PRIVACY AND TECHNOLOGY

By David Friedman

I. Introduction

Privacy: 1. state of being apart from the company or observation of others. . .[1]

The definition above nicely encapsulates two of the intertwined meanings of 'privacy'. In the first sense—*physical seclusion*—the level of privacy in modern developed societies is extraordinarily high by historical standards. We take it for granted that a bed in a hotel will be occupied by either one person or a couple—not by several strangers. At home, few of us expect to share either bed or bedroom with our children. In these and a variety of other ways, increased physical privacy has come as a by-product of increased wealth.[2]

The situation with regard to the second sense—*informational privacy*—is less clear. While the ability of other people to see with their own eyes what we are doing has decreased as a result of increased physical privacy, their ability to observe us indirectly has increased for two quite different reasons.

One reason is the development of increasingly sophisticated technologies for transmitting and intercepting messages. Eavesdropping requires that the eavesdropper be physically close to his victim; wiretapping does not. Current satellite observation technology may not quite make it possible to read lips from orbit, but it is getting close.

The other reason that indirect observation has become easier is the development of greatly improved technologies for storing and manipulating information. What matters to me is not whether information about me exists, but whether other people can find it. Even if all of the information I wish to keep private—say, my marital history or criminal record—exists in publicly accessible archives, it remains, for all practical purposes, private so long as the people I am interacting with do not know that it exists nor where to look for it. Modern information processing has at least the potential to drastically reduce this sort of privacy. The same search engines and collections of information that provide the ideal tools for the researcher who dives into the World Wide Web in the hope of emerging

[1] *Webster's International Dictionary*, 2d ed., s.v. "privacy."

[2] See the references in Richard Posner, "The Right of Privacy," *Georgia Law Review* 12, no. 3 (Spring 1978): 393–428, to the anthropological literature on the lack of privacy in primitive societies.

with a fact in his teeth work equally well whether the fact is historical or personal. Privacy through obscurity is not, or at least soon will not be, a practical option.

The two sorts of privacy—physical and informational—are connected. Physical privacy is a means, although a decreasingly effective means, to informational privacy. And lack of informational privacy—in the limiting case, a world where anyone could know everything about you at every instant—feels like a lack of physical privacy, a sort of virtual crowding.

Physical privacy can be a means to informational privacy, but so can the lack of physical privacy; the individual in the crowded city is more anonymous, and has more informational privacy, than an individual in the less-crowded village. But the reason for that is that his privacy is protected by the difficulty of sorting through such a vast amount of data in order to find the particular facts relevant to him. That form of protection cannot survive modern information technology. Hence the connection between physical and informational privacy may become stronger, not weaker, over the course of the next few decades.

There is a third sort of privacy not captured by the definition with which I began this essay—*attentional privacy*. It is the privacy that is violated by unsolicited e-mail or telephone calls from people trying to sell you things that you do not want to buy. Modern technology's impact on this type of privacy has been mixed; the technology makes sending messages less expensive, facilitating bulk e-mail and telemarketing calls, but also makes filtering out messages without human intervention easier, thus lowering the cost of dealing with unwanted messages.

In this essay I will be focusing on issues of informational privacy. As we will see, however, the technology of protecting informational privacy may depend in part on the existence of physical privacy. One interesting question for the future will be whether it is possible to develop technologies that break that link by making it practical to engage in informational transactions without taking any physical actions that can be observed and understood by an outside observer.

Section II of this essay explores the questions of what informational privacy is, why and whether it is a good thing, and why it is widely regarded as a good thing. Section III surveys new technologies that are useful for either protecting or violating an individual's control over information about himself. The final section summarizes my conclusions.

