A Framework for Comparing Privacy States

Alan Rubel
School of Library and Information Studies
Program in Legal Studies
University of Wisconsin-Madison
arubel@wisc.edu

Ryan Biava
Department of Political Science
Holtz Center for Science and Technology Studies
University of Wisconsin-Madison
biava@wisc.edu

Abstract

This paper offers a framework for analyzing and comparing privacy and privacy protections across (inter alia) time, place, and polity and for examining factors that affect privacy and privacy protection. This framework provides a way to describe precisely aspects of privacy and context and a flexible vocabulary and notation for such descriptions and comparisons. Moreover, it links philosophical and conceptual work on privacy to social science and policy work and accommodates different conceptions of the nature and value of privacy. The paper begins with an outline of the framework. It then refines the view by describing a hypothetical application. The paper concludes with an argument that the framework offers important advantages to privacy scholarship and for privacy policy makers.

Keywords: privacy, information privacy, comparative privacy, privacy policy

Introduction

There is a substantial popular concern about privacy in light of technological advances, greater sharing of information via social networks, and increased power of state and non-state actors to collect information about individuals and institutions. That concern coincides with a growing body of privacy scholarship spanning a broad range of disciplines. One area of inquiry concerns making comparisons of privacy and protections in different places or at different times, for example across national boundaries (Regan 2010; Bennett 1992; Altman 1977; Spiro 1971). A related line of inquiry concerns contextual factors that affect privacy protections and privacy rights. For example, whether the search of one's briefcase constitutes a privacy violation depends on the setting in which it occurs: an airport security zone, a public sidewalk, or elsewhere (Nissenbaum 2010). Although these lines of scholarship are important and growing, they are in their early stages. This paper seeks to advance the scholarship in making privacy comparisons by providing a framework and conceptual foundation for defining and identifying aspects of privacy and its context in order to better analyze privacy, privacy protections, and privacy rights.

The framework we provide accomplishes several things. First, and most important, it provides a way to describe with precision particular aspects of privacy and privacy's context. It also allows one to compare privacy in different settings according to variables such as time, location, and polity. To do so, it provides a flexible vocabulary and notation to facilitate such descriptions and comparisons. The framework provides, so far as possible, a morally neutral way of describing and comparing privacy states, and hence does not assume the answers to any questions about the moral importance of privacy in particular cases. Finally, the framework provides a way to link philosophical and conceptual work on privacy to social science and policy work by providing a tool for describing and comparing privacy that both instantiates aspects of the philosophical literature and can accommodate different conceptions of the nature and value of privacy itself.

Acknowledgements: Thanks to Ian Brown, Robert Streiffer, Marc Blitz, Scott Gehlbach, David Weimer, the participants of the Comparative Politics Colloquium at the University of Wisconsin-Madison Political Science Department, and three anonymous reviewers for iConference 2013 for their comments on the full version of this paper.
Rubel, A. & Biava, R. (2013). A framework for comparing privacy states. *iConference 2013 Proceedings* (pp. 85-90). doi:10.9776/13150

The paper begins with a discussion of a number of conceptions of privacy and privacy protections. It will argue that those conceptions are incomplete, fail to capture the full range of possibilities for the state of personal privacy, and do not allow for comparisons of privacy states. We offer instead a conception that focuses on privacy as a three-part relation between some individual or institution, some domain of information, and some other individual or institution with respect to whom the first has (or lacks) privacy. Put another way, the three-part relation is a general feature of privacy, and any privacy state (i.e., state of affairs regarding the privacy of some individual or entity) can be expressed in terms of that three-part relation. Rather than arguing for a particular conception of that relation, our view is compatible with a broad range of views about the nature and value of privacy. After setting forth this conception, we further specify the view by describing a hypothetical comparison across states.

