CERIAS Tech Report 2000-18

PRIVACY, SECRECY, AND SECURITY

by Paul B. Thompson

Center for Education and Research in
Information Assurance and Security,
Purdue University, West Lafayette, IN 47909

Privacy, Secrecy and Security

Paul B. Thompson
Philosophy Department
Purdue University
West Lafayette, IN 47907-1360
U.S.A.
Telephone: 765 463-5782 FAX: 765 496-1616
Email: pault@purdue.edu

2000-10

ABSTRACT

I will argue that one class of issues in computer ethics often associated with privacy and a putative right to privacy is best-analyzed in terms that make no substantive reference to privacy at all. These issues concern the way that networked information technology creates new ways in which conventional rights to personal security can be threatened. However one chooses to analyze rights, rights to secure person and property will be ~~will be~~ among the most basic, the least controversial and the most universally recognized. A risk-based approach to these issues provides a clearer statement of what is ethically important, as well as what is ethically problematic. Once the issues of security have articulated clearly, it becomes possible to make out genuine issues of privacy in contrast to them.

KEYWORDS: PRIVACY, DATA-SECURITY, LOGICAL SECURITY, PERSONAL SECURITY, RISK

INTRODUCTION

Within law, ethics and public affairs, the term 'privacy' does not specify a particular concept or good so much as it indicates a class of issues related to one another as much by habit and convenience as by unity of content or conceptual similarity. The seminal article of Warren and Brandeis (1890) initiated the view that privacy is a positive good, and that individuals and non-governmental organizations have an interest in maintaining a political right to privacy. This was, in Warren and Brandeis words, a 'right to be let alone.' The right to privacy prohibits intrusion upon a person's seclusion or solitude not only by government, but also by other parties. In the intervening decades, the notion of privacy has been subjected to expansive reinterpretation by lumpers who make very broad claims for privacy and even describe it as the quintessential political right. Much of the recent literature on privacy and information technology is characteristic of this tendency.

This paper is an exercise in splitting. My general presumption is that we cannot arrive a clear understanding of why information technology might threaten privacy in the narrow and important sense that does follow from Warren and Brandeis's original analysis so long as our attention is directed to moral issues that do not depend upon that analysis or its legitimate successors. I will not argue for this thesis directly, but I will describe a class of ethical issues that involve secrecy and confidentiality in a manner that does not require reference to privacy. I will sketch a framework for the analysis of these issues that frames them as issues of security and risk, rather than privacy. Once this class of issues has been described, the true issues of privacy can be characterized in contrast to them. But any substantive discussion of these issues falls beyond the scope of the present discussion.

PRIVACY AND SECRECY

Privacy has become a standard issue for computer ethics, but why is privacy important, and why would information technology bear upon it? Stacey Edgar's book *Morality and Machine: Perspectives in Computer Ethics* (1997) interprets privacy as a straightforward extension of Lockean non-interference rights and Kantian autonomy, then offers some indicative examples of how computers have been used to

violate privacy. These include the 1989 murder of actress Rebecca Shaeffer, whose assailant obtained her address from an electronic database, and the use of computers to reproduce an unpublished text from the Dead Sea Scrolls from a published concordance of key words. Mary B. Williams (1997) cites examples of electronic surveillance, noting the emotional stress felt by workers who are aware that their movements might be monitored at any time, and also notes how economic data analysis can be used in making decisions such as whether to retain an employee or make a loan. This leads her to characterize privacy as an instrumental, rather than an intrinsic value, and to conclude that remedies which govern the control and flow of data can mitigate the risks of information abuse. Articles in Williams' anthology (with David Ermann and Michelle Shauf) discuss electronic fraud, the security of electronic transactions and the technical and legal approaches that have been developed to combat these problems.