In the course of my discussion, I will be using the term 'privacy rights' in a sense that some readers may find confusing. What I mean by a privacy right is neither a legal nor a moral right, but a *positive* right—a description of an individual's ability to control something. I have strong informational privacy rights if I can easily and inexpensively control other people's access to information about me. If I have a legal right not to have you tap my phone, but it is impractical to enforce that right—the situation at present for those using cordless phones without encryption—

then I have only a very weak right, in the sense that I am using here, to that particular form of privacy. In contrast, I have substantial rights to privacy with regard to my own thoughts, even though it is perfectly legal for other people to use the available technologies—listening to my voice and watching my facial expressions—to try to figure out what I am thinking. I have strong privacy rights over my thoughts because those technologies are not adequate to read my mind.[3]

One source of strong positive rights might be strong legal rights—provided that the legal rights are readily enforceable. Another source might be widely held beliefs about moral rights; it is easier to keep personal matters secret in a society where violating other people's privacy is considered wicked. Positive rights can also be affected by things unrelated to legal or moral rights, such as technological changes. If, for example, someone invented an easy and accurate way of reading minds, positive privacy rights would be radically reduced, even if there were no change in legal or moral privacy rights.

There are two reasons why I define rights in this way. The first is that I am interested in the consequences of privacy rights, that is, in the ways in which my ability to control information about me benefits or harms myself and others—whatever the source of that ability may be. The second is that I am interested in the ways in which technology is likely to change the ability of an individual to control information about himself—hence in changes in positive rights that are due to sources other than changes in legal or moral rights.

II. What Is Informational Privacy and Why Does It Matter?

If all information about you is readily available to anyone who wants it, you have no informational privacy. If nobody else knows anything about you, you have perfect informational privacy. All of us live between those two extremes.

Informational privacy is not always desirable. Film stars and politicians pay to have their privacy reduced by getting (some) information about themselves widely distributed by professional public relations firms. Many other people, however, bear costs in order to reduce the amount that other people know about them, demonstrating that, to them, privacy has positive value. Many people also bear costs to learn about others, demonstrating that to them the privacy of those other people has negative value. At the same time, most people regard privacy in the abstract as a good thing. It is common to see some new product, technology, or legal rule

[3] For a more general discussion of rights from a related perspective, see David Friedman, "A Positive Account of Property Rights," *Social Philosophy and Policy* 11, no. 2 (Summer 1994): 1–16.

attacked as reducing privacy, rare to see anything attacked as increasing privacy.

This raises two related questions. The first is why individuals (sometimes) value their own privacy, and so are willing to take actions to protect it. The second is why many individuals speak and act as though the cost to them of a reduction in their privacy is larger than the benefit to them of a similar reduction in other people's privacy, making privacy in general, not merely privacy for themselves, a good.

The answer to the first question is fairly straightforward. Information about me in the hands of other people sometimes permits them to gain at my expense. They may do so by stealing my property—if, for example, they know when I will or will not be home. They may do so by getting more favorable terms in a voluntary transaction—if, for example, they know just how much I am willing to pay for what they are selling.[4] They may do so by preventing me from stealing their property—by, for example, not hiring me as company treasurer after discovering that I am a convicted embezzler, or by not lending me money after discovering that I have repeatedly declared bankruptcy.

Information about me in other people's hands may also sometimes make me better off—for example, the information that I am an honest and competent attorney. But privacy rights do not prevent people from giving out information about themselves; they merely prevent people from obtaining information about others without their consent. If I have control over information about myself, I can release it when doing so benefits me and keep it private when releasing it would make me worse off.[5] Hence it is not surprising that people value having such control.

This does not, however, answer the second question. To the extent that my control over information about me makes me better off at the expense of other people, and their control over information about them makes them better off at my expense, it is not clear why I should regard privacy rights as on net a good thing. The examples I offered above included one

[4] One example of this occurs in the context of a takeover bid. In order for the market for corporate control to discipline corporate managers, it must be in the interest of someone to identify badly managed corporations and take them over. Doing this requires that a takeover bid can remain secret long enough for the person responsible to accumulate a substantial ownership in a corporation at the pre-takeover price. In a very public world, this is hard to do. Currently it is also hard to do in the United States because of legal rules deliberately designed to limit the secrecy of takeover bids. The result is not, of course, to eliminate all takeover bids or all market discipline over corporate managers, but merely to reduce both below what they would be in a more private and less regulated market.

