A Framework for Analyzing and Comparing Privacy States

Alan Rubel
Information School
Legal Studies Program
University of Wisconsin, Madison
arubel@wisc.edu

Ryan Biava
Department of Political Science
University of Wisconsin, Madison
biava@wisc.edu

Abstract: This paper develops 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. Finally, it applies the framework to a real-world privacy issue—campaign finance disclosure laws in the U.S. and in France. The paper concludes with an argument that the framework offers important advantages to privacy scholarship and for privacy policy makers.

1. 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 (Bellman et al. 2004;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.

Cite to revised and final version: Rubel, A. and Biava, R. (2014), A Framework for Analyzing and Comparing Privacy States. JASIST: Journal of the Association for Information Science and Technology, 65: 2422-2431. doi:10.1002/asi.23138.

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.

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. We then apply it to a real case, comparing campaign financing privacy in the U.S. and France. We conclude by arguing that this conception offers important advantages, by providing a common vocabulary, by not presupposing any particular view regarding the moral value of privacy, and by not making any assumptions about what sorts of entities can have privacy or have claims to privacy.

1.1. 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 approach we take will run counter to important threads in contemporary privacy scholarship, such as those arguing that privacy is a "concept in disarray" and that looking at unifying threads across aspects of privacy is not a fruitful endeavor (Solove 2005, 477). Recently, for example, Daniel Solove has argued that instead of looking at privacy per se, we should take a problem-based or pragmatic approach to analyzing privacy, looking first to issues or disputes before doing the conceptual work because "the attempt to locate the essential or core characteristics of privacy has led to failure" (Solove 2008, 8). Note, though, that many morally important concepts are disputed and have no universally agreed-upon "core"—rights, speech, law, property, justice, well-being, and health being just a few. Surely, though, it is worthwhile to hone our conceptions and we can make progress doing so; that's our task here.

Solove is right that we should look to particular disputes, but our approach is to use particular disputes about privacy (or rights, or speech, or law, etc.) as a way to refine our conceptions. Hence, looking at particular privacy disputes is part of a process of broad reflective equilibrium necessary for reasoning about moral and political principles, which in turn depend on, rather than undermine, core concepts. Broad reflective equilibrium, as described by John Rawls and developed by numerous others, uses concepts and principles coupled with considered judgments about particular cases to arrive at the best overall coherence between concepts, principles, and considered judgments (Rawls 1999; Daniels 1979, 258).[1] Our framework is based on considerations of particular disputes and conceptions of privacy, and it aims to incorporate those disputes and conceptions into a framework that can coherently accommodate a wide array of conceptions while also providing demarcation criteria for privacy. And while one might argue that such demarcation criteria are a problem that pragmatic conceptions seek to avoid, even pragmatic conceptions must deploy some conception of privacy and some set of relevance criteria. After all, one cannot write about privacy problems and disputes as *privacy* problems or disputes without some idea of what privacy is. Our framework seeks to make explicit just what those criteria are.

Moreover, it is an important task to compare systematically privacy and privacy protections across time, place, and polity, in the same way that researchers have made such comparisons regarding liberty, rights, and rule of law. Doing so requires operationalizing the thing to be compared, in this case privacy. But abandoning the attempt to draw a parsimonious conception of privacy forecloses our ability to do such empirical work. We need a model to study and evaluate different privacy regimes. That's our goal here.

The specificity provided by our framework can also be useful in developing indices measuring various aspects of privacy protections around the world. The ability to examine targeted areas of law and regulation represents a step along the way from rich, narrative accounts to more quantifiable descriptions. The framework allows pair-wise comparisons between countries, which can be compiled by researchers into rankings or indices. An analogous, well-known index, produced and updated

annually by Freedom House, measures democracy around the world (Freedom House 2013). Quantifying such a difficult and contested notion as democracy has contributed to the broader field of democratization and human rights studies. This has developed the field by encouraging meta-studies that audit the indices' performance over time (Gupta et al. 1994; Bollen 1993). Our framework cannot by itself result in the same outcome for privacy, but it does contribute to a literature that aims at comparison.

2. 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.[2] 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.[3] 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*.

