4

The meaning and value of privacy

DANIEL J. SOLOVE

Our privacy is under assault. Businesses are collecting an unprecedented amount of personal data, recording the items we buy at the supermarket, the books we buy online, our web-surfing activity, our financial transactions, the movies we watch, the videos we rent, and much more. Nearly every organization and company we interact with now has tons of personal data about us. Companies we have never heard of also possess our profiles. Digital dossiers about our lives and personalities are being assembled in distant databases, and they are being meticulously studied and analyzed to make judgments about us: What products are we likely to buy? Are we a good credit risk? What price would we be willing to pay for certain items? How good a customer are we? Are we likely to be cooperative and not likely to return items or complain or call customer service?

Today, government has an unprecedented hunger for personal data. It is tapping into the data possessed by businesses and other organizations, including libraries. Many businesses readily comply with government requests for data. Government agencies are mining this personal data, trying to determine whether a person might likely engage in criminal or terrorist activity in the future based on patterns of behavior, purchases, and interest (O'Harrow 2005). If a government computer decides that you are a likely threat, then you might find yourself on a watch list, you might have difficulty flying, and there might be further negative consequences in the future.

The threat to privacy involves more than just records. Surveillance cameras are popping up everywhere. It is getting increasingly harder to have an unrecorded moment in public. In the United States, the National Security Agency is engaging in massive telephone surveillance. In the United Kingdom, millions of CCTV cameras monitor nearly every nook

This chapter adapts and discusses the ideas in my book, *Understanding Privacy* (Solove 2008); it was published previously in *OPEN Magazine* on October 19, 2009.

and cranny of public space (Rosen 2004). At work, many employers monitor nearly everything – every call their employees make, every keystroke they type, every website they visit.

Beyond the government and businesses, we are increasingly invading each other's privacy – and exposing our own personal information. The generation of young people growing up today is using blogs and social network websites at an unprecedented rate, spilling intimate details about their personal lives online that are available for anybody anywhere in the world to read (Solove 2007). The gossip that circulates in high school and college is no longer ephemeral and fleeting – it is now permanently available on the Internet, and it can readily be accessed by doing a Google search under a person's name.

With all these developments, many are asking whether privacy is still alive. With so much information being gathered, with so much surveillance, with so much disclosure, how can people expect privacy anymore? If we can't expect privacy, is it possible to protect it? Many contend that fighting for privacy is a losing battle, so we might as well just grin and bear it.

Do people expect privacy anymore?

These attitudes, however, represent a failure to understand what privacy is all about. The law often focuses on whether we expect privacy or not – and it refuses to protect privacy in situations where we do not expect it. But expectations are the wrong thing to look at. The law is not merely about preserving the existing state of affairs – it is about shaping the future. The law should protect privacy not because we expect it, but because we desire it.

Privacy is often understood narrowly, and these restrictive concepts lead to people neglecting to recognize privacy harms (for example Westin 1967; Gavison 1980; Posner 1981; Etzioni 1999). For example, it may be true that many businesses hold a lot of personal data about you. Does this mean you lack a privacy interest in that data? Those who view privacy narrowly as keeping information totally secret might say that you no longer have privacy in information that others possess.

But privacy is about much more than keeping secrets. It is also about confidentiality – data can be known by others, yet we have social norms about maintaining that information in confidence. For example, although librarians know information about the books we read, they understand that they have an obligation to keep the information confidential.

Doctors know our medical information, but they, too, are under a duty of confidentiality.

Privacy also involves maintaining data security. Those who possess data should have an obligation to keep it secure and out of the hands of identity thieves and fraudsters. They should have an obligation to prevent data leaks.

Another dimension of privacy is having control over our information (Westin 1967; Fried 1968; Miller 1971). Just because companies and the government have data about you does not mean that they should be allowed to use it however they desire. We can readily agree that they should not be able to use personal information to engage in discrimination. The law can and should impose many other limits on the kinds of decisions that can be made using personal data.

Those that use data about us should have the responsibility of notifying us about the data they have and how they plan to use it. People should have some say in how their information is used. There needs to be better "data due process." Currently, innocent people are finding themselves on terrorist watch lists and with no recourse to challenge their inclusion on the list. Financial and employment decisions are made about people based on profiles and information they do not even know about.