Privacy and Context

Several things motivate this paper. One is scholarly interest in comparing the laws and norms protecting privacy across different states or countries. Relatedly, there are important questions surrounding the explanations for such differences. To understand how and why countries offer different types of privacy protections it will be useful to have a framework to systematically describe those differences. This interest in differences in privacy norms is manifest in recent scholarship focusing on privacy's *context*. In her recent book *Privacy in Context*, Helen Nissenbaum makes the case that privacy norms must be understood in terms of "contextual integrity." She argues that privacy losses are distressing when they violate informational norms, which is to say when they violate norms restricting flows of information. Important here is that those norms are "systematically related to characteristics of the background social situation."(Nissenbaum 2010, 129) She maintains that "disparities across societies, cultures, and historical periods may manifest in differences" in privacy and informational norms.(Nissenbaum 2010, 134–35) Despite this emphasis on the social factors affecting informational norms, Nissenbaum leaves to "empirical social scientists" the question of how societal and cultural factors give rise to privacy and informational norms.

This paper takes up the task of understanding privacy's context in three ways. First, it specifies several relevant aspects of any privacy context. Second, by imposing a structure on analyzing privacy it allows for comparisons across "societies, cultures, and historical periods" that may have different privacy norms, and allows one to analyze underlying causes of such differences. Thus, third, the framework provides a tool to predict what privacy norms will be and how they will change.

The View

The foundation of our framework is that any conception of privacy must account for three things that stand in some relation to one another. So, for example, Martijn Blaauw argues that privacy is fundamentally about some person or persons, some set of propositions about the first person, and some other person or persons who know, or do not know, the propositions in the set (Blaauw n.d.). On this view, in order to understand Zeke's privacy in health information, we must account not just for Zeke, but also for some set of propositions regarding Zeke's health (e.g., propositions regarding Zeke's medical history, physiological traits, habits, and so forth) and for some other person or persons who knows, or does not know each of the propositions regarding Zeke's health. The key point here is that simply describing Zeke as having or lacking privacy is incomplete without specifying the range of propositions regarding which he has (or lacks) privacy and the other persons with respect to whom he has (or lacks) privacy. This is important, for one will often have privacy in some respects but not others. Zeke may have privacy regarding the set of propositions concerning his health with respect to his coworker, but not with respect to his insurer. And he may lack privacy regarding the set of propositions concerning his health with respect to his insurer but retain privacy regarding the set of propositions concerning his reading habits with respect to his insurer. Understanding privacy as a three-part relation forces us to be specific.

A related account is proffered in (Rubel 2011). Like Blaauw, Rubel argues that privacy should be understood as a three-part relation, though he articulates the relevant parts differently. On this view any particular instance of privacy must involve some person or persons *P*, some domain of information *O*, and some other person or persons *Q*. And for *P* to have privacy regarding *O* with respect to *Q* is for *Q*'s ability to make reasonable particularized judgments about *P* regarding *O* to be limited (Rubel 2011, 278–79).

Important for our purposes here is that by understanding privacy as necessarily involving three parts, we can use an expression such as *POQ* to denote any privacy instance or privacy *state*.

The difference between the Blaauw account and the Rubel account concerns the nature of the privacy relation. On Blaauw's view, privacy is a knowledge relation. If we let *O* be the relevant set of propositions concerning *P*, on Blaauw's view, *P* will have privacy regarding *O* with respect to *Q* if, and only if, *Q* does not know the propositions in *O*. In contrast, on the Rubel account privacy is about reasonable, particularized inferences, such that *P* has privacy regarding *O* with respect to *Q* to the extent that *Q*'s ability to make reasonable particularized judgments about *P* and *O* is limited. Suppose, for example, that *Q* reads *P*'s medical record, which states that *P* has Lyme disease. It would under normal circumstances be reasonable for *Q* to make the inference that *P* has Lyme disease, and hence *P*'s privacy regarding her health information (*O*) decreases with respect to *Q*. However, because *Q* can make such judgments without actually knowing propositions within the domain *O*, the Rubel account will recognize some cases as privacy losses that Blaauw would not so-recognize. Returning to the Lyme disease example, if *P*'s medical record states *incorrectly* that *P* has Lyme disease, *Q*'s reasonable inference would be false. *Q* would *believe* that *P* has Lyme disease and *Q* would be *justified* in that belief, but the belief would be false. *Q* therefore does not *know* that *P* has Lyme disease (for one cannot know something that is false). On a knowledge account of privacy, such that *P*'s privacy regarding *O* with respect to *Q* decreases only if *Q* gains knowledge of *P* regarding *O*, *P*'s privacy regarding his health status with respect to *Q* would not decrease.