Another view, prominent in the legal scholarship, abandons any attempt to articulate a single conception of privacy, instead maintaining that privacy is either a variety of things, or a cluster-concept, or a family-resemblance concept. This possibility can also be accommodated by the *POQ* framework. Solove (2002) argues that different conceptions of privacy are appropriately employed in different circumstances. For example, Solove maintains that a court's ruling that a newspaper did not violate a soccer player's privacy by publishing a photograph in which the player's genitalia were inadvertently exposed during a game mistakenly applied a *secrecy* conception of privacy, when a different conception (perhaps an access conception) would have been appropriate.[4] Similarly, he argues that courts' determinations that disclosure of information by third-parties to police does not constitute a search under the Fourth Amendment are the result of an inappropriate application of an *invasion* conception of privacy.[5] The idea is that there are lots of different ways in which privacy might diminish, and we cannot conclude that privacy has not diminished merely on the ground that one aspect of privacy has not diminished. Notice, though, that we can still denote privacy instances in our *POQ* formulation, even though privacy might involve secrecy, or invasion, or something else altogether. All we must do is

specify the particular privacy facet we are concerned about. So, if we are concerned with *secrecy*, the *POQ* relation will denote *P*'s maintaining secrecy regarding domain of information *O* with respect to all other *P*s. If we are concerned with invasion, *POQ* will denote *P*'s freedom from *Q*'s invasion of domain *O*, regardless of whether *O* is secret or not.

Put another way, despite the variation among philosophical conceptions of privacy, each can be understood in terms of a three-part relation. One must merely specify what the three-part *POQ* relation denotes (control, access, knowledge, particularized judgments, secrecy, and so forth). Below we suggest that each different conception of privacy should be represented by a different term in a function with *P*, *O*, and *Q*. For example, privacy as access can be represented as α_{POQ} . Thus, understanding privacy as a three-part relation internalizes and forces one to specify several necessary facets of privacy's context. As we will see below, this allows one to isolate, compare, and explain other aspects of contexts.

2.1. Individualistic conceptions, moral claims

With this framework in mind, it is worth clarifying two matters. First regards the type of entity that can have privacy. Generally, privacy claims are understood to attach to individuals. That is, privacy is typically understood as the ability of an individual to restrict flows of information about her to others.[6] There are a variety of reasons for that to be the case. One would be humanistic concerns about prioritizing humans versus non-humans or institutions. Another would be that, in the U.S. at least, legal protections for privacy are often stated in individualistic terms.

But it is by no means obvious that *only* individuals can have privacy or claims to privacy. Richard Posner, for example, argues that it is best (by which he means economically efficient) in many cases to allocate property rights in personal information—which is to say privacy rights—toward businesses rather than individuals (Posner 1984), as does Alan Westin (1967). In a recent case the U.S. Supreme Court determined that the personal privacy exemption under the Freedom of Information Act applies only to individuals, not to corporations.[7] Although that case affirmed privacy as attaching to individuals, the fact that a lower court determined that the privacy exemption applied to corporations, and the fact that the Supreme Court's ruling was based on statutory language (specifically referring to "personal" privacy) rather than the meaning of privacy simpliciter, suggest that it is at least plausible that institutions or groups can have privacy along with individuals.[8] Moreover, there are lots of ways in which law and social norms already protect information flows regarding institutions: government secrecy, trade secrets protections, work product protections under freedom of information laws, attorney-client privileges, and so forth. We see no a priori reason to preclude understanding these as privacy protections.

Second, the framework articulated here does not presuppose that privacy per se is valuable. Some conceptions of privacy build in value, either by understanding privacy as a right or as a realm that warrants protection from others' incursion (Moore 2010, 26–27). Understanding privacy as a three-part relation as in Blaauw or Rubel is compatible with privacy having some inherent value; the domain (*O*) would in those cases be limited to information to which persons (*P*) have some claim regarding or

information that is valuable to *P*. But the framework neither presupposes nor depends on privacy having value. Because our framework does not presuppose that privacy is valuable, it will not directly address important aspects of some other views. For example, Nissenbaum includes *transmission principles* in her contextual integrity view (Nissenbaum 2010, 145–147). Such principles, however, are norms governing information flows and, hence, norms governing whether privacy may justifiably diminish or not. Because the framework here simply describes different privacy states, it leaves aside such principles.