Edgar and Williams exemplify an expansive approach to the interpretation of privacy. In the cases noted, computers have been or could be used to make the violation of personal security rights easier and more convenient for the criminal. Other authors are more focused on legitimate actors than the criminal class. David Lyon and Elia Zureik (1995) describe an approach to privacy based on sociological theories of social control and the expansion of state power. Marxian, Weberian and Foucouldian social theories each stress the state's growing capacity to maintain surveillance over its population as an expression of social power. In addition, Daniel Bell's *The Coming of Post-Industrial Society* stressed the growth of technology and technical elites as a new source of social power that will limit democratic control and the growth of civil society. (Sparks, 1994). Theorists working in these sociological traditions have tended to interpret the emergence of computerized information technology and the new forms of surveillance that it enables as an evolution in social power relations that favors governmental and commercial organizations against the interests of individual citizens. Like Edgar and Williams, these theorists use an expansive interpretation of privacy, and presume that privacy subsumes a broad class of moral rights and civil liberties.

Calvin Gotlieb (1995) has criticized this literature on two counts. First, it takes a sweeping approach that neglects important distinctions between kinds of interests affected by computerization. Second, it downplays the voluntary nature of the way in which individuals have surrendered control over personal information in exchange for the benefits that information technology brings. Gotlieb begins with a set of definitions:

> **Privacy** is a social, cultural and legal concept, all three aspects of which vary from country to country. **Confidentiality** is a managerial responsibility: it concerns the problems of how to manage data by rules that are satisfactory to both the managers of data banks and the persons about whom the data pertain. **Security** is a technical issue. It focuses on how the rules of data access established by management can be enforced, through the use of passwords, cryptography, and like techniques. [p. 156, emphasis added]

Gotlieb's thesis is that while confidentiality continues to be an important ethical problem for computer professions, and security is an increasingly important technical issue, privacy is a red herring. 'What must be secured in every civilized and free society,' he writes, 'is, of course, security of person,' (p. 168). While security of personal data may be instrumental for this purpose, 'data security is a very different thing from privacy,' (p. 169).

I would like to build upon the first of Gotlieb's critiques and the distinctions that he draws without endorsing his broader conclusions. In distinguishing privacy and data security, Gotleib follows an approach that has been taken in the technical literature for some time (Spafford, Heaphy and Ferbrache, 1989; Bynom, 1998). I am, however, more interested in the way that Gotleib links data security and personal security. This, too, is not without precedent. In a 1975 article, James Rachels lists several cases where 'information about a person might provide someone with a reason for mistreating him in some way.' Rachels suggests that such cases are misleading when they are taken to indicate why privacy is important. Rachels main thesis is that we have a need to maintain different types of relationships with different people, and that our notion of privacy is better elucidated by attending to these differences than to instances where information might be used in an abusive way. Unlike Gotleib, Rachels is far from dismissive about the value of privacy, but like him, he dissociates the abuse of personal information from the issue of privacy.

Sissela Bok published an influential book in 1986 that discussed issues such as the abuse of medical or financial records, and the potential for embarrassment or blackmail when sensitive information is disclosed. Bok analyzed the need that businesses and governments have pursue certain of their activities shielded from the scrutiny of the public and the press, and weighed this need against the public's right to know. The title of bok's book was not 'privacy', but *Secrets*. Though some of the topics in *Secrets* do bear on Warren and Brandeis-style rights to privacy, I think that Bok basically had it right. What is ethically problematic

and interesting in all these cases is more precisely captured when we ask whether secrecy can be defended against a general presumption toward publicity. In many of Bok's examples, secrecy is defensible exactly when we can show that basic rights of personal security and protection of property would be jeopardized without it.