Privacy thus involves more than keeping secrets – it is about how we regulate information flow, how we ensure that others use our information responsibly, how we exercise control over our information, how we should limit the way others can use our data.

Some argue that it is impossible for the law to limit how others use our data, but this is false. Copyright law is a clear example of the law regulating the way information is used and providing control over that data. I am not suggesting that copyright law is the answer to privacy, but it illustrates that it is possible for the law to restrict uses of data if it wants to.

We can protect privacy, even in light of all the collection, dissemination, and use of our information. And it is something we must do if we want to protect our freedom and intellectual activity in the future.

But how? The first steps involve rethinking the concept and value of privacy.

Rethinking the concept of privacy

Privacy is a concept in disarray. Commentators have lamented that the concept of privacy is so vague that it is practically useless. When we speak of privacy invasions, we often fail to clearly explain why such an

infringement is harmful. The interests on the other side – free speech, efficient consumer transactions, and security – are often much more readily comprehended. The result is that privacy frequently loses in the balance. Even worse, courts and policymakers often fail to recognize privacy interests at all.

Many attempts to conceptualize privacy do so by attempting to locate the common denominator for all things we view as private (for example Fried 1968; Miller 1971; Gavison 1980; Inness 1992). This method of conceptualizing privacy, however, faces a difficult dilemma. If we choose a common denominator that is broad enough to encompass nearly everything, then the conception risks the danger of being over-inclusive or too vague. If we choose a narrower common denominator, then the risk is that the conception is too restrictive.

There is a way out of this dilemma: We can conceptualize privacy in a different way. The philosopher Ludwig Wittgenstein argued that some concepts are best understood as family resemblances – they include things that "are *related* to one another in many different ways" (Wittgenstein 1958: § 65, original emphasis). Some things share a network of similarities without one particular thing in common. They are related in the way family members are related. You might have your mother's eyes, your brother's hair, your sister's nose – but you all might not have one common feature. There is no common denominator. Nevertheless, you bear a resemblance to each other.[1] We should understand privacy in this way. Privacy is not one thing, but a plurality of many distinct yet related things.

One of the key issues in developing a theory of privacy is how to deal with the variability of attitudes and beliefs about privacy. Privacy is a product of norms, activities, and legal protections. As a result, it is culturally and historically contingent. For example, it is widely accepted today that the naked body is private in the sense that it is generally concealed. But that was far from the case in ancient Greece and Rome. At the gymnasium in ancient Greece, people exercised in the nude. In ancient Rome, men and women would bathe naked together (Goldhill 2004: 15, 19). In the Middle Ages, people bathed in front of others and during social gatherings (Rybczynski 1986: 28, 30). Norms about nudity, bathing, and concealing bodily functions have varied throughout history and in different cultures. Likewise, although the home has long been viewed as a private

[1] As Wittgenstein observes, instead of being related by a common denominator, some things share "a complicated network of similarities overlapping and crisscrossing: sometimes overall similarities, sometimes similarities of detail" (Wittgenstein 1958: § 66).

space, in the past it was private in a different way than it is now. Until the seventeenth century, many homes merely consisted of one large room where there was scant seclusion for "private" activities such as sex and intimacy. A married couple would often sleep in the same bed as their children, and would share it with houseguests (Flaherty 1972: 45). Like the body, the home is not inherently private – at least not in the same way we view it as private today.

Many theories of privacy focus on the nature of the information or matter involved. They seek to identify various types of information and matters that are private. But as I illustrated with the body and the home, no particular kind of information or matter is inherently private. Others contend that we should define privacy with the reasonable expectation of privacy test. This method defines privacy based on expectations that society considers reasonable. This is the prevailing method that American courts, as well as courts in many other countries and the European Court of Human Rights, use to identify privacy interests protected by the Fourth Amendment as well as other areas of law (Tomás Gómez-Arostegui 2005: 153).

But how are reasonable expectations of privacy to be determined? The US Supreme Court has never engaged in giving empirical evidence when applying the reasonable expectation of privacy test. It merely guesses at what society expects. One way of determining societal expectations is to take polls. But people's stated views about privacy often differ dramatically from their actions. A person might say she values privacy greatly, but then she will trade away her personal data for tiny discounts or minor increases in convenience. For this reason, others contend that we should examine behavioral data rather than polls. There are several factors, however, that make people's behavior unreliable as a measure for their views on privacy. In many circumstances, people relinquish personal information to businesses because they do not have much of a choice or because they lack knowledge about how the information will be used in the future.