2.2. Making comparisons

Thus far, we've described different accounts of the nature of privacy and fixed a means of denoting privacy relations—*POQ*. That 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. The following is a standardized, but non-exclusive, set of terms to refer to four principal conceptions of privacy.

Conception of privacy	Associated symbol
Access	α
Control	κ
Particularized judgment	π
Knowledge	υ

Consider the case of patient *P*'s privacy regarding 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 health information with respect to their doctor, but *P* might have more privacy in this regard with

respect to neighbors. To represent this difference we will need to expand our formula. Let *P* denote a normal patient, O_1 denote medical information, Q_1 denote *P*'s doctor, and Q_2 denote *P*'s neighbor. In the normal case, the following will be true:

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

That is, normal patients' privacy regarding their medical information with respect to their doctor will be less than normal patients' privacy regarding their medical information with respect to their neighbors. Now, let O_2 denote gardening habits. Likewise, the following will be true:

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

That is, patients' privacy regarding gardening habits with respect to neighbors will be less than patients' gardening habits with respect to their doctors.

This example simply analyzes a single type of 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 the relation between privacy in Greenacre before and after the database with a simple table:

Variable	T_1 T_2
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.

3. A Case Study: Campaign Finance Regulation in the United States and France

The usefulness of the framework becomes clearer when we look at the settings in which privacy matters. One such setting is campaign finance. An important topic in any time, recent changes in U.S. law following the *Citizens United* case has made the politics of presidential campaign finance a particularly central issue to American politics (*Citizens United v. Federal Election Commission*, 2010).

The regulation of campaign finance – both the inflows to and outflows from campaign treasuries – revolves largely around two substantive areas: first, limitations on contributions and spending; and second, disclosure requirements regarding such receipts and spending of campaign funds.

We focus on the second area, providing a way to describe formally and to compare candidates' relative ability to keep confidential the information about campaign funding—a candidate's (*P*) privacy regarding campaign funding (*O*) with respect to third parties (*Q*). We compare the state of this privacy relation in the presidential campaigns in United States and France.[9]

Understanding this privacy relation is important for several reasons. First, the non-disclosure of donor information and the amounts they contribute to a campaign deprives other actors of information about systemic power relations within the polity. Consider the importance of learning about donations to a legislative candidate from a corporation regulated by a legislative committee chaired by that candidate. Second, information about finances not only affects election outcomes, but can also incentivize the official behavior of elected officials. Finally, privacy claims related to government action, including electioneering, have implications for the character of liberal democracy.

One way to undertake this type of assessment is to provide narrative, descriptive accounts of laws and regulation. That is where we begin. Then, we add to this narrative by deploying the framework we have established to make clear the comparisons of privacy.

3.1. Narrative account

In the United States, federal campaign laws and regulations are overseen principally by the Federal Election Commission (FEC). These laws require candidates for president to disclose the total amount of donations received from individuals. Disclosure of donor identifying information (including name, occupation, address, and employer) is required for those who contribute $200 or more to a campaign; for those contributing less, the campaign may keep confidential such identifying information.[10] All of the data disclosed to the state, in addition to being made available for inspection and enforcement actions by the FEC and any other relevant federal agencies, are also made available to the public via federal government[11] and third-party search engines.[12]

This differs from the situation in France in several ways. The French election regulation enforcement authority – the CNCCFP[13] – sets out rules on how campaigns must document both receipts and expenses.[14] These rules require that the campaign retain documentation (e.g., copies of checks, receipts issued for cash donations, credit card receipts) to prove to the government that the campaigns are not taking donations from non-physical persons; corporate (i.e., non-personal) donations are forbidden by law.[15] Additionally, the CNCCFP requires campaigns to compile and submit a list containing the name of all donors and the amount each contributed.

Following each election, the CNCCFP audits the required documentation of the campaigns, and issues an activity report. In years where presidential elections have taken place, this annual report contains donation totals by individuals, but the government does not make donor information available to the public. Members of the public may request, in writing and for a standard copying fee, the summary donor lists filed by the campaigns, but the CNCCFP redacts all names and other identifying information of donors prior to releasing the list.