What is important, though, is that despite this disagreement about the particular nature of the privacy relation, both accounts understand privacy as involving a three-part, or *POQ*, relation. More strongly, understanding privacy as involving a three-part relation is compatible with any plausible account of the nature of the privacy relation. Consider two of the predominant views of privacy in the literature: first, that privacy is fundamentally about access to information, and second, that privacy is about control of information. On access accounts, privacy turns on whether others physically access, cognitively access, or have the ability to physically or cognitively access one's information. Thus, on access accounts, a person's privacy does not depend on whether one has the ability to prevent others from impinging her privacy.[1] On control views, one's having privacy depends on whether one has the ability to decide who can access information about her. So, one can lose privacy if information about her is dispersed (and hence out of her control), even if others do not or cannot actually access that information.[2] Notice, though, that on either type of view, we can articulate some person *P*, some domain of information *O*, and some person or persons with respect to whom *P* has privacy regarding *O*. On access views, *P* will have privacy regarding *O* with respect to *Q* if *Q*'s access to *O* regarding *P* is limited in the relevant way. On control views, *P* will have privacy regarding *O* with respect to *Q* if *P* has the power to control whether *Q* can access information in *O* regarding *P*.

Making Comparisons

Fixing a means of denoting privacy relations (*POQ*) allows us to describe one privacy state in isolation. However, there are two problems. First, it is crucial for understanding privacy and context to be able to compare privacy across, for example, time, technology, place, and other relevant variables. Once researchers can make those comparisons with some precision, empirical social scientists can begin to account for the causes of any differences. Second, there are different conceptions of privacy (e.g., control, knowledge, access), all of which we want to be able to compare. That is, we do not want to tie this model to any particular conception of the nature of privacy.

In order to accommodate this last problem, we can use terms to represent particular conceptions of privacy that might obtain in any *POQ* relation. Hence, let α represent an access account of privacy, and α_{POQ} represent a particular three-part privacy relation under that conception. Table 1 shows a standardized, but non-exclusive, set of terms to refer to four principal conceptions of privacy.

[1] Examples of access accounts include (Powers 1996; Allen 1988, 15; Gavison 1984, 349–50; Parent 1983, 269).

[2] Examples of control accounts include (Moore 2010; Westin 1967, 7; Rachels 1975)

Table 1
Privacy conceptions notation

Conception of Privacy	Associated Symbol
Access	α
Control	κ
Particularized Judgment	π
Knowledge	ν

Consider the case of *P*'s privacy regarding his health information. We might want to compare *P*'s privacy in that regard with respect to various entities. So, *P* likely has relatively little privacy regarding his health information with respect to his doctor, but he might have more privacy in this regard with respect to his neighbor. To represent this difference we will need to expand our formula. Let *P* denote Peter, O_1 denote medical information, Q_1 denote Peter's doctor, and Q_2 denote Peter's neighbor. In the normal case, the following will be true:

$$\alpha_{PO_1Q_1} < \alpha_{PO_1Q_2}$$

That is, Peter's privacy regarding his medical information with respect to his doctor will be less than Peter's privacy regarding his medical information with respect to his neighbor. Now, let O_2 denote Peter's gardening habits. The following will be true:

$$\alpha_{PO_2Q_1} > \alpha_{PO_2Q_2}$$

That is, Peter's privacy regarding his gardening habits with respect to his neighbor will be less than Peter's gardening habits with respect to his doctor.