[5] An exception is the case where the relevant information is negative. If I have control over information about me, potential lenders have no way of knowing whether the reason they have seen no reports of my having ever declared bankruptcy is that I have not done so, or that I have done so and have suppressed the information. Thus, borrowers who have not declared bankruptcy in the past will be better off in a world where privacy rights with regard to such information are weak. The problem disappears if a borrower can take an observable action—such as signing a legally enforceable waiver of the relevant legal privacy rights—which demonstrates that the information is not being suppressed.

case in which my privacy protected me from burglary; in this case, privacy produced a net benefit, since the gain that a burglar receives from a theft is normally less than the loss suffered by his victim. They included one case in which my privacy permitted me to steal from or defraud others; in this case, privacy produced a net loss, for similar reasons. And they included one case—bargaining—in which the net effect appears to be a wash.[6]

The bargaining case is worth a little more attention. Suppose you have something to sell—say an apple. I am the only buyer. The apple is worth one dollar to you and two to me. We are engaged in the game known as *bilateral monopoly*.[7] At any price between one dollar and two, both of us benefit from the transaction, but as the price increases within that range, the amount of the benefit that you get rises and the amount of the benefit that I get falls.

I can try to get you to sell at a lower price by persuading you that the apple is worth less to me than it really is, and hence that if you insist on a high price there will be no sale. You can try to get a higher price by persuading me that the apple is worth more to you than it really is, so that if I do not agree to a higher price there will be no sale. One risk with both tactics is that they may succeed too well. If you persuade me that the apple is worth more than two dollars to you, or if I persuade you that it is worth less than one dollar to me, the deal will fall through.

Suppose I get accurate information on the value of the apple to you. One result of this is that your persuasion no longer works, making it more likely that I will get the apple at a low price. That is merely a transfer from you to me, involving no change in the net benefit of the transaction. A second result is to make bargaining breakdown less likely. I will still try to persuade you that the apple is worth less than two dollars to me, but I will not try to persuade you that it is worth less than one dollar, because I now know that doing so is against my interest. This second result produces a net benefit, since it increases the chance that you will end up selling me the apple instead of keeping it yourself (leading to a net gain of one dollar, since the apple is worth a dollar more to me than it is to you).

Generalizing the argument, it looks as though privacy produces, on average, a net loss in situations, such as the one just discussed, where

[6] Many of the points made in this section of the essay can be found, in somewhat different form, in Posner, "The Right of Privacy," and Posner, "An Economic Theory of Privacy," *Regulation* 2, no. 3 (May/June 1978): 19. He finds the case for the general desirability of privacy to be weak.

[7] It is called bilateral monopoly because it corresponds to a situation in which there is both a monopoly seller and a monopoly (strictly speaking, monopsony) buyer. Discussions of bilateral monopoly can be found in David Friedman, *Hidden Order: The Economics of Everyday Life* (New York: HarperBusiness, 1996), chap. 11; and in David Friedman, *Law's Order: What Economics Has to Do with Law and Why It Matters* (Princeton, NJ: Princeton University Press, forthcoming), chap. 8. *Law's Order* is also available on the World Wide Web at http://www.best.com/~ddfr/Laws_Order/laws_order_ToC.htm.

parties are seeking information about each other in order to improve the terms of a voluntary transaction. This is because privacy, in these situations, increases the risk of bargaining breakdown, when one party's ignorance leads to an incorrect estimate of the terms that the other will accept.[8] In situations involving involuntary transactions, privacy produces a net gain if it is being used to protect other rights (the burglary example), and a net loss if it is being used to violate other rights (the embezzler and fraudulent loan examples). (In both sets of examples, I assume that those rights have been defined in a way that makes their protection efficient.) There is no obvious reason why the former situation should be more common than the latter. So it remains puzzling why people in general support privacy rights—why they think it is, on the whole, a good thing for people to be able to control information about themselves.

