Published by Blackwell Publishing Ltd, 9600 Garsington Road, Oxford OX4 2DQ, UK, and 350 Main Street, Malden, MA 02148, USA
METAPHILOSOPHY
Vol. 38, No. 1, January 2007
0026-1068

PHILOSOPHICAL THEORIES OF PRIVACY: IMPLICATIONS FOR AN ADEQUATE ONLINE PRIVACY POLICY

HERMAN T. TAVANI

Abstract: This essay critically examines some classic philosophical and legal theories of privacy, organized into four categories: the nonintrusion, seclusion, limitation, and control theories of privacy. Although each theory includes one or more important insights regarding the concept of privacy, I argue that each falls short of providing an adequate account of privacy. I then examine and defend a theory of privacy that incorporates elements of the classic theories into one unified theory: the Restricted Access/Limited Control (RALC) theory of privacy. Using an example involving data-mining technology on the Internet, I show how RALC can help us to frame an online privacy policy that is sufficiently comprehensive in scope to address a wide range of privacy concerns that arise in connection with computers and information technology.

Keywords: control theory of privacy, informational privacy, nonintrusion theory of privacy, online privacy policies, privacy in public, RALC theory of privacy, seclusion theory of privacy.

Introduction

> Defining privacy requires a familiarity with its ordinary usage . . . but this is not enough since our common ways of talking and using language are riddled with inconsistencies, ambiguities, and paradoxes. What we need is a definition which is by and large consistent with ordinary language, so that capable speakers of English will not be genuinely surprised that the term "privacy" should be defined in this way, but which also enables us to talk consistently, clearly, and precisely about the family of concepts to which privacy belongs.
>
> —W. A. Parent 1983, 269

Framing a definition of privacy that satisfies the conditions specified by Parent poses a significant challenge. Yet we must meet this challenge if we are to succeed in understanding and evaluating recent claims about the threat to privacy, including the threat posed by computers and information technology. One aim of this essay is to articulate a definition of privacy that responds to Parent's challenge and serves as the foundation

for an adequate theory of privacy.[1] Another, related, aim is to show how this theory enables us to frame online privacy policies that are clear, transparent, and consistent.

The essay is divided into two main parts. Part 1, which examines the theory of privacy, begins with a brief analysis of the concept of privacy and draws some preliminary distinctions between rights-based and interests-based conceptions of privacy. It then offers a critical evaluation of some classic or standard philosophical and legal theories of privacy. I organize these accounts of privacy into four broad categories, referring to them as the nonintrusion, seclusion, limitation, and control theories. Next I examine a theory of privacy introduced by James Moor (1990 and 1997) that incorporates key elements of the classic theories into one unified theory, referred to as the Restricted Access/Limited Control (RALC) theory of privacy.[2] I then defend the RALC theory, arguing that it includes some important distinctions that are critical for an adequate theory of privacy. For example, I show how RALC successfully differentiates between descriptive and normative aspects of privacy, which enables us to distinguish between concerns having to do with the loss of privacy (in a purely descriptive sense) and claims alleging a violation or invasion of privacy (in a normative sense involving a right to privacy). I also show how RALC differentiates the concept of privacy from both the justification and the management of privacy.

In Part 2, I show how the RALC theory provides a procedure for determining whether and how to protect certain kinds of personal information that, arguably, have both private and public characteristics—a concern that Helen Nissenbaum describes as the challenge of protecting "privacy in public" (Nissenbaum 2004). I also show how this problem is at the heart of privacy controversies involving the use of information technologies, including computerized data mining. Although the data-mining case that I examine illustrates only one way in which RALC can be used to frame an adequate online privacy policy affecting computer/information technologies, I conclude by arguing that the RALC theory is sufficiently comprehensive in scope to be applied to a wide range of privacy concerns associated with contemporary information technologies.

[1] An earlier version of this essay was presented at Purdue University's 2000–2001 Philosophy Colloquium, April 19, 2001. My analysis here of the classic theories of privacy draws from and expands upon a critique of privacy theories in my 1999, 2000, and 2004.

[2] In his 1997 essay, Moor uses the expression "control/restricted access theory" to refer to his theory of privacy. He has since revised his theory, however, and has indicated to me that he is not fully satisfied with the original label used to describe his account of privacy. So, with Moor's permission, in this essay I use the RALC acronym to refer to the revised version of that privacy theory.

Part 1: Theories of Privacy

What, exactly, is personal privacy? Because privacy is difficult to define, it is often described in terms of, and sometimes confused with, such notions as liberty, autonomy, secrecy, and solitude. Privacy has been described as something that can be "intruded upon," "invaded," "violated," "breached," "lost," "diminished," and so forth. Each of these metaphors reflects a conception of privacy that can be found in one or more standard models or theories of privacy. Whereas some privacy theories are essentially descriptive in nature, others are normative. Many normative theories are rights-based, such as those that analyze privacy in terms of a zone or space that can be intruded upon or invaded by others. However, not all normative accounts necessarily presuppose a rights conception of privacy.[3] For example, some normative frameworks view privacy in connection with confidentiality that can be breached or trust that can be betrayed. Descriptive accounts of privacy, on the contrary, sometimes suggest that privacy can be understood in terms of a repository of personal information that when accessed by others can lead to one's privacy being diminished, or perhaps even lost altogether.

Some authors have argued that it is more useful to view privacy in terms of *interests*[4] that individuals have, rather than to think about privacy as a *right*.[5] For example, Roger Clarke believes that privacy is best defined as "the interest individuals have in sustaining a personal space, free from interference by other people and organizations" (1999, 60).[6] While a detailed description and analysis of the differences between interests-based and rights-based conceptions of privacy is beyond the scope of this essay, it is worth noting that a number of arguments have been advanced for a conception of privacy based on interests. Some

[3] It is not the purpose of this essay to determine whether privacy is or ought to be a right—legal, moral, or otherwise. For an analysis of whether a right to privacy is best understood as a derivative right inferred from a cluster of rights, as opposed to being viewed as a distinct right, see Thomson 1975 and Scanlon 1975. And for a discussion of this question from the Lockean perspective of natural rights, see Volkman 2003.