It is easy to see how the lumpers arrive at expansive interpretations of privacy that encompass almost all of Bok's cases, especially when considering the impact of computing and information technology. In some contexts the word 'private' is virtually synonymous with the word 'secret; or 'confidential.' For example, when we say 'She wants to keep some aspect of her life private in order to avoid embarrassment,' or 'Medical records should be kept private,' we can substitute the word 'confidential' for 'private' without altering the meaning of statement. Throughout this paper I will use the terms 'secrecy' and 'confidentiality' almost interchangeably. Notably, these examples (which are among those specifically described by Rachels as misleading) involve cases where disclosure of a secret might be used to harm very non-controversial interests. Medical information can be used to deny employment and other opportunities to which a person is entitled, and embarrassment is a form of emotional harm that can have extreme consequences in certain situations. One need not appeal to a Warren and Brandeis-style privacy right, or to Rachels' notion of relational differences in order to articulate why emotional distress or the denial of opportunity is a bad thing. As Gotleib suggests, these are interests that would be protected in any free and civilized society.

In contrast to Williams claim that privacy is of merely instrumental value, the Warren and Brandeis conception of privacy is clearly intended to articulate a conception of privacy that is of more than instrumental value. Privacy is at least a Rawlsian primary good, a good essential to the realization of any person's conception of the good life. Privacy rights are intended to protect a sphere of activity, often a physical place but sometimes an interpersonal relationship, from intrusion by government and other private parties. Beyond that, privacy can be vague and highly situational, but privacy need not involve secrecy at all. Two roommates might claim that a neighbor's constant pounding violates their privacy, while they could not claim that the annoyances they perpetrate on each other are violations of privacy. They are, instead, competitive uses of a space that they have agreed to share.

Unlike privacy, secrecy appears to have a tight connection to information. If something is secret, there is at least one person to whom information is not known. Yet there are clear cases when general knowledge of private matters does not abrogate their privacy in any morally significant way. A person's religious practices may be widely known, but that in no way makes them less private. Having information about a person's religious practice may make it possible for someone to violate that person's privacy by discriminating for or against them in an inappropriate way. But such information is readily available in most societies. The significance of such information lies not in simple knowledge of it, but in its further use.

Given the vagueness and situational character of privacy, I will not attempt to say a great deal more about Warren and Brandeis style privacy rights in the present context. In the following section I will sketch an approach to the ethics of secrecy as it relates to information systems. Significantly, my approach does not rely on a conception of privacy, or on an extension of the Warren and Brandeis literature.

SECRECY AND SECURITY

There may be innumerably many reasons why people want to keep secrets, but there are three that are particularly relevant to computer technology. First, there are cases where agents bent on harm can be stopped or slowed in their progress when vital information is not readily available. Computers and databases can have an enormous effect on the ease and speed with which criminal intent can be realized. Second, there are cases where information is itself a form of private property that should be protected by rights of personal security. Information technology has had a tremendous impact on the nature and extent of such information. Finally, the functioning of many vital systems for commerce and public protection have now come to be so dependent on computers and electronic data bases that either sabotage or accidental failure of these systems is a threat to public safety and personal security. While each set of cases involves very different ethical considerations in certain respects, they share two features of interest in the present context. First, each set of cases can be usefully elucidated in terms of secrecy and security. Second, there a broad heuristic of risk analysis can be used to characterize a common set of ethical issues. I will first review each the secrecy and security issues involved in each set of cases.

Malicious Intent. The Rebecca Shaeffer case already mentioned illustrates why people may wish to keep fairly unexceptional bits of information—one's address, one's telephone number—as well as sensitive account numbers and passwords out of the hands of those who will use this information in a harmful

manner. Computers and electronic databases have multiplied the types of information that might be so abused, and they have created opportunities for clever people to obtain such information and to exploit it with little chance of detection. This is a fairly unexceptional observation that undoubtedly covers a significant proportion of the cases where computers are alleged to threaten personal privacy, but in many cases it is secrecy in the interest of personal security that is at issue, and nothing more.