There is, therefore, a general similarity in individual donation disclosure requirements with respect to governmental authorities, in this case the FEC and CNCCFP. However, American presidential candidates' campaigns have more privacy regarding the identity of their donors than similarly situated French candidates, given the sub-$200 donor exception. Both countries do require individual donor information for all donors over $200. As to public disclosure, France differs in that it demands, but does not disclose to others, all individual donors' names. The public and the press, in France, are deprived of the

individual names, whereas their American counterparts are given access to significantly more information about which individuals and interests exert financial influence within presidential election campaigns.

3.2. Applying Our Framework

The narrative account provides an overview of similarities and differences between the two countries with respect to this privacy claim. Our model can parsimoniously present this information in the following way.

Let us examine, first, overall privacy for American and French presidential campaigns. Let *P* denote a presidential candidate's campaign. As to types of information, *O*, let O_1 denote individual-donor totals, and let O_2 denote individual-identifying donor information. As to the third-party to whom information is disclosed, *Q*, let Q_1 denote the country's campaign finance enforcement authority (i.e., the state), and let Q_2 denote the general public.

From this, we derive the following four comparison states:

$$\alpha_{PO_1Q_1}^{U.S.} = \alpha_{PO_1Q_1}^{France}$$

$$\alpha_{PO_1Q_2}^{U.S.} = \alpha_{PO_1Q_2}^{France}$$

$$\alpha_{PO_2Q_1}^{U.S.} > \alpha_{PO_2Q_1}^{France}$$

$$\alpha_{PO_2Q_2}^{U.S.} < \alpha_{PO_2Q_2}^{France}$$

Using our model, the reader is able, at a glance, to note that in two of the situations the privacy state of presidential candidates is identical: in both countries, information about total donations received from individuals must be disclosed both to the state and to the public. It is the third and fourth equations that show us the state of inequality between candidates in the two countries: (1) candidates have greater privacy in the United States, due to the lack of mandated disclosure to the state of the identifying information for donors giving between $1 and $199; and (2) French candidates have greater privacy with respect to the disclosure to the public of individual-identifying information, since the CNCCFP redacts this information from all reports disclosed to the public.

The flexibility of the model allows us, however, to be more specific in our notation and to take account of these differences between the U.S. and France. Let O_3 denote donor-identifying information for sub-$200 donations, and let O_4 denote donor-identifying information for donations of $200 and above. From these, we derive four additional comparison states:

$$\alpha_{PO_3Q_1}^{U.S.} > \alpha_{PO_3Q_1}^{France}$$

$$\alpha_{PO_3Q_2}^{U.S.} = \alpha_{PO_3Q_2}^{France}$$

$$\alpha_{PO_4Q_1}^{U.S.} = \alpha_{PO_4Q_1}^{France}$$

$$\alpha_{PO_4Q_2}^{U.S.} < \alpha_{PO_4Q_2}^{France}$$

We'll explicate these a bit. The first equation compares political candidates' privacy regarding the identities of sub-$200 campaign donors with respect to the state. American candidates have greater privacy in this regard, since the U.S. does not require disclosure of such donations to the FEC. The second equation compares political candidates' privacy regarding the identities of sub-$200 campaign donors with respect to the public. French and American candidates have the same degree of privacy in this regard. In the U.S., the FEC does not have that information and hence cannot reveal it. In France, the CNCCFP redacts that information in public reports. The third equation compares political candidates' privacy regarding the identities of campaign donors who give $200 or more with respect to the state. Again, French and American candidates have the same degree of privacy in this regard; both states require campaigns to disclose such information to the state election authorities. Finally, the fourth equation compares political candidates' privacy regarding the identities of campaign donors who give $200 or more with respect to the general public. French candidates have greater privacy in this regard; the CNCCFP redacts such information in its reports whereas the FEC makes such information available in its databases.