[4] "Interests" can be understood in at least two different, but not mutually exclusive, senses: (1) interests in terms of desires or intentions that one has in achieving a goal (such as having one's information protected), and (2) interests that one has in enhancing one's well-being.

[5] DeCew notes that in recent years there has been "a shift away from reasoning that takes a rights-oriented approach toward arguments that use a utilitarian cost benefit analysis," and that arguments for the latter view attempt to balance the "costs to privacy and the benefits to public safety and crime control" (1997, 21).

[6] As Clarke notes, an important implication of an interest-based definition of privacy is that privacy has to be balanced against many other, often competing, interests, such as those of "the individuals themselves, of other individuals, of groups, and of society as a whole" (1999, 60).

authors have suggested that privacy can be thought of in terms of a "property interest" that individuals have with respect to their personal information.[7] Others who defend an interests-based conception of privacy have suggested that privacy-protection schemes can simply be stipulated (as a practical matter) rather than having to be grounded in philosophical and legal theories, noting that discussions involving a right to privacy often get mired in controversy.[8]

Whereas some authors slide back and forth between rights-based and interests-based conceptions of privacy, others confuse aspects of privacy that are essentially descriptive in nature with those that are primarily normative.[9] We will see how some of these confusions are apparent in the classic privacy theories. Our purpose in analyzing those theories is to gain a clearer understanding of what privacy is, why it is valued, and how it is currently threatened by certain kinds of practices involving computer- and Internet-related technologies.[10] As noted above, I organize these privacy theories into four broad types or categories: the nonintrusion, seclusion, limitation, and control theories.[11] We'll begin with an analysis of the view of privacy as nonintrusion.

[7] As Hunter (1995) points out, one way to give individuals control over information about themselves is to vest them with a "property interest" in that information. Some who have argued for an "economic" perspective on privacy suggest that personal information can be viewed as a kind of property that a person can own and barter in the commercial sphere. An interesting version of the economic theory of privacy has been defended by Richard Posner (1978).

[8] The debate about privacy as a legal right in the United States has been rooted in extensive legal and philosophical argumentation, including debate in both Constitutional and tort law. An important distinction needs to be drawn between Constitutional privacy, as debated in the U.S. courts and legislative bodies, and philosophical theories of privacy that can be used to defend U.S. Constitutional privacy.

[9] We might be inclined to assume that accounts of privacy based on interests (rather than on rights) are nonnormative or descriptive. However, an anonymous *Metaphilosophy* reviewer pointed out to me that when we make generalizations about what interests individuals have, we could be making evaluative claims.

[10] Not considered in this essay is what kind of value privacy is. For discussions of whether privacy should be regarded as an intrinsic value or as an instrumental value, see Fried 1990, Johnson 2001, and Moor 1997. And for a discussion of whether privacy should be regarded primarily as an individual good or as a social value, see Schoeman 1992 and Regan 1995.

[11] Note that I do not argue for the view that classic privacy theories should be conceived of exclusively in terms of these four categories, nor do I believe that such a claim is central to my essay. Many alternative schemes for categorizing privacy theories have been suggested. DeCew (1997) and Parent (1983) organize the classic privacy theories they examine into three major categories; Johnson and Nissenbaum (1995) suggest that we can analyze information-related privacy issues in terms of two broad categories; others have differentiated as many as nine distinct categories. I believe that the four categories used in this essay fairly represent the standard views about privacy considered important by most of the philosophers and legal scholars who have analyzed the concept (see my 1999 and 2000).

The Nonintrusion and the Seclusion Theories of Privacy

In 1890, in a classic article that many scholars now regard as a seminal work on privacy, Samuel Warren and Louis Brandeis described privacy in terms of "being let alone"[12] or being free from intrusion.[13] This conception of privacy, as *nonintrusion*, is also evident in the writings of two U.S. Supreme Court justices: Louis Brandeis in *Olmstead v. U.S.* (1928) and William Brennan in *Eisenstadt v. Baird* (1972). Is such a view of privacy adequate? We should first note that some versions of the nonintrusion theory tend to confuse the condition (or content) of privacy with a right to privacy. This confusion is especially apparent in the writing of nonintrusion theorists, such as Brandeis, who defines privacy as "the *right* to be let alone" (*Olmstead* 475, Brandeis dissenting; italics added), and Brennan, who describes privacy as the "*right* of the individual . . . to be free from unwarranted government intrusion" (*Eisenstadt* 453; italics added).[14]

Another kind of problem with the nonintrusion theory is that, in defining privacy in terms of being free from intrusion, it confuses privacy with liberty. Although the two notions are closely related, they can also be distinguished from one another. Consider that privacy is essential for liberty in that it makes possible the *exercise of* liberty. Whereas liberty allows individuals to hold ideas that might be politically unpopular, it is privacy that enables them to disclose their ideas to certain individuals while concealing from others the fact that they hold those unpopular ideas. So it is useful to distinguish between the concepts of privacy and liberty. Unfortunately, the nonintrusion theory of privacy does not help us to do so.

Let us now consider the *seclusion* theory of privacy. According to this view, privacy is identified with "being alone." One variation of this theory can be found in remarks by Ruth Gavison, who describes a person as enjoying "perfect privacy" when that person is "completely inaccessible

[12] DeCew (1997, 14) points out that the notion of "the right to be let alone" was first articulated by Thomas Cooley in his *Treatise on the Law of Torts* (1880), approximately a decade before the publication of the famous article by Warren and Brandeis. DeCew also notes that the term "privacy" was evoked for the first time in a court decision in 1881 in *DeMay v. Roberts.*

[13] A variation of the nonintrusion theory, which also appeals to the notion of being let alone, is what can be described as the "noninterference" theory of privacy. Whereas the nonintrusion theory focuses on being let alone with respect to privacy invasions involving physical space (affecting one's papers, home, and so forth), the noninterference theory is concerned with the kind of intrusions that affect one's ability to make important decisions without external interference. The latter view traces its origins to an interpretation of privacy advanced in the 1965 case of *Griswold v. Connecticut*.