A. Privacy rights and rent seeking

One possible approach to this puzzle starts by viewing privacy rights as a mechanism for reducing costs associated with *rent seeking*, that is, expenditures by one person that are designed to benefit him at the cost of another. Consider again our bilateral-monopoly bargaining game. Assume this time that each player can, at some cost, obtain information about the value of the apple to the other player. For example, suppose that I can plant listening devices or miniature video cameras about your home in the hope of seeing or hearing something that will tell me just how much you value the apple; suppose also that you can take similar actions with regard to me. Such activities may produce a benefit by reducing the risk of bargaining breakdown, but there is no guarantee that that benefit will be larger than the cost of the spying. Even if it is not, my spying may still be in my interest, since it is a way of getting better terms and thus gaining at your expense.

The rent seeking becomes clearer if we include not only your efforts to learn things about me but also my efforts to prevent you from doing so. Suppose, for example, that I have a taste for watching pornographic videos, and that my boss is a puritan who does not wish to employ people who enjoy pornography. We consider two possible situations—one in which my boss is able to keep track of what I am renting from the local video store, and another in which he is not.

[8] This might not be the case if we are frequently faced with situations in which my prospective gains from the bargain provide the incentive for me to generate information that is of value to other people as well. There is little point to spending time and money predicting a rise in wheat prices if everything you discover is revealed to potential sellers before you have a chance to buy from them. See Jack Hirschleifer, "The Private and Social Value of Information and the Reward to Inventive Activity," *American Economic Review* 61, no. 3 (September 1971): 561–74.

If I know the boss may be monitoring my rentals from that store, I respond by renting videos from a more distant and less convenient outlet. My boss is no better off as a result of the reduction in my privacy; I am still viewing pornography, and he is still ignorant of the fact. I am worse off as a result of the additional driving time required to visit the more distant store.

Generalizing the argument, we consider a situation where I have information about myself and can, at some cost, prevent other people from having that information. Under one legal (or technological) regime, the cost of doing so is low, under another, it is high. Under both regimes, however, the cost is low enough that I am willing to pay it. The former regime is then superior, not because I end up with more privacy, but because I end up getting it at a lower cost. Therefore, laws, norms, or technologies that lower the cost of protecting privacy may produce net benefits.[9]

I say "may" because the conclusion depends on assuming that it will, in either case, be worth the cost to me to protect my privacy.[10] If we assume instead that under the second regime protecting my privacy is prohibitively expensive, and if we are considering situations where the loss of privacy produces a transfer from me to someone else but no net cost (or, a fortiori, if it produces a net benefit), we get the opposite result. If privacy is cheap, I buy it and, even though it is cheap, it still costs something and produces no net benefit. If privacy is expensive, I do not buy it and, while I am then worse off for not having it, my loss is balanced by someone else's gain, so on net we are better off by the amount saved through not bearing the cost of protecting my privacy.

Viewing privacy as a way of reducing rent seeking provides a possible explanation for why circumstances that make privacy easier to obtain might be desirable, but it is an explanation very much dependent on assumptions about the technology of getting and concealing information. In a world where concealing information is costly, but not too costly to be worth doing, making concealment less costly produces a net benefit. In a world where concealing information is so costly that nobody bothers to do it, making concealment less costly increases the amount spent protect-

[9] This argument is proposed as a possible justification for trade secret law in David Friedman, William Landes, and Richard Posner, "Some Economics of Trade Secret Law," *Journal of Economic Perspectives* 5, no. 1 (Winter 1991): 61–72.

[10] One reason that the assumption may be correct is the difficulty of propertizing information. Suppose that keeping some particular fact about me secret benefits me at the expense of people that I deal with; for simplicity, assume that I get this benefit through a simple transfer with no net gain or loss. If you discover the fact, you have no incentive to keep it hidden, so you tell other people. You end up getting only a small fraction of the benefit, while I bear all of the cost, so I am willing to spend much more to conceal the fact than you would be willing to spend to discover it. This would not be the case if you could sell the information to other people who deal with me—as credit agencies, of course, do. But in many contexts such sales are impractical, due to the problems of transacting over information (briefly discussed below).