Our framework also allows for variation in the variable *P*, to permit privacy comparisons between different actors. To provide an example, we use the same legal situation with respect to campaign finance in France and the United States, but from the perspective of the individual donor—a developing concern, referred to as "political privacy", in campaign finance and democratic governance. Let P_1 represent a sub-$200 donor, and let P_2 represent a $200-and-above donor. Let *O* represent the donor's personally identifying information. Finally, as above, let Q_1 represent the state, and let Q_2 represent the general public. The following privacy comparison states result:

$$\alpha_{P_1OQ_1}^{U.S.} > \alpha_{P_1OQ_1}^{France}$$

$$\alpha_{P_1OQ_2}^{U.S.} = \alpha_{P_1OQ_2}^{France}$$

$$\alpha_{P_2OQ_1}^{U.S.} = \alpha_{P_2OQ_1}^{France}$$

$$\alpha_{P_2OQ_2}^{U.S.} < \alpha_{P_2OQ_2}^{France}$$

Note that in this case the privacy states, viewed from the position of the donor, are similar to the privacy states as viewed from the position of the candidate; that is, if *P* represented political candidates, the relations would be the same as above. This could have been otherwise, but the fact that the interests of the candidates and the donors overlap is helpful from the position of privacy analysts.

It is also possible to make comparisons across contexts (here, between the U.S. and France) wherein two or more of the variables *P*, *O*, and *Q* vary, as well. We have, until now, avoided doing so, for the simple reason that the more one varies these when comparing across contexts, the less coherent the comparison becomes; holding variables constant across contexts imposes an internal consistency that motivates a comparison of truly like situations. That said, there are instances where a researcher might need to compare two different sorts of privacy relationships, in order to draw specific inferences, and

our notation scheme permits such cases. Continuing on the above analysis of individual donors' privacy, consider the following comparison in which *P* and *Q* are both made to vary across contexts:

$$\alpha^{U.S.}_{P_1OQ_1} = \alpha^{France}_{P_2OQ_2}$$

Notice, in this comparison, that the identifying-informational privacy of a sub-$200 donor in the U.S. with respect to the state is equal to the privacy of a $200-and-above donor in France with respect to the general public. That is, in neither case is *O*, the identifying-information, disclosed to the third-party in question (Q_1 and Q_2). In the American case, the state remains ignorant as to the identity of the donor, P_1, because it does not collect such information, and in the French case, the public remains ignorant as to the identity of P_2 because the state does not make such information available to the public.

3.3. Toward social scientific explanations 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.

It is also worth noting that not developing a framework to operationalize the broadest notion of privacy would have negative consequences for developing policy and for the empirical work upon which policy depends. Some conceptions of privacy, either because they are incomplete or proceed a priori, exclude certain actors and privacy relationship. Actors that are systematically excluded—and hence ignored—may include the socially, economically, or politically less-powerful. Our framework restores the full field of vision about privacy states, bringing to light the privacy states of any actor upon which the analyst wishes to focus. Privacy studies, under this pluralistic analysis, will be broader and more complete with a

framework that excludes neither certain relationships between previously ignored actors nor certain philosophical approaches to the nature of privacy.

4. Objections and Limitations

There are several potential objections to the framework offered here. Perhaps the most important is that the notation does not offer much advantage over narrative accounts describing and comparing privacy states. We see two primary advantages. First, while it is true that any privacy relation represented using the framework offered here can in principle be described in narrative form, narrative forms make it easier to skip over important aspects of privacy relations. In contrast, formalizing privacy relations forces one to be precise about who has (or lacks) privacy, the domain of information in which she has (or lacks) privacy, the other person(s) with respect to whom she has (or lacks privacy), and the type of privacy she has (or lacks). This forced precision is important in avoiding hidden ambiguities or vagueness. Consider, for example, one of the examples that purportedly shows the disarray in privacy conceptions. As noted, Solove argues that when a court determined that a newspaper's publication of a revealing photograph of a soccer player did not constitute a privacy violation it made a mistake regarding the appropriate conception of privacy (i.e., applying a "secrecy" conception instead of something else). Simply describing the situation in a narrative form, one might say that at the time the photograph was taken, the player's genitals were exposed to the public and, hence, the act of taking and publishing a photograph does not expose something new. Indeed, the court's reasoning as to why the photograph was protected speech and not a privacy violation warranting restriction turns on the "public" nature of the event.