Even with a reliable way of measuring societal expectations of privacy, such expectations only inform us about existing privacy norms. Privacy law and policy depend on more than merely preserving current expectations. The history of communications privacy best illustrates this point. In colonial America, mail was often insecure. Letters, sealed only with wax, left many people concerned that they were far from secure. For example, Thomas Jefferson, Alexander Hamilton, and George Washington all complained about the lack of confidentiality in their correspondence (Solove 2004: 225). Despite the expectation that mail was not very private, the law

evolved to provide strong protection of the privacy of letters. Benjamin Franklin, the colonial postmaster general before the Revolution, made postal workers take an oath not to open mail (Solove 2004: 225). After the Revolution, the US Congress passed several statutes to protect the privacy of letters. In 1877 the US Supreme Court held that the Fourth Amendment protected sealed parcels despite the fact that people handed them to the government for delivery (*Ex Parte Jackson* 1877: 727, 733). The extensive protection of the privacy of written correspondence stemmed from a public desire to keep them private, not from an expectation that they were already private.

A similar story can be told with electronic communications in the USA. Concerns over telegraph privacy were legion in its early days during the mid nineteenth century. Laws in almost every state ensured that telegraph employees could not improperly disclose telegrams. State laws also prohibited the interception of telegraph communications. During the telephone's early days, calls were far from private. Until well into the twentieth century many people had party lines – telephone lines that were shared among a number of households. There were rampant concerns about eavesdropping and wiretapping. Legislatures responded by passing laws to protect the privacy of phone communications. More than half the states had made wiretapping a crime by the early twentieth century.

The moral of the story is that communications *became* private because people wanted them to be private. Privacy is not just about what people *expect* but about what they *desire*. Privacy is something we construct through norms and the law. Thus we call upon the law to protect privacy *because* we experience a lack of privacy and desire to rectify that situation, not because we already expect privacy.

What, then, should we focus on when seeking to understand privacy? I contend that the focal point for a theory of privacy should be on the problems we want the law to address. According to John Dewey, philosophical inquiry begins with problems in experience, not with abstract universal principles. A theory of privacy should focus on the problems that create a desire for privacy. Privacy problems arise when the activities of the government, businesses, organizations, and other people disrupt the activities of others. Real problems exist, yet they are often ignored because they do not fit into a particular conception of privacy. Many problems are not even recognized because courts or policymakers cannot identify a "privacy" interest involved. Instead of pondering the nature of privacy in the abstract, we should begin with concrete problems and then use theory as a way to better understand and resolve these problems. In my book

Understanding Privacy (2008) I develop a framework for recognizing privacy problems, and I identify and examine sixteen such problems.

There are four basic groups of harmful activities: (1) information collection, (2) information processing, (3) information dissemination, and (4) invasion. Each of these groups consists of different related subgroups of harmful activities.

I have arranged these groups around a model that begins with the data subject – the individual whose life is most directly affected by the activities classified in the taxonomy. From that individual, various entities (other people, businesses, and the government) collect information. The collection of this information itself can constitute a harmful activity, though not all information collection is harmful. Those that collect the data (the "data holders") then process it – that is, they store, combine, manipulate, search, and use it. I label these activities "information processing." The next step is "information dissemination," in which the data holders transfer the information to others or release the information. The general progression from information collection to processing to dissemination is the data moving further away from the individual's control. The last grouping of activities is "invasions," which involve impingements directly on the individual. Instead of the progression away from the individual, invasions progress toward the individual and do not necessarily involve information.

The first group of activities that affect privacy is information collection. *Surveillance* is the watching, listening to, or recording of an individual's activities. *Interrogation* consists of various forms of questioning or probing for information.

A second group of activities involves the way information is stored, manipulated, and used – what I refer to collectively as "information processing." *Aggregation* involves the combination of various pieces of data about a person. *Identification* is linking information to particular individuals. *Insecurity* involves carelessness in protecting stored information from leaks and improper access. *Secondary use* is the use of collected information for a purpose different from the use for which it was collected without the data subject's consent. *Exclusion* concerns the failure to allow the data subject to know about the data that others have about her and participate in its handling and use. These activities do not involve the gathering of data because it has already been collected. Instead, these activities involve the way data is maintained and used.