ing privacy, which is a net loss. More generally and precisely, lowering the cost of privacy reduces expenditures on privacy if the demand for privacy is inelastic, and increases them if it is elastic.[11]

This explanation also depends on another assumption—that the information about me starts in my control, so that facilitating privacy means making it easier for me to protect what I already possess. But much information about me comes into existence in other people's possession. Consider, for example, court records of my conviction on a criminal charge, or a magazine's mailing list with my name on it. Protecting my privacy with regard to such information requires some way of removing that information from the control of those people who initially possess it and transferring control to me. That is, in most cases, a costly process. There are lots of reasons, unconnected with privacy issues, why we generally want people to have access to court records, and there is no obvious nonlegal mechanism by which I can control such access.[12] If we do nothing to give people rights over such information about them, the information will remain public and nothing will have to be spent to restrict access to it.

B. Privacy as property

An alternative argument in favor of making privacy easier to obtain starts with a point that I made earlier: if I have control over information about me, but transferring that information to someone else produces net benefits, then I can give or sell that information to him. Hence, one might argue, by protecting my property rights in information about me, we establish a market in information. Each piece of information moves to the person who values it most, maximizing net benefit.

So far this is an argument not for privacy, but for private property in information.[13] To get to an argument for privacy requires two further steps. The first is to observe that most information about me starts out in my possession, although not necessarily my exclusive possession. Hence, giving anyone else exclusive rights to it requires somehow depriving me of it—which, given the absence of technologies that produce selective

[11] A demand is elastic if a 1 percent decrease in price results in more than a 1 percent increase in quantity demanded. A demand is inelastic if a 1 percent decrease in price results in less than a 1 percent increase in quantity demanded.

[12] There may be very costly ways of doing so. At one point during litigation involving conflicts between the Church of Scientology and discontented ex-members, information that the Church wished to keep private became part of the court record. The Church responded by having members continually checking out the relevant records, thus keeping anyone else from getting access to them. And I might preserve my privacy in a world where court records were public by changing my name.

[13] For a discussion of why it makes sense to treat some things as property and some as commons, see David Friedman, "Standards as Intellectual Property: An Economic Approach," *University of Dayton Law Review* 19, no. 3 (Spring 1994): 1109–29; and Friedman, *Law's Order*, chap. 10.

amnesia, is difficult. It would be possible to deprive me of control over information by making it illegal for me to make use of it or transmit it to others, but enforcing such a restriction would be costly, perhaps prohibitively costly.

The second step, following a general line of argument originated by economist Ronald Coase,[14] is to note that, to the extent that our legal rules assign control over information to the person to whom it is most valuable, they save us the transaction costs of moving it to that person. My earlier arguments suggest that information about me is sometimes most valuable to me (for example, when it protects me from a burglar), and sometimes it is most valuable to someone else. There are, however, a lot of different "someone elses." Giving each person control over information about himself, then, especially information that starts in his possession, is a legal rule that should minimize the transaction costs of getting information to the users that value it the most.

Stated in the abstract, this sounds like a reasonable argument. It would be one if we were talking about other forms of property. But there are problems with applying a property solution to personal information. The first problem is that transacting over information is often difficult, because it is hard to tell the customer what you are selling without giving it to him in the process. The second is that a given piece of information can be duplicated almost costlessly; thus, while the efficient allocation of a car is to the one person who values it the most, the efficient allocation of a piece of information is to everyone to whom it has positive value.[15] This implies that legal rules that treat information as a commons, such that everyone is free to make copies of it, lead to the efficient allocation.

This conclusion must be qualified in two ways. First, as we have already seen, legal protection of information may be a cheaper substitute for private protection; if the information is going to be protected because it is in someone's interest to do so, we might as well have it protected as inexpensively as possible. Second, you cannot copy information unless it exists. Thus we get the familiar argument from the economics of intellectual property, which holds that patent and copyright result in a suboptimal use of existing intellectual property, since they allow owners to sell the right to copy the protected material at a positive price even though the marginal cost of that right is zero. In exchange for this suboptimal *use* of existing intellectual property, however, patent and copyright allow us to get a more nearly optimal *production* of intellectual property.

