy, again regardless of entity type. This assumption is operationalized in the following proposition:
P3b: An individual’s privacy awareness will positively impact the individual’s attributions of other entities’ rights to privacy.

One’s ability to invade privacy is the extent to which an individual has the technical skills needed to hack into systems and gain access to private information. Drawing from the self-efficacy literature (Bandura, 1991), we can infer a relationship between an individual’s belief in his/her ability to perform some behavior and the attitudes he/she forms regarding the appropriateness of that behavior. People tend to view positively those behaviors at which they are more proficient (Bandura, 1991). Thus individuals who have the skills necessary to invade the privacy of another entity will generally have higher approval of such invasion. The resulting effect is a negative effect on the ratings of another entity’s right to privacy. We thus state:

P3c. An individual’s high rating in ability to invade privacy will negatively impact the individual’s attributions of other entities’ rights to privacy.

There are times when the public finds out about someone or some organization that has violated the privacy rights of another. One recent example of this is the revelation regarding the NSA’s surveillance and gathering of phone records of American citizens (among others). When this was discovered, many expressed a general sentiment regarding a reduction in the NSA’s right to privacy, requesting that the agency reveal more specifically exactly what the agency has been collecting and why. Thus, if an entity has previously invaded others’ privacy, individuals will believe that the entity has given up a measure of its right to privacy. Therefore, we propose:

P3d. An individual’s perceptions of an entity’s prior privacy-invading behavior will negatively impact the individual’s attributions of privacy rights to that entity.
Transparency Literature

*Transparency* is the “degree of visibility and accessibility of information” (Zhu, 2004). There are four proposed benefits of transparency: 1) because people know their works and contributions are public, they will provide better quality products and services, 2) because people have access to the data of others, everyone can learn better, 3) because data, works, and contributions are public, it is easier to receive feedback to improve themselves (Baltzersen, 2010), and 4) because data are public, people, organizations, and governments can be held accountable for their decisions (Birchall, 2012). Of course, transparency can be abused allowing people to use data for nefarious purposes. Therefore, the ideal of transparency rests on the assumption that people are trustworthy and will use the information appropriately (de Laat, 2010). We are studying one’s beliefs in the extent to which others (people, organizations, and governments) should be transparent, and this we call transparency beliefs.

Individuals with high transparency beliefs will be more likely to want their citizen’s right to access policy documents and records and request government transparency (Baltzersen, 2010). These individuals with high transparency beliefs will favor free access of information and proactive interactions between the organization and all stakeholders and therefore be in favor of organizational transparency (Baltzersen, 2010; Vaccaro & Madsen, 2009). Some individuals take transparency beliefs to the extreme and believe that all possible processes should be publically available and that there should be no more secrets, termed radical transparency (Baltzersen, 2010; Roberts, 2012). Thus, individuals with high transparency beliefs will be less likely to support an entity’s right to privacy because in their view transparency provides more benefits than risks. Formally stated,
P6. An individual with high transparency beliefs will decrease the right to privacy of any entity.

Implications for Research

The model presented in this paper lays the groundwork for future research in at least three ways. First, the IS community has recently called for research that addresses privacy issues in the context of groups such as companies and governments (Smith et al., 2011). In answer to this call, we provide an initial exploration of how individuals assign the right to privacy to individuals, companies, and governments. Future empirical research related to our theoretical model will help to build understanding at these additional, under-explored areas of privacy research.

Second, we introduce in this paper a unique and helpful lens through which researchers can examine privacy and security issues beyond the narrow focus of individual’s own privacy concerns or fears, which has been the focus of the majority of prior IS privacy research (Bélanger & Crossler, 2011; Smith et al., 2011). Our theoretical model draws from multiple disciplines to help us understand external attributions regarding privacy, allowing future researchers to answer questions about the consequences of privacy to others. This model is the first of its kind in the IS literature, and our hope is that future research can expand the model and validate its relationships empirically.

Finally, we have provided a general theoretical model that is testable using a wide variety of methodological approaches, including surveys, experiments, and qualitative methods. Surveys can be used to test relationships in our model across a broad population, which may be useful, for example, in understanding public opinions regarding governments’ rights to privacy.
Experiments could be used to carefully examine specific relationships in the model with maximal control. Such experiments may be the best way to confirm the different effects of one’s ability to invade an entity’s privacy or the entity’s past privacy invasions on the privacy rights attributed to various entity types. Qualitative methods such as interviews could also be employed to extract rich, in-depth understanding on the political and sociological issues presented in our model.

**Implications for Practitioners**

The ideas presented in this paper also have direct application in modern society. While previous IS research has largely focused on individuals’ perceptions regarding their own privacy, companies and other organizations, as well as governments within society, are also deeply concerned about protecting their privacy. With our focus on company and government rights to privacy, we hope to encourage future research that provides insight into these issues beyond the individual level. Second, the model proposed here will inform companies and governments with new ways regarding how to better protect themselves against privacy invasions. Insider threats are among the most significant threats to organizations’ security (Holmlund et al., 2010, 2011), and better understanding why or whether individuals believe that a given organization has a right to retain its privacy could prove highly valuable. Using such knowledge, organizations and governments can take steps to mitigate risks and better legitimize their right to privacy.

Finally, for governments and politicians, the theory presented here can help generate ideas on how to best engender positive evaluations regarding privacy from their citizens. Our model provides specific guidance regarding how political and sociological factors impact
individuals’ views regarding whether and to what extent a government deserves a right to privacy.

**Conclusion**

In this paper we have theorized various predictors of individual attributions of others’ rights to privacy, differentiating between individuals, companies, and governments. We theoretically justify different origins of these entity types’ right to privacy, and propose different effects from predictors in our model. The model incorporates three bases of literature (human rights, privacy, and transparency) to propose several factors that should explain why an individual does or does not believe another entity deserves a right to privacy. This question is particularly relevant for organizations and governments, for whom insider threats to corporate or government privacy present a dangerous risk. Empirical validation of the model proposed in this paper will lead to unique and valuable understanding regarding an important antecedent to breaches in privacy.

**References**