However, if Peter's doctor is the same person as Peter's neighbor, then:

$$\alpha_{PO_1Q_1} = \alpha_{PO_1Q_2}$$

And:

$$\alpha_{PO_2Q_1} = \alpha_{PO_2Q_2}$$

This example simply analyzes a single subject (*P*) across different domains (*O*) and third parties (*Q*). The framework, though, helps us describe privacy relations according to variables such as time and location. Consider, for example, records of persons' real property. In the U.S. municipalities' real property records are public records and anyone may access those records. Prior to the digitization of those records, the uptake of the Internet, and the move to place public records online, one generally had to make a request by mail, by fax, or in person to receive those records, and one generally had to pay for processing, photocopying, and postage. Now, in many places one can simply enter a person's name, a property address, or a parcel number in an online form and receive property records immediately and for free. We can represent this difference using our framework.

Let *P* represent a property owner in Greenacre, a municipality in the U.S. Let *O* represent information about real property (tax assessment value, property description, purchase price, encumbrances, and so forth). Let *Q* represent the general public. Suppose that in the pre-Internet era (T_1) Greenacre kept its property records in paper files, which could be accessed in person at City Hall during standard business hours, for a standard fee. However, as of 2010 (T_2) Greenacre keeps all of its property records in an electronic database, which may be accessed by members of the public on the city's website free of charge.

We can easily see, in Table 2, the relation between privacy in Greenacre before and after the database.

Table 2
Privacy state comparison across time

Variable	T_2 T_1
Privacy relation	$\alpha_{POQ} > \alpha_{POQ}$

We can replace the table by modifying the notation, including not only the privacy relation α_{POQ}, but also adding the relevant variable, in this case time (*T_1* and *T_2*). Hence, we can represent the overall privacy relation of a property owner regarding information about her property with respect to the general public as follows:

$$\alpha_{POQ}^{T_1} > \alpha_{POQ}^{T_2}$$

We can also construe the change at Greenacre as a change in technology rather than as a change in time. That is, we can analyze it as the difference between paper-based records and digitized, online records, represented slightly differently:

$$\alpha_{POQ}^{Paper} > \alpha_{POQ}^{Digital}$$

Indeed, a similar notation can be used to represent whatever comparison one wishes to make. So, rather than comparing privacy in Greenacre over time or across technologies, we might instead wish to compare privacy regarding property information between Greenacre and Blueacre. If Blueacre, even at this late date, has not created an Internet-accessible electronic database of its property records, the following would represent property owner privacy in the two locales:

$$\alpha_{POQ}^{Blueacre} > \alpha_{POQ}^{Greenacre}$$

We can also combine them:

$$\alpha_{POQ}^{Blueacre \cdot T_1} = \alpha_{POQ}^{Greenacre \cdot T_1}$$

Whereas:

$$\alpha_{POQ}^{Blueacre \cdot T_2} > \alpha_{POQ}^{Greenacre \cdot T_2}$$

Hence, the framework here specifies and isolates aspects of privacy's context, and is flexible enough to account for different variations. These include, but are not limited to, place, time, and technological developments.

Toward Social Scientific Explanation of Variance

This type of structured, rigorous analysis encourages us to look at privacy relations within specific situations: in particular places or times, or under various technological conditions. Once this work is complete, social scientists – and indeed all those who seek to determine the reasons behind the variations elicited – can treat the resulting privacy comparisons as bases for further research.

For instance, once the privacy comparison related to presidential campaigns in the US and France presented above is established, scholars can seek to explain the causal factors behind the differences. It may well be that France's political culture has been so influenced by the presence of a centralized, powerful state that its government is more likely to demand a fuller accounting of donations from its candidates. By comparison, Americans' tendency toward skepticism, antagonism toward state action, or affinity for small-scale political actors may contribute to the exclusion of sub-$200 donations from federal reporting requirements.