[14] Ronald Coase, "The Problem of Social Cost," *Journal of Law and Economics* 3, no. 1 (October 1960): 1-44. See also Friedman, *Law's Order*, chap. 4.

[15] This assumes that A's possession of information does not impose a cost on B. But the argument generalizes to the case where the cost to B of A possessing information is typically lower than the benefit to A, which brings us back to the earlier discussion of reasons why privacy is likely to result in net costs.

Establishing rights to information in order to give an incentive to create that information is a legitimate argument for property rules in contexts such as copyright or patent. It is less convincing in the context of privacy. Information about me is either produced by me as a by-product of other activities, in which case I do not need any additional incentive to produce it, or else produced by other people about me, in which case giving me property rights in the information will not give them an incentive to produce it. It does provide an argument for privacy in some contexts, most obviously the context of trade secrets, where privacy is used to protect produced information and so give people an incentive to produce it.[16]

C. *Privacy as an inefficient norm*

Legal scholar Robert Ellickson, in *Order Without Law* (1991), argues that close-knit communities tend to produce efficient norms.[17] One of his examples is the set of norms developed by nineteenth-century whalers to deal with situations in which one ship harpooned a whale and another ship eventually brought it in. He offers evidence that those norms changed over time in a way that efficiently adapted them to the characteristics of the changing species of whales that were being hunted.

This story raises a puzzle. The reason the whalers had to change the species that they were hunting, and the associated norms, was that they were hunting one species after another into near extinction. That suggests that a norm restricting the catch would have produced sizable benefits. Yet no such norm developed.

My solution to that puzzle starts with a different puzzle: what is the mechanism that produces efficient norms? My answer begins by distinguishing between two different sorts of efficient norms. A *locally efficient* norm is a norm that it is in the interest of a small group of individuals to follow among themselves—for example, a norm of fair dealing. A *globally efficient* norm is one that it would be in the interest of everyone in the population to have everyone follow.

Locally efficient norms can be adopted by small groups. Since the groups benefit by adopting the norm, adoption of the norm will spread. Eventually everyone in the larger society will follow the norm. This mechanism does not work for a norm that is globally but not locally efficient, such as a norm against overwhaling. If some whalers follow it, it is in the interest of other whalers to take advantage of the opportunity by increasing their whaling efforts. Hence we would expect systems of private

[16] Friedman, Landes, and Posner, "Some Economics of Trade Secret Law."

[17] Robert Ellickson, *Order Without Law: How Neighbors Settle Disputes* (Cambridge, MA: Harvard University Press, 1991).

norms to be locally but not globally efficient, which corresponds to what Ellickson found for whaling.[18]

This brief sketch of norms provides a possible explanation for the widespread existence of norms of privacy, that is, norms holding that individuals are entitled to conceal personal information about themselves and that other individuals ought not to seek to discover such information. Such norms may well be locally efficient even if they are globally inefficient.

Why would such norms be locally efficient? Consider some piece of information about me: for example, my value for the apple in the earlier discussion of bilateral monopoly. If I am the sole possessor of that piece of information, I can either withhold it, to my benefit, or offer to sell it to my trading partner, supposing that there is some way in which I can prove to him that the information I am selling is truthful. If a third party is the sole possessor of the information, he can offer to sell it to either me or my trading partner, whoever bids more. But if several people possess the information, none of them can sell it for a significant price; anyone who tries will be underbid by one of the others, since the cost of reproducing the information is nearly zero. The logic is exactly the same as it would be in a situation in which we wished to maximize the revenue from a patent and were comparing the alternatives of having one owner of the patent or several, where in the latter case each owner could freely license to third parties.

It follows that if we are members of a close-knit group containing all of the people who can readily discover personal information about each other, and if we are also engaged in dealings with nonmembers of the group such that possession by them of personal information about one of us would make them better off at his expense, a norm of privacy is likely to be in our interest. Its effect is to give each of us monopoly ownership of information about himself, permitting each to maximize the return from that information, whether by keeping it secret or by selling it. To the extent that this return comes at the expense of the nonmembers with whom we are dealing, the norm may be globally inefficient. But it is locally efficient, which provides a possible explanation of why it exists.