[14] Justice William Brennan referred to being free from unwarranted government intrusion not simply in matters of physical access but also in matters "so fundamentally affecting a person as the *decision* whether to bear or beget a child" (italics added). See my note 13.

to others''—that is, when no one has ''physical access to [the individual]'' (1980, 428). Another variation of the seclusion theory can be found in Alan F. Westin's description of privacy as the ''voluntary and temporary withdrawal of a person from the general society through physical [means] in a state of solitude'' (Westin 1967, 7).[15] Warren and Brandeis also suggest a variation of the seclusion theory when they describe privacy in terms of ''solitude'' and the necessity for individuals sometimes to ''retreat from the world'' (1890, 196).

The seclusion theory, unlike the nonintrusion theory, avoids confusing privacy and liberty. And because the seclusion theory provides an account of privacy that is essentially descriptive, it avoids confusing the content or condition of privacy with a right to privacy. In describing privacy in terms of one's being secluded from others, however, the seclusion theory tends to confuse privacy with solitude. It suggests that the more alone one is, the more privacy one has. In this scheme, it would seem to follow that a person stranded on an island in which there are no human inhabitants would have complete privacy, or what Gavison refers to as ''perfect privacy.'' We can, however, question whether a person in such a situation enjoys privacy in any meaningful sense. We can also ask whether one's ability to experience solitude is essential for an individual to have privacy. Contrary to what is implied in the seclusion theory, we will see that it is possible for one to enjoy privacy while not necessarily having solitude.

Both the nonintrusion and seclusion theories address privacy concerns that pertain to physical access to individuals—that is, in the form of (physical) access through observation (as in the case of the seclusion theory) or in the form of unwarranted intrusion into one's personal space through someone physically accessing one's personal papers, home, and so forth (as in the nonintrusion theory). These kinds of privacy concerns are sometimes addressed under the category of ''accessibility privacy'' (DeCew 1997, 76). Other aspects of the nonintrusion theory pertain to concerns about interference with an individual's ability to make certain kinds of decisions, which are sometimes analyzed under the category of ''decisional privacy.'' Privacy analysts note that in the United States the concept of privacy has evolved, initially being associated with intrusion (physical access), then being associated with concerns about interference (in decision making), and, more recently, being associated with concerns

[15] I do not wish to claim that either Gavison or Westin is a thoroughgoing seclusion theorist. In fact, much of Gavison's writing on privacy is consistent with what I refer to in this essay as the limitation theory, and much in Westin's account of privacy is compatible with the control theory. However, certain passages in their works, including those cited above, suggest that both authors sometimes view privacy in a way that accords with the seclusion theory. Others who have described privacy in a way that is compatible with the seclusion theory include Weinstein (1971). Also, certain passages in U.S. tort law, such as sections that describe the ''intrusion upon the plaintiff's seclusion or solitude,'' are compatible with the seclusion theory of privacy.

about the flow of personal information. So, perhaps not surprisingly, recent privacy theories have tended to analyze the concept of privacy in terms of conditions having to do with access to and control over *personal information*. In describing information-related privacy concerns, including access to personal information stored in computer databases, many authors now use the expression "informational privacy." Two kinds of theories that pay particular attention to informational-privacy issues are the *control* and the *limitation* theories.

The Control and Limitation Theories of Privacy

Variations of the control theory of privacy—the view that one has privacy if and only if one has control over information about oneself—can be found in the writings of Charles Fried (1990), Arthur Miller (1971), Alan F. Westin (1967), James Rachels (1975), and others (e.g., Elizabeth Beardsley [1971]). According to Fried, privacy "is not simply an absence of information about us in the minds of others, rather it is the control over information we have about ourselves" (1990, 54). Miller embraces a version of the control theory when he describes privacy as "the individual's ability to control the circulation of information relating to him" (1971, 25). A version of the control theory is also endorsed by Westin when he describes privacy as the "claim of individuals . . . to determine for themselves when, how, and to what extent information about them is communicated to others" (1967, 7). And Rachels appeals to a version of the control theory of privacy in his remarks concerning the connection between "our ability to control who has access to information about us and our ability to create and maintain different sorts of relationships" (1975, 297).

Unlike the nonintrusion and the seclusion theories, the control theory of privacy separates privacy from both liberty and solitude. Perhaps the control theory's most important insight is recognizing the role of choice that an individual who has privacy enjoys. Consider the fact that someone who has privacy is able to grant, as well as to deny, others access to information about himself or herself. But the control theory is unclear with respect to two important points, viz., in telling us: (a) *which kinds of personal information* one can expect to have control over, and (b) *how much control* one can expect to have over one's personal information.

Regarding (a), we can ask whether someone can reasonably expect to have control over all of his or her personal information. For example, if you are seen by an acquaintance while shopping at a certain grocery store, you have no control over whether your acquaintance has gained information about the fact that you shop at this particular store (even if for some reason you do not wish this information about you to be known by that person). Perhaps the kind of personal information over which you can expect to have control is limited to "nonpublic personal information"

(what some now refer to as NPI), which includes information about sensitive and confidential data, such as financial and medical records. This kind of information can be contrasted with personal information that is public in nature, or "public personal information" (PPI), such as information about where a person works, lives, shops, dines, and so forth.[16] However, a distinction between one's having control over NPI and having control over PPI is not always made—at least not explicitly—by those who subscribe to the control theory of privacy.

As noted above, control theorists are also unclear with respect to (b)—that is, *how much* control one can expect to have. What, exactly, are control theorists asserting when they say that one must have control over one's personal information in order to have privacy? Are they claiming that one must have total or absolute control over one's personal information as a necessary condition for privacy? If so, this would seem implausible on practical grounds. Consider the fact that people are required to disclose certain kinds of information about themselves in ordinary day-to-day transactions, especially those involving commerce. Control theorists need to specify more clearly how much control over one's personal information, in particular how much control over one's PPI versus one's NPI, one can expect to have in order to enjoy privacy.

Control theorists can also be interpreted as holding a conception of privacy that is counterintuitive to our conventional understanding of that notion. For example, many control theorists seem to imply that one could reveal every bit of personal information about oneself and yet still enjoy privacy. However, the prospect of someone disclosing all of his or her personal information and still somehow retaining privacy, merely because he or she had control over whether to reveal that information, would seem to be counter to our intuitions about what is required for privacy, as well as to the way we use that concept in ordinary discourse. Although one could exercise one's individual autonomy in choosing to disclose every piece of one's personal information to others, it would be difficult to understand how one could still retain one's privacy in that case.[17] It would seem that the control theory confuses privacy with autonomy.