We can also imagine any number of further applications and comparisons, depending on the interest of the social scientist or other analyst. Perhaps computer scientists, information scientists, and designers of technological systems will wish to evaluate the privacy impacts of existing technologies with an eye toward predicting privacy outcomes of future technologies (see, e.g., Detweiler et al. 2011). Or sociologists may wish to look into the past to compare privacy states under various social regimes in order to make predictions about societal outcomes. Others may wish to examine privacy regimes in various historical periods to identify causes of differences in privacy protections.

Conclusion

Our task here has been to advance privacy inquiry by providing a bridge between several discrete areas of privacy scholarship: work emphasizing the importance of privacy's context, philosophical work regarding conceptions of privacy, and empirical social science looking at differences in privacy regimes and underlying causes of such difference. To do so we've offered a framework and conceptual foundation for isolating aspects of privacy and privacy's context and for comparing other aspects of privacy's context: privacy is a three-part relation between some person, persons, or entity *P*, some set of propositions or domain of information *O*, and some other person, persons, or entity *Q* with respect to whom *P* has privacy regarding *O*.

We have argued that the framework is important insofar as it forces specification regarding these three necessary aspects of privacy and, hence, allows for comparing privacy across contexts such as time, location, and polity. Although it forces some specificity, it is flexible insofar as it allows comparisons of myriad contexts and accommodates different philosophical conceptions of the nature of privacy (access, control, knowledge, inference) and types of privacy protections (legal, moral, technological).

References

Allen, A. L. (1988). *Uneasy Access: Privacy for Women in a Free Society*. Totowa, N.J.: Rowman & Littlefield.

Altman, I. (1977). Privacy regulation: Culturally universal or culturally specific? *Journal of Social Issues 33*(3), 66–84.

Bennett, C. J. (1992). *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*. Ithaca: Cornell University Press.

Blaauw, M. (n.d.). Privacy and Knowing Who. *Journal of Social Philosophy* (forthcoming).

Citizens United v. Federal Election Commission, 558 U.S. 50 (2010).

DeCew, J.W. (1997). *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology*. Ithaca, N.Y.: Cornell University Press.

Detweiler, C., Pommeranz, A., Hoven, J., and Nissenbaum, H. F. (2011). Values in Design - Building Bridges Between RE, HCI and Ethics. In P. Campos, N. Graham, J. Jorge, N. Nunes, P. Palanque, and M. Winckler (Eds.), *Human-Computer Interaction – INTERACT 2011* (6949:746–747). Lecture Notes in Computer Science. Berlin: Springer.

Gavison, R. (1984). Privacy and the Limits of Law. In F. Schoeman (Ed.), *Philosophical Dimensions of Privacy* (pp. 346–402). Cambridge: Cambridge University Press.

Moore, A. D. (2010). *Privacy Rights: Moral and Legal Foundations*. University Park, Pa: Pennsylvania State University Press.

Nissenbaum, H. F. (2010). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, Calif.: Stanford Law Books.

Parent, W. A. (1983). Privacy, Morality, and the Law. *Philosophy and Public Affairs 12*(4), 269–288.

Posner, R. A. (1984). An Economic Theory of Privacy. In F. Schoeman (Ed.), *Philosophical Dimensions of Privacy* (pp. 333–345). Cambridge: Cambridge University Press.

Powers, M. (1996). A Cognitive Access Definition of Privacy. *Law and Philosophy 15*(3), 369–386.

Rachels, J. (1975). Why Privacy Is Important. *Philosophy and Public Affairs 4*(4), 323–333.

Regan, P. (2010). The United States. In J. B. Rule & G. W. Greenleaf (Eds.), *Global Privacy Protection: The First Generation* (pp. 50-79), Cheltenham, UK : Edward Elgar.

Rubel, A. (2011). The particularized judgment account of privacy. *Res Publica 17*(3), 275–290.

Spiro, H. J. (1971). Privacy in comparative perspective. In J. R. Pennock and J. W. Chapman (Eds.), *NOMOS XIII: Privacy* (pp. 121–148). New York: Atherton Press.

Westin, A. F. (1967). *Privacy and Freedom*. New York: Atheneum.