D. Blackmail and privacy

> If blackmail were legal, blackmailers and their customers (today called "victims") would enter into legally enforceable contracts whereby the blackmailer would agree for a price never to disclose the infor-

[18] A longer version of this argument can be found in David Friedman, "Less Law than Meets the Eye," review of *Order Without Law*, by Robert Ellickson, *Michigan Law Review* 90, no. 6 (May 1992): 1444–52.

mation in question; the information would become the legally protected trade secret of the customer.[19]

Laws against blackmail provide an interesting puzzle. Suppose you know something about me that I would prefer not to be public. I offer to pay for your silence. At first glance, the transaction seems obviously beneficial. I value your silence more than the money, which is why I made the offer; you value the money more than publishing my secret, which is why you accepted. We are both better off, so why should anyone object?[20]

One way to respond to this is to assert that by posing this question after you obtained the information, we have started too late in the process. The possibility of blackmail gives people an incentive to spend resources acquiring information about other people and gives potential targets an incentive to spend resources concealing such information. If blackmail is legal, I might spend a thousand dollars' worth of time and effort trying to conceal the information, and you might spend a thousand dollars trying to discover it. If you succeed, I would then pay you three thousand dollars to keep your mouth shut. This would leave us, on net, two thousand dollars worse off than when we started: you would be two thousand dollars better off, I would be four thousand worse off. If you fail, we would have each spent a thousand dollars, so again we would be, on net, two thousand dollars worse off than when we started. A law that made it impractical for you to profit by discovering such information thus provides a net benefit of two thousand dollars. We are back to the rent-seeking explanation of privacy.

An alternative reason why we might object to blackmail is that we ought to include more people in our calculations of costs and benefits. In particular, we ought to include the people to whom you are threatening to tell my secret. The reason I am willing to pay for your silence is that doing so makes me better off, possibly at their expense. Perhaps the secret is my record for fraud or malpractice; having moved from where my

[19] Richard Posner, "Blackmail, Privacy, and Freedom of Contract," *University of Pennsylvania Law Review* 141, no. 5 (May 1993).

[20] These issues are explored in an extensive literature, including: James Lindgren, "Blackmail: On Waste, Morals, and Ronald Coase," *UCLA Law Review* 36, no. 3 (February 1989): 597–608; Lindgren, "Kept in the Dark: Owens's View of Blackmail," *Connecticut Law Review* 21, no. 3 (Spring 1989): 749–51; Lindgren, "Secret Rights: A Comment on Campbell's Theory of Blackmail," *Connecticut Law Review* 21, no. 2 (Winter 1989): 407–10; Lindgren, "In Defense of Keeping Blackmail a Crime: Responding to Block and Gordon," *Loyola of Los Angeles Law Review* 20, no. 1 (November 1986): 35–44; Lindgren, "More Blackmail Ink: A Critique of Blackmail, Inc., Epstein's Theory of Blackmail," *Connecticut Law Review* 16, no. 4 (Summer 1984): 909–23; Lindgren, "Unraveling the Paradox of Blackmail," *Columbia Law Review* 84, no. 2 (March 1984): 670–717; Richard S. Murphy, "Property Rights in Personal Information: An Economic Defense of Privacy," *Georgia Law Journal* 84, no. 7 (July 1996): 2381–417; Posner, "The Right of Privacy"; Posner, "An Economic Theory of Privacy"; Posner, *The Economics of Justice* (Cambridge, MA: Harvard University Press, 1981), chaps. 9–10, pp. 231–309; Posner, *Overcoming Law* (Cambridge, MA: Harvard University Press, 1995), chap. 25, pp. 531–51; and Posner, "Blackmail, Privacy, and Freedom of Contract."

misdeeds were first unveiled, I may be looking for new, poorly informed customers. Perhaps the secret is what happened to my first wife; I may now be seeking to obtain a replacement. In these and many other circumstances, when a blackmailer accepts a payment for silence, he imposes an external cost on those who would otherwise have learned what he knows. Perhaps legal rules permitting me to buy his silence would make the society as a whole worse off, by keeping him silent and others ignorant.