[16] NPI and PPI are both forms of personal information in the sense that they are *information about persons*. However, the kind of personal information included in NPI is such that it is accessible only to certain individuals or organizations that have been designated as appropriate parties (e.g., medical doctors, financial advisors, and so on) to have that particular kind of personal information. In the case of PPI there are no designated boundaries beyond which that kind of information about persons can be excluded from, or made inaccessible to, others. For a detailed account of the differences between PPI and NPI, see my 2004.

[17] So, one can have control over information without necessarily having privacy, and we will see that one can have privacy even when one has limited control over one's personal information.

Let us now examine the *limitation* theory of privacy, variations of which can be found in the writings of Gavison (1980), Parent (1983), and others (e.g., Allen [1988]). In this scheme, one has privacy when access to information about oneself is limited or restricted in certain contexts. Gavison embraces a variation of this theory when she describes privacy as a "limitation of others' access" to information about individuals (1980, 428). And Parent seems to endorse a version of the limitation theory when he defines privacy as the "condition of not having undocumented personal knowledge about one possessed by others" (1983, 269).

One virtue of the limitation theory of privacy is that it correctly recognizes the importance of setting up contexts or "zones" of privacy to limit or restrict others from access to one's personal information. Another strength of this theory is that it avoids confusing privacy with autonomy, as well as with liberty and solitude. Unfortunately, the limitation theory seems to underestimate the role of control or choice that is also required in one's having privacy; it does not take into account that someone who has privacy can choose to grant others access to information about himself or herself, as well as to limit (or even deny) others from access to that information. The limitation theory also seems to imply that one has privacy only to the extent that access to information about oneself is limited or restricted. For example, Gavison notes that an individual, X, enjoys "perfect privacy" when "no one has information about X" (1980, 428). On this view, the more one's personal information can be withheld (or kept secret) from others, the more privacy one has. Thus, in the account of privacy offered in the limitation theory, privacy can easily be confused with secrecy.[18]

It would seem that each of the four traditional privacy theories examined thus far is inadequate. We saw that each confuses privacy with such notions as liberty, solitude, autonomy, and secrecy. We saw also that with respect to informational-privacy concerns the control and the limitation theories provide a better account than do the nonintrusion and the seclusion theories. Thus both the control and the limitation theories would seem to be more promising frameworks for analyzing privacy concerns affecting computers and information technology. Next we consider how key elements in these two theories can be incorporated into one unified and comprehensive account of privacy.

The Restricted Access/Limited Control Theory

Moor (1990, 1997) introduced, and Moor and I (2001) expanded upon, a model of privacy referred to here as the Restricted Access/Limited

[18] For an interesting discussion of some ways in which concerns affecting privacy and secrecy overlap, see Bok 1983 and Thompson 2001.

Control (RALC) theory of privacy. RALC proceeds on the assumption that an adequate theory of privacy needs to differentiate the concept of privacy from both the justification and the management of privacy. Accordingly, the RALC framework has three components: an account of the concept of privacy, an account of the justification of privacy, and an account of the management of privacy. Let us briefly examine each component.

In analyzing the concept of privacy, RALC distinguishes between the *condition* of privacy (that is, what is necessary to have privacy in a descriptive sense) and a *right* to privacy. We will see how this distinction enables us to differentiate between a loss of privacy and a violation or invasion of privacy. But how, exactly, is privacy defined in this framework? According to RALC, an individual has privacy "in a *situation* with regard to others [if] in that situation the individual . . . is protected from intrusion, interference, and information access by others" (Moor 1997, 30; italics added).[19] The notion of a "situation," which has a critical role in the definition of privacy, is left deliberately indeterminate or unspecified so that it can "range over states of affairs" that we normally regard as private. A situation, says Moor, can be an "activity in a location," a "relationship," or the "storage and access of information, such as that stored in . . . or manipulated in a computer" (1990, 76). In a situation in which one is naturally protected or shielded from intrusion and access by others, one has descriptive or "natural" privacy.

RALC also draws an important distinction between a *naturally private situation* and a *normatively private situation*. In the former type of situation, individuals are shielded or blocked from observation, interference, and intrusion by natural means—for example, physical boundaries in natural settings, such as when one is hiking or camping in the woods. In a naturally private situation, privacy can be lost but not violated or invaded, because there are no norms—conventional, legal, or ethical—according to which one has a right to be protected. This is not the case, however, with normatively private situations, which can include the following: locations, such as a person's house (where outsiders are expected to knock and get permission to enter); relationships, such as religious confessions; activities, such as voting; and information, such as medical records (Tavani and Moor 2001). In normatively private situations, one's privacy can be violated or invaded, in addition to being lost, because of laws and norms that have been established to protect those situations.

[19] Note that because RALC requires that one must have protection from intrusion *and* interference *and* information access, it addresses concerns not only about protecting informational privacy (as described in the control and the limitation theories) but also about protection against the kinds of threats described in the nonintrusion and the seclusion theories as well.

Because the RALC theory links the concept of privacy with the notion of protecting individuals by limiting or restricting access to persons or information about persons, RALC might initially appear to be simply a variation of the limitation theory. In fact, Dag Elgesem interprets RALC, as articulated in an earlier formulation (Moor 1997), in this way when he writes:

> But it seems that on [Moor's] view, we have to admit that we always have some degree of privacy, since there will always be billions of people who have physically restricted access to us . . . [and] . . . precisely because all situations are private to some degree, it is difficult to see how the private situations are distinguished from the public ones on this theory. (1999, 289)

Moor and I (2001) have responded to Elgesem's criticism by pointing out that the relevant public/private distinction involving situations is one that is drawn normatively and not descriptively, as Elgesem seems to infer in his interpretation of RALC.[20] In our reply to Elgesem, we show as well why the RALC theory is not merely another variation of the restricted-access theory by pointing out that RALC also recognizes the role that *control* plays in the theory of privacy—viz., in the justification and management of privacy.