> The picture accurately depicted a public event and was published as part of a newspaper article describing the game. At the time the photograph was taken, McNamara was voluntarily participating in a spectator sport at a public place (*McNamara v. Freedom Newspapers*, 1991).

But eliding so easily between exposure in a public event at a single moment and exposure to the public, period, is impossible if we are being precise in the way required under our framework. So, let P be the soccer player, *O* be images of his genitalia, and *Q* be the general public. T_1 will represent the period after the photograph was take but before it was published and T_2 will represent the period after the photograph was published.

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

Of course the court might still reason that the decrease in privacy is insufficiently weighty to override First Amendment protections, but it would have to do so by explicit appeal to underlying principles about the relative weight of speech and privacy loss rather than quickly dispensing with the privacy issue. Hidden ambiguities are often the source of moral disagreements (see Daniels (1979), 262-263). Those crop up frequently in narrative accounts, and our framework goes some way in revealing and avoiding them.

A second advantage of our framework over narrative accounts is in advancing empirical social science regarding privacy. Narrative accounts can provide rich detail in small numbers of cases, but they become unwieldy when trying to make broader comparisons based on multiple cases. So, if we wanted to compare the privacy protections for, say, medical information in Western Europe and North America, we would need to look at various aspects of medical privacy practices, laws, and technologies in a variety of countries. Using our framework we could pick out a few relevant privacy relations and variables and compare across places. The result would be a set of tables, which would be relatively easy to scan and understand. A narrative account would have to describe each in detail, and would be more difficult to understand.

This ability to compress lots of aspects of privacy across numerous variables gives rise to a second objection, namely that operationalizing a complex concept such as privacy will gloss over important nuances. While it is true that some aspects of privacy are not represented explicitly in our framework, the goal is to be able to analyze nuances effectively. Being explicit about a definite set of variables allows us to see nuances more clearly. That the framework leaves out nuances is a feature not a bug; it forces commentators to define the context enough to see and examine nuances. Moreover, the framework is flexible so users can either add nuance or account for nuances within it. That is, the framework allows the user tremendous flexibility in the definition of the account being described and compared.

5. 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, particularized judgment, knowledge).

Notes

1. As Daniels puts it, wide reflective equilibrium is a method of producing coherence among an "order triple" of propositions: "(a) a set of considered moral judgments, (b) a set of moral principles, and (c) a set of relevant background theories" (Daniels 1979, 258).
2. Examples of access accounts include (DeCew 1997; Powers 1996; Allen 1988, 15; Gavison 1984, 349–50; Parent 1983, 269).

3. Examples of control accounts include (Moore 2010; Westin 1967, 7; Rachels 1975).
4. (Solove 2002, 1147–48) (Citing *McNamara v. Freedom Newspapers, Inc.*, 802 S.W.2d 901 (Tex. Ct. App. 1991)).
5. (Solove 2002, 1152–53) (Citing *United States v. Miller*, 425 U.S. 435 (1976) and *Smith v. Maryland*, 442 U.S. 735 (1979)).
6. This paper is about informational privacy. We leave aside the relation between informational privacy and *decisional* or *constitutional* privacy, which may involve information flows, but which also concern autonomy over certain kinds of decisions.
7. *Federal Communications Commission v. AT&T*, 562 U.S. __ (2011).
8. *Id.* at __; *Federal Communications Commission v. AT&T*, 582 F. 3d 490 (3rd Cir. 2009).
9. Our account ignores differences in the nature of the office of president from one country to the other, wanting to focus attention simply on the highest elected executive office in each political system.
10. Federal Election Campaign Act, 2 U.S.C. § 434(b)(3)(A).
11. Campaign Finance Disclosure Portal, Federal Election Commission. http://www.fec.gov/pindex.shtml. Accessed August 2013.
12. Presidential Donor Lookup (2012), OpenSecrets.org. http://www.opensecrets.org/pres12/search_donor.php. Accessed August 2013.
13. The CNCCFP, *Commission nationale des comptes de campagne et des financements politiques* (National Commission for Campaign Accounts and Political Financing), is an independent administrative authority created by the French Parliament in 1990. The intent behind its existence in many ways mirrors that of the FEC in the United States, though its internal composition and decision-making procedures vary in non-trivial ways.
14. Commission nationale des comptes de campagne et des financements politiques (France). *Mémento à l'usage du candidat et de son mandataire* (2012), 13-19, 37, http://www.cnccfp.fr/docs/presidentielle/cnccfp_presidentielle_2012_memento_v20120322.pdf.
15. French Electoral Code (*Code électoral*), Art. L52-8.