As should be clear, these two arguments for banning blackmail are not only different, they are in an important sense inconsistent. If we assume that the same amount of information will be produced whether or not blackmail is legal—if, that is, we imagine that the typical blackmailer obtained his information by accident, not effort—then the rent-seeking argument vanishes, but the public-benefit argument replaces it. The potential blackmailer has the information; if he cannot sell it, he might as well give it away. If, on the other hand, we assume that the information on which blackmail is based is primarily obtained for that purpose, the rent-seeking argument is revived, but the public-benefit argument vanishes. If blackmail is illegal, the information will never be generated, so the public will never be warned.

At this point, we seem to have arguments against permitting blackmail both when blackmailers discover information by accident and when they deliberately search for it. This conclusion becomes less clear if we assume that the information a blackmailer discovers is not merely useful to other people in dealing with the victim, but is also discreditable to the victim—as we usually do assume when discussing blackmail. If we suppose that the blackmailer discovered the information by accident and will publish it—perhaps in the hope of a financial or reputational reward—if he cannot sell it to the victim, then laws against blackmail make sense, since they result in the potential victim being exposed for his misdeeds. If we permit blackmail, the victim still suffers—but his suffering takes the form of a payment to the blackmailer. The reason why the victim makes the payment is that it costs him less than it would cost him if his misdeed were revealed. Therefore, the result is a lower cost to the victim; furthermore, other people will never receive the information, and so will not be able to modify their behavior to take account of it, making them worse off than they would have been if the information had been revealed.

Suppose, however, that the incentive provided by the ability to blackmail people plays a major role in the discovery of the information. In that case, blackmail becomes a useful mechanism for the private enforcement of law.[21] If blackmail is legal, people have an incentive to look for evidence of other people's crimes and use it to blackmail them, thus impos-

[21] Posner has argued that laws against blackmail are desirable in circumstances where private law enforcement is for some reason inefficient. See, for example, Posner, *Economic Analysis of Law*, 5th ed. (New York: Aspen Law & Business, 1998), 660–61.

ing a punishment on criminals who would otherwise go free. The same argument applies if the information concerns violations of norms rather than laws, assuming that we believe the norms are efficient ones and that punishment for their violation is, therefore, desirable.

I previously pointed out that one argument for intellectual property law is that it provides an incentive to generate valuable information. Similarly here, the form of transferable property right that exists if blackmail is legal also creates an incentive to generate valuable information. The information, once generated, is suppressed, but there is still a benefit, since the process generates a penalty for the behavior that the information concerns, and blackmail is particularly likely to occur with regard to behavior that we would like to penalize.

E. Privacy and government

> It would have been impossible to proportion with tolerable exactness the tax upon a shop to the extent of the trade carried on in it, without such an inquisition as would have been altogether insupportable in a free country.[22]
>
> (Adam Smith's explanation of why a sales tax is impractical.)
>
> The state of a man's fortune varies from day to day, and without an inquisition more intolerable than any tax, and renewed at least once every year, can only be guessed at.[23]
>
> (Smith's explanation of why an income tax is impractical.)

Until now, I have ignored an issue that is central to much of the concern over privacy: privacy from government. The logic is the same as in the situations we have been discussing. If the government knows things about me—for example, my income—that permits the government to benefit itself at my expense. In some cases, it also permits the government to do things that benefit me—for example, pay me money because my income is low—but in such situations, privacy rights would leave me free to reveal the information if I wished.

However, privacy from government differs from privacy from private parties in two important respects. First, although private parties occasionally engage in involuntary transactions such as burglary, most of their interactions with each other are voluntary ones, which makes it less likely that someone else having information about me will result in an inefficient transaction. Governments engage in involuntary transactions on an

[22] