ETHICS & BEHAVIOR, 7(3), 207–219

Toward an Approach to Privacy in Public: Challenges of Information Technology

Helen Nissenbaum
University Center for Human Values
Princeton University

This article highlights a contemporary privacy problem that falls outside the scope of dominant theoretical approaches. Although these approaches emphasize the connection between privacy and a protected personal (or intimate) sphere, many individuals perceive a threat to privacy in the widespread collection of information even in realms normally considered "public." In identifying and describing the problem of privacy in public, this article is preliminary work in a larger effort to map out future theoretical directions.

Key words: privacy, information technology

Many influential approaches to privacy emphasize the role of privacy in safeguarding a personal or intimate realm where people may escape the prying and interference of others. This *private realm,* which is contrasted with a *public realm,* is defined in various ways. It is delimited by physical boundaries, such as the home; by personal relationships, such as family, friends, and intimates; and by selected fields of information, such as personal, sensitive, or embarrassing information. Privacy is worthy of safeguarding, these approaches argue, because intimacy is important; privacy is worth protecting because we value the sanctity of a personal realm.

This article does not dispute the importance of securing intimate and personal realms. Nor does it challenge the compelling connection between privacy norms and the ability to protect these realms against unwarranted intrusion. It argues, however, that an account of privacy is not complete that stops with the intimate and

Requests for reprints should be sent to Helen Nissenbaum, University Center for Human Values, Marx Hall, Princeton University, Princeton, NJ 08544.

personal realms. The widespread use of information technology, such as in personal profiling, to assemble and transmit vast stores of information—even so-called "public" information—has shown than an adequate account of privacy should neither neglect the nonintimate realm nor explicitly exclude it from consideration. Loud calls of public protest in response to information harvesting strongly indicate that implicit norms of privacy are not restricted to personal zones. I henceforth call this challenge to existing theoretical frameworks the problem of protecting "privacy in public."

PRIVACY AND THE PERSONAL REALM—BACKGROUND

The idea that privacy functions to protect the integrity of a private or intimate realm spans scholarly work in many disciplines, including legal, political, and philosophical discussions of privacy. James Fitzjames Stephen (1873), a 19th century British legal theorist, wrote in his treatise on law, "there is a sphere, nonetheless real because it is impossible to define its limits, within which the law and public opinion are intruders likely to do more harm than good" (p. 160). The political scientist Carl Friedrichs (1971) remarked that the goal of legal protections is "primarily that of protecting the private sphere against intruders, whether government or not" (p. 105). Law in many countries recognizes realms that are basically off-limits. In the United States, for example, constitutional prohibitions on unreasonable searches and seizure, protection against self-incrimination, and guarantees of freedom of conscience delineate for each citizen a personal zone that is free from the prying and interference of government. This zone covers the home and personal effects as well as certain areas of his life such as family, "conscience," sexual and marital relations, and reproduction.[1] Tort Law has also helped insulate this personal zone against intrusion by nongovernmental agents.

Prominent among contemporary philosophical works on privacy is Charles Fried's. Fried (1984) argued that privacy is important because it renders possible important human relationships. Privacy provides "the necessary context for relationships which we would hardly be human if we had to do without—the relationships of love, friendship and trust" (p. 211). Although Fried conceived of privacy as control over all information about oneself, he defended a moral and legal right to privacy that extends only over the far more limited domain of intimate, or personal, information. He accepted this narrowing of scope because even a limited domain of intimate or personal information provides sufficient "currency" for people to differentiate relationships of varying degrees of intimacy. The danger of

[1]For an excellent discussion see DeCew (1986).

extending control over too broad a spectrum of information is that privacy may then interfere with other social and legal values. Fried wrote, "The important thing is that there be some information which is protected" (p. 214), namely, information about the personal and intimate aspects of life. According to Fried, the precise content of the class of protected information will be determined largely by social and cultural convention. Prevailing social order "designates certain areas, intrinsically no more private that other areas, as symbolic of the whole institution of privacy, and thus deserving of protection beyond their particular importance" (p. 214).