References

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

Altman, Irwin. 1977. Privacy Regulation: Culturally Universal or Culturally Specific? *Journal of Social Issues* 33 (3): 66–84.

Bellman, Steven, Eric Johnson, Stephen Kobrin, and Gerald Lohse. 2004. International Differences in Information Privacy Concerns: A Global Survey of Consumers. *Information Society* 20 (5): 313–324.

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

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

Bollen, Kenneth. 1993. Liberal Democracy: Validity and Method Factors in Cross-National Measures. *American Journal of Political Science* 37(4): 1207-30.

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

Daniels, Norman. 1979. Wide Reflective Equilibrium and Theory Acceptance in Ethics. *The Journal of Philosophy* 76 (5): 256–282.

DeCew, Judith Wagner. 1997. *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology*. Ithaca, N.Y.: Cornell University Press.

Detweiler, Christian, Alina Pommeranz, Jeroen Hoven, and Helen Nissenbaum. 2011. Values in Design - Building Bridges Between RE, HCI and Ethics. In *Human-Computer Interaction – INTERACT 2011*, eds. Pedro Campos, Nicholas Graham, Joaquim Jorge, Nuno Nunes, Philippe Palanque, and

Marco Winckler, 6949:746–747. Lecture Notes in Computer Science. Springer Berlin / Heidelberg. http://www.springerlink.com.ezproxy.library.wisc.edu/content/q182242760430730/abstract/.

Freedom House. 2013. "Freedom in the World 2013: Democratic Breakthroughs in the Balance." Available at http://www.freedomhouse.org/report/freedom-world/freedom-world-2013. Accessed 16 July 2013.

Gavison, Ruth. 1984. Privacy and the Limits of Law. In *Philosophical Dimensions of Privacy*, ed. Ferdinand Schoeman, 346–402. Cambridge: Cambridge University Press.

Gupta, Dipak K., Albert J. Jongman, and Alex P. Schmid. 1994. Creating a Composite Index for Assessing Country Performance in the Field of Human Rights: Proposal for a New Methodology. *Human Rights Quarterly* 16(1): 131-162.

McNamara v. Freedom Newspapers, 802 S.W.2d 901 (Tex. Ct. App. 1991).

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

Nissenbaum, Helen Fay. 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, Richard A. 1984. An Economic Theory of Privacy. In *Philosophical Dimensions of Privacy*, ed. Ferdinand Schoeman, 333–345. Cambridge: Cambridge University Press.

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

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

Rawls, John. 1999. *A Theory of Justice*. Cambridge, Mass.: Belknap Press of Harvard University Press.

Regan, Priscilla. 2010. The United States. In *Global Privacy Protection: The First Generation*, ed. James B. Rule and G. W. Greenleaf. Cheltenham, UK ; Northampton, MA: Edward Elgar.

Rubel, Alan. 2011. The Particularized Judgment Account of Privacy. *Res Publica* 17 (July 20): 275–290.

Solove, Daniel J. 2002. “Conceptualizing Privacy.” *California Law Review* 90: 1087–1155.

———. 2005. A Taxonomy of Privacy. *University of Pennsylvania Law Review* 154: 477.

———. 2008. *Understanding Privacy*. Cambridge, Mass: Harvard University Press.

Spiro, Herbert J. 1971. Privacy in Comparative Perspective. In *NOMOS XIII: Privacy*, ed. J. Roland Pennock and John W. Chapman, 121–148. New York: Atherton Press.

Westin, Alan F. 1967. *Privacy and Freedom*. New York: Atheneum.