The third group of activities involves the dissemination of information. *Breach of confidentiality* is breaking a promise to keep a person's

information confidential. *Disclosure* involves the revelation of truthful information about a person that affects the way others judge her reputation. *Exposure* involves revealing another's nudity, grief, or bodily functions. *Increased accessibility* is amplifying the accessibility of information. *Blackmail* is the threat to disclose personal information. *Appropriation* involves the use of the data subject's identity to serve another's aims and interests. *Distortion* consists of disseminating false or misleading information about individuals. Information dissemination activities all involve the spreading or transfer of personal data or the threat to do so.

The fourth and final group of activities involves invasions into people's private affairs. Invasion, unlike the other groupings, need not involve personal information (although in numerous instances, it does). *Intrusion* concerns invasive acts that disturb one's tranquility or solitude. *Decisional interference* involves incursion into the data subject's decisions regarding her private affairs.

Privacy is not one thing, but many distinct but related things. For too long, policymakers and others have viewed privacy too myopically and narrowly, failing to recognize many important privacy problems. Understanding privacy in a more pluralistic manner will hopefully improve the way privacy problems are recognized and addressed.

The social value of privacy

Another problem with the way privacy is often conceptualized involves how its value is assessed. Traditional liberalism often views privacy as a right possessed by individuals. For example, legal theorist Thomas Emerson declares that privacy "is based upon premises of individualism, that the society exists to promote the worth and dignity of the individual … The right of privacy … is essentially the right not to participate in the collective life – the right to shut out the community" (Emerson 1970: 545, 549). In the words of one court: "Privacy is inherently personal. The right to privacy recognizes the sovereignty of the individual" (*Smith* v. *City of Artesia* 1989).

Framing privacy exclusively in individualistic terms often results in privacy being undervalued in utilitarian balancing, which is the predominant way policymakers resolve conflicts between various interests. When individual interests are pitted against the common good, the latter often wins out. The interests often in tension with privacy – free speech, efficient consumer transactions, or security – are frequently understood

as valuable for all of society. Privacy, in contrast, is seen as a zone of respite for the sake of the individual.

There is a way, however, to justify privacy from a utilitarian basis. Pragmatist philosopher John Dewey has articulated the most coherent theory of how protecting individual rights furthers the common good. For Dewey, there is no strict dichotomy between individual and society. The individual is shaped by society, and the good of both the individual and society are often interrelated rather than antagonistic: "We cannot think of ourselves save as to some extent *social* beings. Hence we cannot separate the idea of ourselves and our own good from our idea of others and of their good" (Dewey 1908: 268, original emphasis). Dewey contended that the value of protecting individual rights emerges from their contribution to society. In other words, individual rights are not trumps, but are protections by society from its intrusiveness. Society makes space for the individual because of the social benefits this space provides. Therefore, Dewey argues, rights should be valued based on "the contribution they make to the welfare of the community" (Dewey 1936: 374). Otherwise, in any kind of utilitarian calculus, individual rights would not be valuable enough to outweigh most social interests, and it would be impossible to justify individual rights. As such, Dewey argued, we must insist upon a "social basis and social justification" for civil liberties (Dewey 1936: 375).

I contend, like Dewey, that the value of protecting the individual is a social one. Society involves a great deal of friction, and we are constantly clashing with each other. Part of what makes a society a good place in which to live is the extent to which it allows people freedom from the intrusiveness of others. A society without privacy protection would be suffocating, and it might not be a place in which most would want to live. When protecting individual rights, we as a society decide to hold back in order to receive the benefits of creating the kinds of free zones for individuals to flourish.

As Spiros Simitis declares, "privacy considerations no longer arise out of particular individual problems; rather, they express conflicts affecting everyone" (Simitis 1987: 707, 709).[2] Privacy, then, is not the trumpeting of the individual against society's interests but the protection of the individual based on society's own norms and practices. Privacy is not simply

[2] In analyzing the problems of federal legislative policymaking on privacy, Priscilla Regan demonstrates the need for understanding privacy in terms of its social benefits. See Regan 1995: xiv ("[A]nalysis of congressional policy making reveals that little attention was given to the possibility of a broader social importance of privacy").

a way to extricate individuals from social control, as it is itself a form of social control that emerges from the norms and values of society.