Intellectual Property. Computers and digital information systems allow the reproduction, use and exchange of texts, images, audio recordings and a host of other items. When and whether digitized information can be owned, and what ownership entails is, of course, an entirely different and very large issue in computer ethics, but once a property right *is* established, the owner is vulnerable to violations of that right. Expropriation of personal property without permission of the owner is conventionally considered to be a violation of the owner's personal security, though this is certainly a contestable claim. However, those who have their intellectual property stolen electronically have had something taken as sure as if they had been plagiarized or had a patent violated through conventional means. Thus issues of intellectual property are, in one sense, simply a sub-class of issues associated with malicious intent. However, the role of secrecy in protection of intellectual property differs significantly. Secrecy is the essence of trade secrets and of much information that is considered to be proprietary, while both copyright and patents provide legal protections in lieu of secrecy. In any case, theft of copyright, trade secret, patent or even service is not usually considered to be a violation of privacy, though it is clearly a violation of security.

System security. With the Y2K scare and the 'I LOVE YOU' virus, we are becoming depressingly aware of the extent to which our social order and our personal security depends on the proper functioning of information systems. As systems have become linked, system security has come to depend more heavily on various forms of secrecy or logical security, rather than on physical isolation and protection by lock and key. There has been little temptation to characterize this type of secrecy as a privacy right. Secrets needed to protect the logical security of information systems do in any obvious way pertain to the personal lives of individuals. It is thus all the more significant that the measures needed to address issues of system security are same as those needed to address malicious intent and theft of intellectual property to a significant degree. In each of these cases, security depends on excluding someone from a key piece of information. In many instances, the mere fact that an excluded party is seeking information is often itself evidence that a harmful use will be attempted. In each set of cases, at least three questions bear on the overall security goals that secrecy is invoked to serve.

1. What is the probability that an excluded party will acquire the information? The answer will be a function of the probability of inadvertent disclosure, the probability that an excluded party seeking information will succeed, and the difference between the two. Information that would be evident even to those who do not seek it can hardly be considered confidential, yet when the probabilities of both inadvertent disclosure and successful search are low, overall risk is clearly lower than when these probabilities are high. When the probability of inadvertent disclosure is significantly lower than that of successful search, the possibility of intentional intrusion into the area of secrecy becomes the key factor in analyzing the chance of harm to person or property.

2. What is the likelihood that harm will befall the affected party if the information is acquired by an excluded party? Many facts about the intentions of the excluded party and the way of acquiring information bear on our assessment of this likelihood. Clearly the chance that harm will follow a maleficent search is high. We are less likely to think that harm will follow inadvertent discovery and beneficent searches, though the chance that it will not is surely greater than zero. The likelihood that harm will follow a search made 'for no reason' falls between the two. Rebecca Shaeffer's murderer used a data based to pursue a harmful end. What is the likelihood that someone idly looking up addresses of the stars will come to a harmful end? Any systematic assessment of the chance that harms will occur would broach a host of additional considerations that would qualify our initial assessment. Nevertheless, we are inclined to think that such searches may be less idle than they appear, that perhaps even a bit of self-deception is occurring with the searcher. These considerations point toward elevated risk.

There is one other consideration that should be noted in taking account of the probability that harm would occur. Harm might be counterbalanced by the possibility that the affected party will receive benefits. Someone who can find your address may use that information to return your lost wallet. People offering an invitation to attend a party or buy a used car might search a database of addresses with beneficent intent. Such opportunities might be welcomed (though, of course, they might not). The ethical significance of beneficial outcomes should be included in discussions of security, but we should not presume that

beneficial outcomes can always be used to counterbalance harmful outcomes in any straightforward manner.

3. How serious is the harm that might befall the affected party? Security rights are violated by violence against a person's body or property. Murder and theft both violate security rights, but death is far more serious. This ranking guides our thinking on the expenditure of resources to mitigate risk. As conventionally conceived, the right to security of person and property will be invoked when harms are rather serious. This suggests that there are some forms of harm—the theft of one's pencil or a mild insult, for example—that do not rise to the level of a security risk.

Whether there are forms of psychological harm or inconvenience that are protected by basic security rights is open to debate. Indeed, there are a number of interpretive and ethical problems that tag along with the risk-based approach, but those issues go far beyond the scope of this paper. Risk analysis has a seductive allure that conceals thorny problems of an epistemological, ethical, political and even psychological nature, (Thompson, 1999). There are also cases where computing technology makes information that individuals have no right to conceal much easier to obtain than it would have otherwise been. Analyzing putative privacy issues as the security issues they are is a step in the direction of clarity and accuracy, but it is also a step into ongoing and hotly disputed debates about the acceptability of risk. Further research in the program outlined above will need to examine how classic problems in technologically induced apply to information technology.

One philosophical approach to technological risk is a qualified form of utilitarianism, in which risks and benefits are interpreted as expected values. This approach inherits the problems of utilitarianism, but with the extra burden of problems that arise with utility maximizing decision rules that range over uncertain predictions of future events. (See Shrader-Frechette, 1991; Cranor, 1997). Of particular importance is the view that sees consent as the ethically appropriate response to risk, rather than utilitarian optimization of cost and benefit (see Sagoff, 1985; Faden, Beauchamp and King, 1986). Furthermore, as issues in information technology come to be conceptualized in terms of weakness in personal or public security, they will inherit a set of problems that have to do with the tension between the public's conceptualization of risk and that of a technically trained elite (see Thompson and Dean, 1996, Thompson 1999).

SOME CONCLUDING THOUGHTS ON PRIVACY

One would hope that when risks to security are more clearly understood as such, there would also be an opportunity for more clearly specified research on privacy rights. When we apply the heuristic of risk analysis to cases where computers scan electronic databases for market research, for example, it will be difficult to characterize this practice as intrusive with respect to a person's security. It is always possible that a grocery store chain will use its register data in a manner that threatens security, but this is not the possibility that alarms those who believe that the lines that separate personal, commercial and public life are being compromised by such practices. To the extent that this intuition can be disentangled from latent security concerns, it may be possible to formulate a right to privacy in terms that bear on the use of information technology in an ethically significant way.

It is worth repeating a point made earlier. Respect for privacy requires non-interference in the protected sphere, even when excluded parties have knowledge of the protected sphere. So, for example, a person's religious or sexual practices would be 'private' even in cases where neighbors and acquaintances might be expected to know quite a bit about them. There is no prima facie reason to think that sharing or discovery of information about a person's protected sphere through computer networks makes the protected sphere any less private. Those who acquire the information are still required to disregard it, whether they got the information from casual observance or data mining.

The question is whether simply *having* this information compromises privacy, and if so, does it matter who has it and in what form. It is possible to argue that information that would be generally known to one's neighbors (what kind of car one drives, what newspapers one subscribes to, what visitors one has) should be treated as 'private' when sought by someone else. But this will not be an easy or straightforward argument to make. Perhaps such information is not concealed from neighbors simply because keeping it secret would be costly and inconvenient. One might, in other words, still assert a **right** to conceal such information on grounds of privacy (and to insist that others do not reveal such information), even when one knows that the right will not be exercised in those circumstances where it is costly and inconvenient to do so. But suppose the cost of keeping information out of others' hands is a factor that bears on the justification of a right to privacy. A utilitarian might take such a view, for example. If computers make it

more or less costly to keep others from having information, they can substantially alter the total social costs that would be incurred by recognizing a legal or customary right to privacy.

As hinted above, I am more inclined to think of privacy as a primary good than as a fundamental liberty or as a merely instrumental good. I am also inclined to think that the pattern of disclosure and the way information is used are more important than the fact that something private is known by others. It is impossible to explore these suggestions here. If privacy is a primary good, it may be more like dignity or autonomy. Rights to dignity and autonomy are often contrasted to the basic rights of non-interference associated with security of person and property. Opportunities for dignity and autonomy are capabilities commonly had by the rich under industrial capitalism, but denied to the poor. So even when personal security and the safety of what meager property owned by the poor has been assured, there are still obligations of justice that may be unmet. Differential access to information about others creates a situation in which the rich can found out much more about the poor than vice versa. It is not difficult to imagine how computers might figure in creating differential access. But it will still be important to distinguish cases where differential access to information would be followed by abuses that threaten the security of the poor from those in which it is the dignity (or privacy) of the poor that is affected. Even on rather conservative and libertarian grounds, the rich have no right to harm the poor.

This observation provides a final argument for splitting rather than lumping where privacy rights are concerned. It is ironic that liberals and radicals who plead for the poor would adopt an approach to the ethics of information technology that obscures the way that fundamental, non-controversial rights of property and personal security are placed at risk. Yet that is exactly what describing threats to personal security as an issue of privacy does. No one will defend uses of computers that cause harm to person or property, and uses that risk such harm are clearly candidates for ethical evaluation and legal action. Let us be clear in articulating the moral basis for addressing the ways that information technology affects personal security, and the genuine problems of privacy will be made somewhat clearer in relief.

REFERENCES

Bok, Sissela. 1983. *Secrets: On the Ethics of Concealment and Revelation.* New York: Vintage Books.

Bynam, Terrel Ward. 1998. 'Global Information Ethics and the Information Revolution,' in *The Digital Phoenix: How Computers Are Changing Philosophy.* Oxford: Basil Blackwell, pp. 274-291.

Cranor, Carl F. 1997. 'The Normative Nature of Risk Assessment Features and Possibilities,' *Risk: Health, Safety and Environment.* 8:123-136.

Edgar, Stacey. 1997. *Morality and Machines: Perspectives in Computer Ethics.* Sudbury, MA: Jones and Bartlett Pubs.

Faden, Ruth, Thomas J. Beauchamp and Nancy M. P. King. 1986. *A History and Theory of Informed Consent.* Oxford: Oxford University Press.

Gotlieb, Calvin C. 1995. 'Privacy: A Concept Whose Time Has Come and Gone,' in *Surveillance, Computers and Privacy*, D. Lyon and E. Zureik, Eds. Minneapolis: University of Minnesota Press, pp. 156-171.

Lyon, David and Elia Zureik. 1995. 'Surveillance, Privacy and the New Technology,' in *Surveillance, Computers and Privacy*, D. Lyon and E. Zureik, Eds. Minneapolis: University of Minnesota Press, pp. 1-18.

Rachels, J. 1975. Why privacy is important. *Philosophy and Public Affairs* 4:323-333.

Sagoff, Mark. 1985. *Risk Benefit Decision Making in Decisions Concerning Public Safety and Health.* Dubuque, IA: Kendall-Hall Pub. Co.

Shrader-Frechette, Kristin. 1991. *Risk and Rationality* Berkeley, CA: University of California Press.

Spafford, Eugene H., Kathleen A. Heaphy and David J. Ferbrache. 1989. Computer Viruses : Dealing with Electronic Vandalism and Programmed Threats. Arlington, VA: ADAPSO.

Sparks, Colin. 1994. 'Civil Society and Information Society as Guarantors of Progress, ' in *Information Society and Civil Society: Changing Perspectives on the Contemporary World Order,* S. Splichal, A. Calabrese, and C. Sparks, Eds., West Lafayette, IN: Purdue University Press, pp. 21-49.

Thompson, Paul B. 1999. 'The Ethics of Truth-Telling and the Problem of Risk,' *Science and Engineering Ethics* 5(4): 489-511.

Thompson, Paul B. and W. E. Dean, 1996. 'Competing Conceptions of Risk,' *Risk: Health, Safety and Environment* 7(4): 361-384.

Warren, Samuel D. and Louis D. Brandeis. 1890. The right to privacy, *Harvard Law Review* 4 (December 15):193-220.