Other philosophers also have focused on the interdependence between privacy and a personal or intimate realm. Robert Gerstein (1984), for example, contended that "intimacy simply could not exist unless people had the opportunity for privacy. Excluding outsiders and resenting their uninvited intrusions are essential parts of having an intimate relationship" (p. 271). Ferdinand Schoeman (1984) noted that "one's private sphere in some sense can be equated with those areas of a person's life which are considered intimate or innermost" (p. 412). Privacy's purpose, he wrote, is to insulate "individual objectives from social scrutiny. Social scrutiny can generally be expected to move individuals in the direction of the socially useful. Privacy insulates people from this kind of accountability and thereby protects the realm of the personal" (p. 415). Schoeman, unlike Fried (1984) however, holds that there are domains of life that are essentially private and not merely determined to be so by social convention.

The views of Schoeman, Fried, and Gerstein, though differing in detail, rest on a common core. Each held that properly functioning, psychically healthy individuals need privacy. Privacy assures these people a space in which they are free of public scrutiny, judgment, and accountability, and in which they may unselfconsciously develop intimate relationships with others.

Other philosophical discussions are less motivated by this underlying conception of human need and more by a perceived need to sharpen the concept and definition of privacy. William Parent (1983), for example, rejected the many over-broad definitions and offered in their places a definition of privacy as "the condition of not having undocumented personal knowledge about one possessed by others" (p. 269). By personal facts Parent means "facts which most persons in a given society choose not to reveal about themselves (except to close friends, family, . . .) or facts about which a particular individual is acutely sensitive" (p. 270). In contemporary America this covers "facts about a person's sexual preferences, drinking or drug habits, income, the state of his or her marriage and health" (p. 270). By "undocumented" Parent means information that has not appeared in a "newspaper, court proceedings, and other official documents open to public inspection" (p. 270). A person's right to privacy restricts access by others to this sphere of personal, undocumented information unless, in any given case, there are other moral rights that clearly outweigh privacy. Although many other writers who have highlighted the connection between privacy and the personal realm have not attended merely

to the status of the "non-personal" realm, Parent is explicit in excluding it. If information is not personal information or if it is documented, then action taken with respect to it simply does not bear on privacy.

Raymond Waks (1989), who is also motivated by the need for a more precise definition with clear boundaries, laid down this foundation:

> At the heart of the concern to protect "privacy" lies a conception of the individual and his or her relationship with society. The idea of private and public spheres or activity assumes a community in which not only does such a division make sense, but the institutional and structural arrangements that facilitate an organic representation of this kind are present. (p. 7)

The work of a theory of privacy is to define legitimate boundaries between these spheres. Like Parent (1983), Waks (1989) did not extend the conception of privacy to freedom of action (such as the right to abortion) but placed at the core of his definition of the right to privacy its "protection against the misuse of personal, sensitive information" (p. 10).

Tom Gerety (1977), too, sought more rigor in his proposed definition of privacy. According to Gerety, the problem of privacy as a legal and moral concept

> comes not from the concept's meagerness but from its amplitude, for it has a protean capacity to be all things to all lawyers. . . . A legal concept will do us little good if it expands like a gas to fill up the available space. (p. 234)

Gerety characterized privacy as a "legal island of personal autonomy in the midst of a sea of public regulation and interaction" (p. 271). The scope of this autonomy is limited to the "intimacies of personal identity" (p. 281). This, and only this, is the domain of privacy.