We have seen that RALC defines privacy in terms of protection from intrusion and information gathering by others (through situations or zones that are established to restrict access), not in terms of control over information. In our analysis of the control theory of privacy, we saw some of the difficulties of trying to define privacy in a way that requires one to have control over one's information. For example, we saw that there were both theoretical and practical difficulties with such a definition. Furthermore, we saw that it was possible for one to have privacy without having complete control, and to have control over information without having privacy. Yet the notion of "limited control" plays an important role in the overall (tripartite) scheme in the RALC theory of privacy.

To see how the notion of control works in the RALC framework, consider the example of one's medical information. That information is private because a normative zone has been established to restrict people from accessing the information, not because an individual has complete control over who has access to that information within a medical setting. Doctors, nurses, financial administrators, and insurance providers may have legitimate access to various pieces of it. But why does information included in one's medical records deserve normative protection? One justification is that individuals seek to avoid embarrassment and discrimination. Another related justification is that individuals seek control

[20] In part 2 of this essay we examine some distinctions involving the private versus the public characteristics of personal information in our analysis of the problem of privacy in public.

over their lives. They need some degree of control, even if limited, over whom they associate with, what jobs they hold, and what insurance plans they select. Privacy policies that protect information in a particular situation by normatively restricting others from accessing that information provide individuals with limited controls.[21]

Control is also important for the *management* of privacy. In managing one's privacy, however, one need not have absolute control over information about oneself (as implied in many versions of the control theory of privacy). Instead, an individual needs to have some degree of control with respect to three elements: choice, consent, and correction. A person needs some control in choosing situations that offer others the level of access the person desires, which can range from total privacy to total publicity. One can also manage privacy through the consent process—for example, one can waive one's right to restrict others from access to certain kinds of information about oneself. Regarding the role that correction of personal information plays in managing privacy, individuals need to be able to access their information and to amend it if necessary.[22] Limited controls such as choice, consent, and correction are made possible by adequate privacy policies. In part 2 of this essay, we will see how RALC provides us with a mechanism for framing such policies.

It is perhaps worth summarizing some key features of RALC at this point. Because RALC differentiates the concept of privacy from both the justification and management of privacy, it has three important components. The concept of privacy is defined in terms of protection from intrusion and information access by others in the context of a situation. One has normative privacy in a situation where one is protected by explicit norms, policies, or laws that have been established to protect individuals in that situation. Although privacy is defined in terms of protection and restricted access, the notion of control also plays an important role in the RALC framework—both in justifying and in managing privacy. Part of the justification for framing privacy policies is that these policies provide individuals with the limited controls they need to manage their privacy. To see how an adequate privacy policy can

[21] Privacy protection is justified, in part, because the protection it provides allows us to plan our lives in certain ways (e.g., to decide which projects we will undertake and which risks we will assume). Private situations also allow for intimacy and close personal relationships. In effect, privacy offers individuals some control over their lives, which can lead to increased autonomy and happiness. It is important to note that the need for control provides only one justification for privacy policies. Moor (1997) notes that privacy protection is also justified because privacy expresses or articulates a "core value"—viz., security—which is essential to human flourishing and is increasingly threatened in computerized societies.

[22] For example, consumers need to be able to access information about their credit history and credit scores, and to challenge and correct any erroneous information contained in them.

be framed, let us apply RALC to a specific privacy issue involving information technology.

Part 2: Applying the RALC Theory to Online Privacy Concerns

Although I've given only an outline of the RALC theory of privacy, we can begin to think about how this framework can be applied to some specific privacy issues, including online privacy concerns introduced by computer and Internet technologies. In part 1, I noted the critical role that *situations* play in RALC. Based on our analysis of that notion, it would seem that activities and practices involving the Internet can be viewed as situations. For example, the following online activities can be analyzed in terms of situations: accessing personal information about individuals via Internet search engines;[23] acquiring information about a user's online preferences through the use of Internet cookies (that is, text files that Web sites send to and retrieve from a user's computer system, which enable Web-site owners to gather information about a user's browsing preferences);[24] monitoring individuals that exchange information over the Internet via file-sharing systems and P2P (Peer to Peer) networks;[25] and gaining information about persons and groups by *mining* personal data from resources accessible to the Internet. While each of these situations could serve as a test case for the RALC theory,[26] we will limit our analysis here to the example of data mining.

Data Mining on the Internet

Data mining is a computerized technique that uses pattern-matching algorithms derived from research and development in the field of artificial intelligence (AI) to analyze vast amounts of information.[27] The use of data-mining tools has frequently led to the "discovery" of patterns in data

[23] For a discussion of how Internet search engines can be used in ways that raise concerns for personal privacy, see my 2000.

[24] For an analysis of privacy issues affecting Internet cookies, see my 2004. RALC provides an ideal framework for analyzing cookies-related privacy concerns and for framing an online privacy policy for resolving these issues.

[25] For a discussion of how RALC can be applied in a controversial case involving Verizon (an Internet service provider that supports P2P networks) and the Recording Industry Association of America, see Grodzinsky and Tavani 2005.

[26] Moor (1999) shows how the RALC theory can also be applied in analyzing and resolving privacy issues affecting personal genetic information and the use of computing technologies.

[27] Data mining is part of, and sometimes confused with, a larger process called Knowledge Discovery in Databases (or KDD). Whereas KDD is the overall process of discovering useful knowledge from data, data mining involves the use of specific algorithms to "discover" and extract patterns or correlations in the data. In this essay, however, I use "data mining" in a more generic sense to include both pattern discovery and analysis/interpretation. For more information about distinctions between data mining and KDD, see my 1999.

that are implicit and nonobvious. When applied to information about persons, data mining can generate new and sometimes nonobvious classifications or categories of people. Thus, individuals whose personal information is accessible to data-mining tools can become identified or associated with newly created groups—including groups whose existence those individuals might never have imagined.[28] It is in this sense that data mining is sometimes said to reveal "new facts" about people.

Because current privacy laws offer individuals little to no protection with respect to how information about them acquired through data-mining activities is subsequently used, the practice of mining personal data raises some serious challenges for protecting personal privacy.[29] For one thing, data-mining tools have provided many information merchants with a wealth of data about individuals, which can be sold to third parties. For another thing, the process used to acquire this kind of information is not transparent to the people affected.

We should first of all ask whether the practice of mining personal data on the Internet necessarily violates or invades an individual's privacy. Applying the RALC theory, we find that an individual, X, may indeed lose some privacy (in a descriptive sense) whenever data about X is accessed. However, we have seen that the mere loss of privacy by an individual in a particular situation does not necessarily constitute an invasion of that individual's privacy. So it is not yet clear whether X's privacy has been violated or invaded in a normative sense. Should all personal information currently accessible to data-mining technology be declared normatively private? In other words, does it constitute a situation in which that information should be protected in some normative sense? Alternatively, should all personal information that is currently available online to those who mine data be viewed as public information? We could begin by asking whether there is something in the nature of personal information itself—that is, some inherent feature or characteristic of that information—that could help us to answer this question.

According to the RALC theory, there is nothing in personal information per se—as a particular category or kind of information, for example—that can help us to determine whether it should be classified as public or private. Rather, it is the context or situation in which personal information is, or can be, used by others that we must take into

[28] Elsewhere (see my 2004) I examine in greater detail some of the specific challenges that data-mining practices pose for privacy. For example, I consider a hypothetical case in which a man with an impeccable credit history is denied a consumer loan because he is classified according to patterns of consumer behavior that are implicit, nonobvious, and seemingly arbitrary.

[29] It is important to point out that not all cases of data mining are controversial from the perspective of personal privacy. Rather, it is the use of data-mining technologies applied to information pertaining to *persons* that has raised concerns among privacy advocates.

consideration in determining whether some particular kind of personal information should or should not be declared normatively private.

Because of the role that specific contexts play in determining when personal information should be granted normative protection, it might seem that privacy standards in the RALC theory are simply arbitrary. Moor (1997, 30), however, shows why this is not so, in his discussion of a case in which we are asked to determine whether information regarding salaries for college professors should be construed as public information that does not need normative protection or be construed as private information that deserves normative protection. Moor notes that we can have good reasons for making information about faculty salaries public in one context—for example, at state colleges; alternatively, we can have good reasons for declaring this same kind of information to be normatively private in other contexts—for example, at small private colleges. So, in the RALC theory there is nothing inherent in information pertaining to faculty salaries per se that tells us whether or not this information, in general, should be protected as a normatively private situation.

As Moor indicates, it is always the situation or the zone, not the kind of information itself, that is used in determining whether information should be normatively protected. This distinction is helpful in analyzing a problem that Nissenbaum describes as the challenge of protecting "privacy in public" (Nissenbaum 2004), which is also a key issue in the controversy over data mining.

Protecting Privacy in Public

Nissenbaum points out that although we have privacy norms (that is, explicit privacy laws and informal privacy policies) that protect personal information considered to be intimate and sensitive—for example, medical records and financial records—normative protection does not generally extend to personal information considered to be neither sensitive nor intimate. She also indicates that most normative accounts of privacy have a theoretical "blind spot" when it comes to questions about how to protect personal information in public contexts or in what she calls "spheres other than the intimate" (Nissenbaum 1998). Her analysis of this problem illustrates some of the controversies associated with the practice of mining personal data from "public" sources. At first glance, such a practice might seem innocuous because of the public aspect of the data involved. Nissenbaum, however, exposes and questions two assumptions regarding the status of personal information in the public sphere: that (a) "there is a realm of public information in which no privacy norms apply" and (b) "an aggregate of information does not violate privacy if its parts, taken individually, do not" (2004, 455 and 458).[30]

[30] Nissenbaum (2004, 458) correctly suggests that a variation of the fallacy of composition is committed whenever one mistakenly infers that because information pertaining to the

Information merchants that use data-mining techniques might be inclined to defend their practices by appealing to the kind of reasoning found in (a) or (b), or both. But do (a) and (b) provide adequate grounds on which to construct an online privacy policy for collecting and processing personal information in the commercial sphere? To comply with RALC, the assumptions in (a) and (b) would first have to be made explicit and then be justified in the court of rational debate. RALC requires that the parameters of a situation involving access to personal information are "completely public" and known to all those in or affected by a situation. The rules and parameters defining the situation must be explicit and public, and individuals must have the opportunity to debate whether or not a certain situation should be declared normatively private. These requirements are specified in Moor's Publicity Principle, which states:

> *Rules and conditions governing private situations should be clear and known to the persons affected by them.* (1997, 32; italics Moor)[31]

Let us now consider how this principle can be applied to situations involving the mining of personal information.

The Publicity Principle and Its Implications for Online Data Mining

To comply with the Publicity Principle, an adequate online privacy policy affecting data mining would need to spell out clearly the privacy requirements for online consumers who engage in commercial transactions with Web sites that use data-mining technology. These consumers must first be informed that data-mining techniques are being used by those Web sites. Furthermore, the consumers must be told that information about them acquired via data mining could subsequently be used in ways they might not have explicitly authorized, and that these uses could threaten their privacy. In this scheme, the onus would no longer be on consumers to discover for themselves that data-mining practices are used in online contexts. Instead, it would be incumbent upon online businesses

part (i.e., individual) is considered nonprivate, information pertaining to the aggregate must be considered nonprivate as well. We should also note that other kinds of questionable inferences involving private versus nonprivate aspects of personal information might be made. For example, Lloyd Carr pointed out to me a potential flaw involving logical implication, by raising an interesting question: If information *P*, which is nonprivate, implies *Q*, does it follow that *Q* must be nonprivate as well? We can imagine how information merchants would be inclined to answer this question.

[31] Moor (1997, 32) includes two additional principles in his system: the Justification of Exemptions Principle, which can be used to justify a breach of a private situation, and the Adjustment Principle, which enables parameters to be changed in a situation in special circumstances to justify it. There is no need to elaborate on these two principles here, however, since they are not critical to my arguments.

to inform consumers whether and how data-mining practices are being used and how a consumer's personal information can be affected.

Why do online consumers need to be explicitly told that information about them is being acquired via data-mining techniques? For one thing, it would not be reasonable to expect that average consumers would be aware that this kind of technology exists and is used to make important decisions about them, such as in determining their credit scores. By having an explicit policy in which consumers are made aware of the existence of data-mining practices and their implications, consumers could negotiate with online business about how their personal information will be used once it has been collected. The ability for consumers to have some say in how their personal information can subsequently be used by businesses would certainly seem to be a key component in any privacy policy that purports to be open or transparent. It would also comply with RALC's Publicity Principle, which requires the explicit consent of the consumer to have his or her data be used for data-mining purposes.

Although many (if not most) users would likely opt out of having their personal data mined, some might be inclined to opt in because of potential financial advantages. For example, some consumers might elect to participate if, in return, they are offered discounts or rebates on items purchased.[32] The important point, of course, is that online consumers who chose to participate would be explicitly aware of what the rules are because the process is open or transparent. Furthermore, they would be able to make informed choices (that is, they would have limited control) about whether and how their personal data could be used.

Alternative proposals for addressing privacy issues generated by data-mining technology have also been advanced. Some proposals advocate the construction of new categories of privacy protection, while others call for privacy solutions that are technology based. I will briefly describe an example of each. Anton H. Vedder (2004) has argued for a new category of privacy protection, which he calls "categorical privacy" because it concerns privacy issues that he believes are peculiar to data mining.[33] Although Vedder's scheme helps us to identify some of the specific

[32] DeCew refers to this process as "dynamic negotiation" (1997, 161). In this scheme, online consumers could determine whether and how much personal information to reveal in each commercial transaction. This process is "dynamic" because a user might, in one online transaction, choose to disclose certain personal information; but in a subsequent transaction with that same online vendor, the user might elect not to disclose some personal information.

[33] Vedder notes that personal data is commonly defined as "data and information related to an identified or identifiable person" (2004, 405). He adds that although this kind of information is protected by many privacy laws and policies, protection does not apply to individuals as part of group profiles of the sort generated by data mining. Hence, he introduces the notion of "categorical privacy" as a scheme for protecting information that applies to individuals once that information about them has been aggregated (408–9).

privacy-related concerns associated with data-mining technology, it does not provide us with either a systematic or a comprehensive solution to online privacy concerns associated with similar kinds of information technologies.[34]

A different kind of proposal has been advanced by advocates of technology-based solutions, such as privacy-enhancing technologies (or PETs). Those who support this view believe that PETs empower users by enabling them to control their privacy in online transactions. Unfortunately, however, technology-based solutions such as PETs, like proposals to expand categories of privacy protection for data mining, do not provide systematic or comprehensive approaches to resolving the broader dimensions of privacy issues affecting online activities.[35] Both kinds of proposals suggest solutions that are narrow and ad hoc, in that they focus on concerns that are specific to data mining per se, as opposed to broader concerns about online privacy in general. A virtue of RALC is that it enables us to address online privacy concerns affecting data mining without having to expand upon our existing categories of privacy protection, as Vedder proposes, or without having to design tools or technology-based solutions, such as PETs, that can at best function as a "quick fix" to privacy concerns that need to be understood in a context much broader than the specific technologies that generate them.

Alternatively, we have seen how RALC enables us to frame a privacy policy for data mining that also has broad applications in online contexts. For example, the same procedure used in determining whether personal information accessible to data-mining technology should be declared a normatively private situation can also be applied in the analysis of other online privacy controversies that qualify as "situations." Consider, for example, privacy controversies surrounding Internet cookies. Applying RALC, we can use a similar procedure to decide whether personal information currently accessed by cookies technology should be protected as a normatively private situation. Again, there is no need to frame a new

[34] In my 2006, I argue that, following Vedder's scheme, we would unnecessarily expand categories of privacy protection if we framed new categories for each new technology that posed serious privacy problems. I have also shown how this same reasoning applies in the case of Fulda (2004), who argues for modifying or expanding U.S. tort laws to respond to privacy issues associated with data-mining technology.

[35] Elsewhere (see my 2004) I argue that PETs do not provide adequate solutions to online privacy concerns. In particular, I consider the example of a former e-commerce Web site, Toysmart.com, which used a PET scheme to ensure the privacy of its customers. Consumers who conducted business transactions with Toysmart were led to believe that their private information was protected via an online policy that the e-commerce site had established. When Toysmart was forced to file for bankruptcy in 2000, however, it was required to list its assets. These included its database of customer information. The parties interested in acquiring Toysmart's assets argued that they were not bound by any privacy policy that the former e-commerce site had established with its customers. So, we see how PETs fall short when used alone to establish adequate online privacy policies.

category of privacy protection or to depend on new tools (for example, PETs) to address privacy concerns associated with cookies. In this way, RALC offers us a comprehensive and systematic procedure for addressing online privacy concerns that can affect a wide range of technologies.

Concluding Remarks

We have seen that none of the classic privacy theories examined in part 1 of this essay provides an adequate account of privacy. Alternatively, I have defended the RALC theory, noting how it differentiated the concept of privacy from both its justification and its management. We saw that RALC, in differentiating normative from descriptive aspects of privacy, enabled us to distinguish between the condition of privacy and a right to privacy and between a loss of privacy (in a descriptive sense) and a violation or invasion of privacy (in a normative sense). In applying the RALC theory to privacy concerns generated by data-mining technology, we saw how RALC enabled us to frame a comprehensive online privacy policy that could be applied not only to situations involving data mining but also to a wide range of privacy controversies associated with computer and information technologies.

Department of Philosophy
Rivier College
420 Main Street
Nashua, NH 03060
USA
htavani@rivier.edu

Acknowledgments

I am grateful to Lloyd Carr (Rivier College), Kenneth Himma (Seattle Pacific University), James Moor (Dartmouth College), and an anonymous *Metaphilosophy* reviewer for their helpful suggestions on an earlier draft of this essay. I am also grateful to Paul Thompson, Martin Curd, and others in the Department of Philosophy at Purdue University for helpful comments I received on a version of this essay that I presented at Purdue's 2000–2001 Philosophy Colloquium, April 19, 2001.

References

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

Beardsley, Elizabeth. 1971. "Privacy: Autonomy and Selective Disclosure." In *Nomos XIII: Privacy*, edited by J. Roland Pennock and John W. Chapman, 56–70. New York: Atherton Press.

Bok, Sisela. 1983. *Secrets: The Ethics of Concealment and Revelation*. New York: Vintage Books.

Clarke, Roger. 1999. "Internet Privacy Concerns Confirm the Case for Intervention." *Communications of the Association for Computing Machinery* 42, no. 2 (February): 60–67.

Cooley, Thomas. 1880. *Treatise on the Law of Torts*. Chicago: Callaghan.

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

DeMay v. Roberts. 1881. 46 U.S. 160ff.

Eisenstadt v. Baird. 1972. 405 U.S. 438ff.

Elgesem, Dag. 1999. "The Structure of Rights in Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data." *Ethics and Information Technology* 1, no. 4:283–89.

Fried, Charles. 1990. "Privacy: A Rational Context." In *Computers, Ethics, and Society*, edited by M. David Ermann, Mary B. Williams, and Claudio Guitierrez, 50–63. New York: Oxford University Press.

Fulda, Joseph S. 2004. "Data Mining and Privacy." In *Readings in CyberEthics*, 2d edition, edited by Richard A. Spinello and Herman T. Tavani, 413–17. Sudbury, Mass.: Jones and Bartlett.

Gavison, Ruth. 1980. "Privacy and the Limits of the Law." *Yale Law Journal* 89:421–71.

Grodzinsky, Frances S., and Herman T. Tavani. 2005. "P2P Networks and the *Verizon v. RIAA* Case: Implications for Personal Privacy and Intellectual Property." *Ethics and Information Technology* 7, no. 4: 243–50.

Griswold v. Connecticut. 1965. 381 U.S. 479ff.

Hunter, Larry. 1995. "Public Image." In *Computers, Ethics, and Social Values*, edited by Deborah G. Johnson and Helen Nissenbaum, 293–99. Englewood Cliffs, N.J.: Prentice Hall.

Johnson, Deborah. G. 2001. "Computers and Privacy." In *Computer Ethics*, 3d edition, 81–102. Upper Saddle River, N.J.: Prentice Hall.

Johnson, Deborah G., and Helen Nissenbaum. 1995. "Privacy and Databases." In *Computers, Ethics, and Social Values*, edited by Deborah G. Johnson and Helen Nissenbaum, 262–68. Englewood Cliffs, N.J.: Prentice Hall.

Miller, Arthur. 1971. *The Assault on Privacy*. Cambridge: Harvard University Press.

Moor, James H. 1990. "The Ethics of Privacy Protection." *Library Trends* 39, nos. 1 and 2 (Summer/Fall): 69–82.

———. 1997. "Towards a Theory of Privacy in the Information Age." *Computers and Society* 27, no. 3 (September): 27–32.

———. 1999. "Using Genetic Information While Protecting the Privacy of the Soul." *Ethics and Information Technology* 1, no. 4:257–63.

———. 2004. "Toward an Approach to Privacy in Public: Challenges of Information Technology." In *Readings in CyberEthics*, 2d edition, edited by Richard A. Spinello and Herman T. Tavani, 450–61. Sudbury, Mass.: Jones and Bartlett.

Nissenbaum, Helen. 1998. "Protecting Privacy in an Information Age." *Law and Philosophy* 17:559–96.

Olmstead v. U.S. 1928. 277 U.S. 438ff.

Parent, W. A. 1983. "Privacy, Morality and the Law." *Philosophy and Public Affairs* 12, no. 4:269–88.

Posner, Richard A. 1978. "An Economic Theory of Privacy." *Regulations* (May–June):19–26.

Rachels, James. 1975. "Why Privacy Is Important." *Philosophy and Public Affairs* 4, no. 4:323–33.

Regan, Priscilla M. 1995. *Legislating Privacy: Technology, Social Values, and Public Policy*. Chapel Hill, N.C.: University of North Carolina Press.

Scanlon, Thomas. 1975. "Thompson on Privacy." *Philosophy and Public Affairs* 4, no. 4:315–22.

Schoeman, Ferdinand D. 1992. *Privacy and Social Freedom*. Cambridge: Cambridge University Press.

Tavani, Herman T. 1999. "KDD, Data Mining, and the Challenge for Normative Privacy." *Ethics and Information Technology* 1, no. 4: 265–73.

———. 2000. "Privacy and Security." In *Internet Ethics*, edited by Duncan Langford, 65–95. London: Macmillan.

———. 2004. "Privacy and Cyberspace." In *Ethics and Technology: Ethical Issues in an Age of Information and Communication Technology*, 117–51. Hoboken, N.J.: John Wiley.

———. 2006. "Environmental Genomics, Data Mining, and Informed Consent." In *Ethics, Computing, and Genomics*, edited by Herman T. Tavani, 167–85. Sudbury, Mass.: Jones and Bartlett.

Tavani, Herman T., and James H. Moor. 2001. "Privacy Protection, Control of Information, and Privacy-Enhancing Technologies." *Computers and Society* 31, no. 1:6–11.

Thompson, Paul B. 2001. "Privacy, Secrecy, and Security." *Ethics and Information Technology* 3, no. 1:13–19.

Thomson, Judith Jarvis. 1975. "The Right to Privacy." *Philosophy and Public Affairs* 12, no. 4:295–315.

Vedder, Anton H. 2004. "KDD, Privacy, Individuality, and Fairness." In *Readings in CyberEthics*, 2d edition, edited by Richard A. Spinello and Herman T. Tavani, 404–12. Sudbury, Mass.: Jones and Bartlett.

Volkman, Richard. 2003. "Privacy as Life, Liberty, Property." *Ethics and Information Technology* 5, no. 4:199–210.

Warren, Samuel, and Louis Brandeis. 1890. "The Right to Privacy." *Harvard Law Review* 14, no. 5:193–220.
Weinstein, Michael A. 1971. "The Uses of Privacy in the Good Life." In *Nomos XIII: Privacy*, edited by J. Roland Pennock and John W. Chapman, 88–104. New York: Atherton Press.
Westin, Alan F. 1967. *Privacy and Freedom*. New York: Atheneum Press.
Whelan v. Roe. 1977. 429 U.S. 589ff.