We protect individual privacy as a society because we recognize that a good society protects against excessive intrusion and nosiness into people's lives. Norms exist not to peek into our neighbor's windows or sneak into people's houses. Privacy is thus not an external restraint on society but is in fact an internal dimension of society (Post 1989: 957, 968, arguing that privacy is society's attempt to promote norms of civility). Therefore, privacy has a social value. Even when it protects the individual, it does so for the sake of society. It thus should not be weighed as an individual right against the greater social good. Privacy issues involve balancing societal interests on both sides of the scale.

Because privacy involves protecting against a plurality of different harms or problems, the value of privacy is different depending upon which particular problem or harm is being protected. Not all privacy problems are equal; some are more harmful than others. Therefore, we cannot ascribe an abstract value to privacy. Its value will differ substantially depending upon the kind of problem or harm we are safeguarding against. Thus to understand privacy, we must conceptualize it and its value more pluralistically. Privacy is a set of protections against a related set of problems. These problems are not all related in the same way, but they resemble each other. There is a social value in protecting against each problem, and that value differs depending upon the nature of each problem.

Clearing away the confusion

Understanding privacy as a pluralistic concept with social value will hopefully help add clarity and concreteness to a concept that has been shrouded in a fog of confusion for far too long. This conceptual confusion has caused policymakers to struggle to respond to the myriad emerging threats technology poses for privacy, from the rise of surveillance cameras to the extensive data trails created by the Internet and electronic commerce. With greater conceptual clarity in understanding the meaning and value of privacy, we can better tackle the difficult task of protecting privacy in the Information Age.

References

Dewey, J. 1978 (1908). "Ethics," in Boydston, J. A. (ed.) *The Middle Works of John Dewey*. Carbondale: Southern Illinois University Press, pp. 31–50.

1991 (1936). "Liberalism and Civil Liberties," in Boydston, J. A. (ed.) *The Later Works of John Dewey*. Carbondale: Southern Illinois University Press, pp. 372–75.

Emerson, T. I. 1970. *The System of Freedom of Expression*. New York: Random House.

Etzioni, A. 1999. *The Limits of Privacy*. New York: Basic Books.

Flaherty, D. H. 1972. *Privacy in Colonial New England*. Charlottesville: University Press of Virginia.

Fried, Ch. 1968. "Privacy. A moral analysis," *Yale Law Journal* 77: 475–93.

Gavison, R. 1980. "Privacy and the limits of law," *Yale Law Journal* 89: 421–71.

Goldhill, S. 2004. *Love, Sex, and Tragedy: How the Ancient World Shapes Our Lives*. University of Chicago Press.

Inness, J. 1992. *Privacy, Intimacy and Isolation*. Oxford University Press.

Miller, A. 1971. *The Assault on Privacy: Computers, Data Banks, and Dossiers*. Ann Arbor: University of Michigan Press.

O'Harrow, R. 2005. *No Place to Hide*, New York: Free Press.

Posner, R. 1981. *The Economics of Justice*. Cambridge, MA: Harvard University Press.

Post, R. C. 1989. "The social foundations of privacy: Community and self in the common law. Tort," 77 *California Law Review*: 957–1010.

Regan, P. M. 1995. *Legislating Privacy*. Chapel Hill: University of North Carolina Press.

Rosen, J. 2004. *The Naked Crowd: Reclaiming Security and Freedom in an Anxious Age*. New York: Random House.

Rybczynski, W. 1986. *Home: A Short History of an Idea*. New York: Penguin Books.

Simitis, S. 1987. "Reviewing privacy in an information society," 135 *University of Pennsylvania Law Review*: 707–46.

Solove, D. J. 2004. *The Digital Person: Technology and Privacy in the Information Age*. New York University Press.

2007. *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet*. New Haven: Yale University Press.

2008. *Understanding Privacy*. Cambridge, MA: Harvard University Press.

Tomás Gómez-Arostegui, H. 2005. "Defining private life under the European Convention on Human Rights by referring to reasonable expectations," *California Western International Law Journal* 35: 153–202.

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

Wittgenstein, L. 1958. *Philosophical Investigations* (trans. G. E. M. Anscombe). Oxford: Basil Blackwell.