VIOLATING PRIVACY IN PUBLIC—THE CASE OF LOTUS MARKETPLACE: HOUSEHOLDS

The approaches described earlier are problematic not because they develop normative accounts of privacy that protect the personal and intimate realms from interference, but because they neglect the relevance to privacy of realms other than the intimate and sensitive. Some, like Parent's and Gerety's, go even further to explicitly deny it. In excluding all but the personal and intimate, they effectively disarm their normative accounts of privacy against one of the most vexing challenges that information technology currently poses. Almost 12 years ago, Hunter (1985) predicted "Our revolution will not be in gathering data—don't look for TV cameras in your bedroom—but in analyzing the information that is already willingly shared" (p. 32). Hunter's comment makes an almost paradoxical point: We

are complicit in an invasion of our own privacy that ultimately we find objectionable. The invasion is not from the realm of the intimate but from the realm that is generally not given serious consideration by many noted theorists of privacy.[2]

Lotus Marketplace: Households,[3] a case that has attracted a great deal of attention among privacy policy advocates, illustrates the distance between public perception of what counts as an unwarranted invasion of privacy and what may be inferred from some of the theoretical positions outlined earlier. In April 1990, Lotus Development Corporation, a developer and marketer of popular software, and Equifax Inc., a company that collects and sells information about consumer financial transactions, announced their intention to produce a comprehensive database called "Lotus Marketplace: Households" that would contain actual and inferred information about approximately 120 million individuals in the United States. It would include name, address, type of dwelling, marital status, gender, age, household income, lifestyle, and purchasing propensity. The two companies expected that the database, which was to have been recorded and sold in the format of a CD-ROM, would be widely adopted by marketers and mailing companies.[4]

They did not, however, anticipate the vigorous public outcry against Lotus Marketplace: Households. An estimated 30,000 letters of protest expressed its displeasure. Defenders were astonished. How was it possible to construe Lotus Marketplace as an invasion of privacy when the information it contained was taken from public sources only and not by violating any sensitive or personal realms? It was to be compiled from information already "out there" and would use no intrusive means to gain information of a personal or intimate nature—no hidden cameras in bedrooms. Information was to be harvested from public records and from records of transactions that individuals carried out in the public arena and made no efforts to hide. No private zones would be breached, the integrity of home and family would be respected, embarrassing personal facts would not be revealed. Defenders argued, furthermore, that opposition to Lotus Marketplace violated the right of its creators to pursue profitable enterprise.

Nevertheless, in January 1991, executives of Lotus Development Corporation and Equifax Inc. announced that they were canceling Lotus Marketplace, insisting that their decision was prompted by negative public reaction and misunderstanding and not because of any real threat to privacy. Normative theories of privacy like the ones advanced by Parent, Gerety, and Waks were compatible with the views expressed by the executives. Gerety (1977), for example, in commenting on

[2]There are exceptions. Schoeman may be the clearest case. In contemporary work on policy issues, privacy advocates and policy analysts such as Regan, Rotenberg, and Goldman have been very vocal in these issues.

[3]For a fuller description of the case see Culnan and Smith (1995).

[4]Other industry analysts were also very encouraging. An interesting example is Esther Dyson, now head of the Electronic Frontier Foundation, in a *Forbes* magazine column (Dyson, 1990).

compilations of nonintimate data wrote, "In these matters privacy affords us a convenient rhetoric of advocacy and legitimacy. Nonetheless, it is not the issue at bottom" (p. 291). And Parent (1983) wrote that as long as the information is neither personal, nor undocumented, it "cannot without glaring paradox be called private" (p. 271).

Although privacy advocates and activists may regard the outcome of Lotus Marketplace Households a victory for privacy, in hindsight the victory appears thin. The loud and determined public outcry carried the day. But if the course of electronic profiling was stalled, it was stalled only temporarily. Personal data services satisfying virtually any conceivable need proliferate at a furious pace. Since Lotus Marketplace, no single case has served as an equivalent lightening rod for public action. Despite the absence of dramatic reaction, however, measures of public opinion continue to show the persistent sense that databases of so-called "public" information do violate privacy. For example, in June 1994, when ABC's *Nightline* anchor Ted Koppel conducted a poll, 73% of respondents said they viewed the sale of records to mail-order companies to be an invasion of privacy. Following Parent, Gerety, and Waks, one may attribute this public reaction to fuzzy thinking. A better alternative, if we are to develop a more meaningful concept of privacy, is to give serious consideration to the concerns expressed in public reactions to Lotus Marketplace and to the opinions from the *Nightline* (and other) polls. Precision may be a worthy goal of scholarship, but not at the cost of missing a significant and persistent worry.

There is a reason, I think, in this divergence of theoretical implications and observed public opinion. Here is where information technology enters the picture. Whereas prior to the proliferation of databases of so-called "public" information, normative theories that focused on protecting a personal realm offered a good approximation to the actual threats to privacy (namely, government intruding into personal lives), it now no longer covers the full sense of what is valuable about privacy, and fails to capture aspects of privacy that we care about. Where previously, physical barriers and inconvenience might have discouraged all but the most tenacious from ferreting out information, technology makes this available at the click of a button or for a few dollars. This has dramatically expanded the scope of what is possible with even public information. As a result, dominant legal and philosophical theory, which has been serviceable until now, is no longer in step with moral norms. Theory tells us Lotus Marketplace is permissible; our norms tell us "no."

TWO MISLEADING ASSUMPTIONS

I argued earlier that if a theory of privacy is not able to give an account of personal information in the so-called "public realm," then it is unable to meet one of the central challenges of information technology. Although ultimately our aim should

be to generate an alternative theoretical framework, or an extension of existing theory, that would meet these new challenges, the following discussion attempts only to clear a way toward this more ambitious goal. It directs attention to two commonly held, but misleading, assumptions about the nonintimate realm and its relation to privacy. These assumptions, cast by supporters as truisms, stand in the way of an adequate conception of privacy.

Erroneous Assumption 1: There is a realm of public information about persons to which no privacy norms apply.

This assumption holds that there is a category of information about persons that is perfectly public (public in a normative sense), which is "up for grabs" for anyone with an interest in and use for it, for which "anything goes." This category, generated by default, consists of information accepted by broad consensus in a given society not to belong to the personal, sensitive, or intimate zone, and not acquired by eavesdropping, spying, or other means generally considered intrusive. Widespread use and abuse of information about persons rests on this assumption.

I argue later that even if, on the one hand, there is broad consensus on what information may be classified personal and intimate, there is, on the other hand, little, if anything, that people universally would admit into a completely public realm if by that we mean that it is governed by no norms of privacy whatever.[5]

Let us consider what might be meant by a category of information for which "anything goes." What might this category include? How might we define it? One possibility is to define the category of public information in terms of a category we understand more directly; namely, that of a public place. Accordingly, public information would include any information observed and recorded in a public place, in keeping with Reiman's (1984) suggestion that the social practice of privacy "does not assert a right never to be seen even on a crowded street" (p. 319). It would be reasonable to conclude, therefore, that information harvested in a public place is "up for grabs" and not covered by norms of privacy.

This proposal would only work if at least two things hold: one, that judgment confirms the inference from public space to public (in this strong sense) information; and another, judgments about information are indeed derivable from judgments about the nature of the place. It is not clear, however, that either of these hold. In the first place, the idea that we judge information to be public merely

[5]Reiman (1984) wrote,

> Privacy is a social practice. It involves a complex of behaviors that stretches from refraining from asking questions about what it none of one's business to refraining from looking into open windows one passes on the street, from refraining from entering a closed door without knocking to refraining from knocking down a locked door without a warrant. (p. 310)

For another account of privacy norms, see Schoeman (1994).

because it is acquired in a public arena is readily challenged. Consider Schoeman's (1994) remarks,

> Just because something happens in public does not mean it becomes a public fact: the Central Park rape occurred in public as did the trial of the accused, but the victim maintains a measure of privacy as to her identity. In less dramatic cases, the notion of civil inattention directs us to the same realization. (p. 81)

In general, even if we agree that a number of familiar places are not part of the "intimate" and private realms, we would not therefore agree that any information harvested from them is completely public. This would mean that facts gleaned from arenas such as public schools, supermarkets, parks, and libraries belong in a category of public information in the strongest sense. By contrast, even quintessential public places—a public square or sidewalk—are governed by some norms of privacy. It would be within one's rights to reply "none of your business" to a stranger who asks your name.

In the second place, at times our public sentiments suggest that the idea of private information may not be derivable from ideas of public space. This is demonstrated in cases where a change of determination occurs as a result of a traumatic incident or public discussion. In 1988, for example, after a newspaper published videotape rental records of then-nominee to the Supreme Court, Robert Bork, the U.S. Congress passed the Video Privacy Protection Act of 1988, which reversed the status of video rental records from public to private (see Regan, 1995). Even though the setting did not change—transactions still occurred in the video rental store—a societal judgment shifted video rentals records from public to private. In other words, privacy norms are not necessarily derivable from setting but can come prior.

Another contender for a category of information that is "up for grabs" is information found in public records such as birth and death records, real estate records, and court records. Here too, however, people are beginning to question the inference that if information is in a public record then it is perfectly public. These doubts have been expressed not only by members of the public but by public officials. In two recent court cases in New Jersey, the New Jersey Supreme Court explicitly asserted that we may not conclude, just because information exists in a public record, that the information is not subject to restrictions in distribution and use.

In *Higg-A-Rella Inc. v. County of Essex,* the Court recognized that the form of public records—computerized versus paper—can affect de facto privacy protection. Even though it ruled in favor of Higg-A-Rella in its bid to gain access to computerized records of municipal tax-assessment data, it stated that

> Release of information on computer tape in many instances is far more revealing than release of hard copies, and offer the potential for far more intrusive inspections. Unlike paper records, computerized records can be easily retrieved, researched, and

> reassembled in novel and unique ways, not previously imagined. (*Higg-A-Rella, Inc. v. County of Essex,* 1995, p. 52)

In another ruling, *Doe v. Poritz,* the New Jersey Supreme Court noted that "an individual's right in controlling the dissemination of information regarding personal matters does not dissolve simply because that information may be available to the public in some form" (*Doe v. Poritz,* 1995, p. 83). The court thereby does not allow us to infer from the presence of information in a public record that it is entirely "up for grabs." By the same token, in states where the names of rape victims are part of the public records there is support for the idea that victims of rape, or for that matter, victims and families of victims of other crime, retain some measure of control over the information about them. Just because people are able to learn these facts by referring to public records does not imply a right to distribute and use the information in any way they choose.

The free dissemination of drivers' records information has also come under public scrutiny and opposition. The murder of actress Rebecca Schaeffer and, as a result, better public understanding of the status of drivers' records led to a revision in the law. Previously, state departments of motor vehicles treated drivers' records as public records—no-holds barred. The Driver's Privacy Protection Act of 1993, which was incorporated into the Violent Crime Control and Law Enforcement Act of 1994, changed this by limiting access to these records. It allows drivers to opt out of lists that previously were freely disseminated by departments of motor vehicles. Here, too, is an example of the way concern over privacy has led to a reevaluation of the norms associated with "public records."[6]

What I have tried to show is that even for two of the most plausible contenders for the category of personal information "up for grabs," there are significant problems. At root, I believe, is a mismatch between intuitively held privacy norms as applied to information and the much touted private–public dichotomy. A promising alternative rejects the relevance of the dichotomy to information about persons in favor of the idea of a multiplicity of contexts. Information learned in one context belongs in that context and is public vis à vis that context. We do not have a dichotomy of two realms but a panoply of realms; something considered public in relation to one realm may be private in relation to another, "disclosure of information to groups, even potentially large groups, might still be considered private provided still larger groups were excluded" (Schoeman, 1984). People count on this contextual integrity as an effective protection of privacy. Nightclub patrons may not mind being seen by other patrons but may reasonably object to having their actions reported outside of that context. Shoppers may not object to using open shopping carts but may sense violation if inquisitive neighbors noted and reported elsewhere on their purchases. Similarly, information such as the number and

[6]For a more complete discussion, see Regan (1995, p. 103).

identities of a person's children, the gender and identity of one's live-in partner, and so forth are facts freely available in some contexts (that is, are "public" in some realms) but considered private in others.[7]

Two philosophers, Schoeman and Rachels, offer additional reasons for protecting contextual integrity. Whereas Fried argued for a single dimension stretching from intimate, on the one end, to public, on the other, Schoeman and Rachels suggested a multiplicity. Privacy, in enabling individuals to maintain contextual integrity, enables them to develop a variety of distinct relationships. Schoeman (1984) wrote, "People have, and it is important that they maintain, different relationships with different people. Information appropriate in the context of one relationship may not be appropriate in another" (p. 408). Rachels (1984) argued that

> the value of privacy based on the idea that there is a close connection between our ability to control who has access to us and to information about us, and our ability to create and maintain different sorts of social relationships with different people. (p. 292)

Erroneous Assumption 2: An aggregation of information does not violate privacy if its parts, taken individually, do not.

At first hearing, the logic behind the assumption may seem unassailable. Consider the rhetoric: Assemble innocuous bits of information and you will have an innocuous assemblage of information, a "benign composite of humdrum data." The assumption plays an important role in defending a position that databases of nonsensitive information are nonsensitive. On closer scrutiny, however, the assumption, and along with it the many activities it supports, are questionable. When bits of information are aggregated, compiled, and assembled, they can be invasive of privacy even if when taken individually they are not. (The remarks that follow are merely suggestive. A fuller discussion, which develops when and why aggregations may violate privacy, is beyond the scope of what I am able to cover in this article.)

Experience with databases of personal information has left no doubt that the value of information can be seriously affected by combining and compiling it with other information. Metaphorically speaking, with information one *can* sew a silk purse out of a sow's ear. Ware (1991) noted, "A whole industry thrives on assembling and selling data"; countless businesses profit from hawking assem-

[7]Some may argue that if information is "in public" then it is obviously up for grabs. This conclusion is far from compelling. As we see in the case of intellectual property, an intellectual work can be viewed (sung, displayed) in public but still be controlled in important ways by its author or owner. In a similar way, despite public display or availability, subjects may continue to maintain control. I do not mean by this that privacy rights are a form of intellectual property rights but that they share this feature.

blages and compilations of otherwise worthless bits of personal information. A single fact about someone takes on a new dimension when it is combined with other facts about the individual, or when it is compared with similar facts about other individuals. Applying ingenuity to one-dimensional bits of information can transform mere "noise" and statistical data into rich portraits of people. Through the powers of information technology we acquire the capability not only to collect and store vast amounts of information, but to bring order to it, to manipulate it and to draw meaningful inferences from it. By these actions we are able to inject shape and also value into a riot of formless data.

At the same time, the capacity to manipulate information in these ways may have significant bearing on the humans who are its subjects. First, the act of compiling almost always involves shifting information from one context to another; it involves using information in a manner not explicitly announced when the information was initially collected. This means that unless the subjects of the information have explicitly granted permission to move it around, they have effectively lost control over it. Moreover, as suggested earlier, although the broadcast of information in one context is perfectly apt, it may be highly inappropriate, demeaning, or awkward when broadcast in another.

The act of compiling information may also transform harmless bits into a picture that can embarrass and hurt. Even when there is no call for this degree of accountability, even when discrete bits of information are all that are needed to carry out efficient transactions with a given agency or business these bits may be conjoined with other bits to form rich portraits capable of revealing character, identity, personality, and lifestyle. "In the information age, our public acts disclose our private dispositions, even more than a camera in the bedroom would," writes Larry Hunter (1985). The subjects of these portraits, or profiles, may well ask what right those who compile the information have to the insights and access to their lives and personalities that these portraits provide. Moreover, portraits are developed not for the purpose of developing friendship or intimate association, but to manipulate, motivate, and judge; to make decisions that will affect the lives of their subjects in important ways.

To sense the nature of this affront, imagine oneself the subject of general but constant surveillance. Although assurances that it covers only nonintimate realms may provide some consolation, the omnipresent record-taking opens one to unbearable exposure.

CONCLUSION: IMPLICATIONS FOR A THEORY OF PRIVACY

This article urges a conception of privacy that would extend consideration to all information, including information gathered in so-called public realms. If successful, it would also block two misleading assumptions that both implicitly and

explicitly have been invoked by those who would justify compilation of complex databases of nonintimate information. Existing theories that limit the scope of privacy to a personal zone or to intimate and sensitive information fail to capture elements of common real-world judgments. Public reaction to Lotus Marketplace: Households and similar computerized databases of nonsensitive information indicates that, by contrast, our common notion of privacy is not thus limited. The power of computers and networks to gather and synthesize information exposes individuals to the scrutiny of others in unprecedented ways. Although guarding the intimate realm against unwarranted invasion is an important aspect of protecting privacy, information technology indicates a need for a more inclusive theory. Neglecting the broader sphere will rob from people the ease and comfort of anonymity as they stroll through actual town squares as well as electronic town squares, conduct trade, socialize, and engage in political and recreational activity both on and off line. It will deprive them of privacy in public.

ACKNOWLEDGMENTS

I acknowledge the perceptive comments of Jonathan Schonsheck and members of the audience. Thanks also to Grayson Barber and Julian Gorelli for legal insights and for drawing attention to recent important and relevant New Jersey cases.

REFERENCES

Culnan, M. J., & Smith, H. J. (1995). Lotus Marketplace: Households . . . Managing information privacy concerns. In D. G. Johnson & H. Nissenbaum (Eds.), *Computers, ethics and social values* (pp. 269–278). Englewood Cliffs, NJ: Prentice Hall.

DeCew, J. W. (1986). The scope of privacy in law and ethics. *Law and Philosophy, 5,* 145–173

Doe v. Poritz, 142 N.J. 1 (1995).

Dyson, E. (1990, April 30). Data is dandy. *Forbes,* p. 180.

Fried, C. (1984) Privacy. In F. Schoeman (Ed.), *Philosophical dimensions of privacy: An anthology* (pp. 203–222). Cambridge, England: Cambridge University Press.

Friedrichs, C. (1971). Secrecy versus privacy: The democratic dilemma. In J. R. Pennock & J. W. Chapman (Eds.), *Privacy: Nomos XIIII* (pp. 105–120). New York: Atherton.

Gerety, T. (1977). Redefining privacy. *Harvard Civil Rights-Civil Liberties Law Review, 12*(2), 233–293

Gerstein, R. (1984). Intimacy and privacy. *Philosophical dimensions of privacy: An anthology.* Cambridge, England: Cambridge University Press.

Higg-A-Rella, Inc. v. County of Essex. 141 N.J. 35 (1985).

Hunter, L. (1985, January). Public image. *Whole Earth Review,* 32–37

Parent, W. (1983). Privacy, morality, and the law. *Philosophy & Public Affairs, 12*(5), 269–288

Rachels, J. (1984). Why privacy is important. In F. Schoeman (Ed.), *Philosophical dimensions of privacy* (pp. 290–299). Cambridge, England: Cambridge University Press.

Regan, P. (1995). *Legislating privacy: Technology, social values, and public policy.* Chapel Hill: University of North Carolina Press.

Reiman, J. (1984). Privacy, intimacy and personhood. In F. Schoeman (Ed.), *Philosophical dimensions of privacy: An anthology* (pp. 300–316). Cambridge, England: Cambridge University Press.

Schoeman, F. (Ed.). (1984). Privacy and intimate information. *Philosophical dimensions of privacy: An anthology.* Cambridge, England: Cambridge University Press.

Schoeman, F. (1994). Gossip and privacy. In R. F. Goodman & A. B. Ze'ev (Eds.), *Good gossip* (pp. 72–84). Lawrence: University Press of Kansas.

Stephen, J. F. (1873). *Liberty, equality and fraternity.* New York: Holt.

Waks, R. (1989). *Personal information: Privacy and the law* Oxford, England: Clarendon.

Ware, W. H. (1991, August). *Contemporary privacy issues.* Address given at the National Convention on Computing and Values, New Haven, CT.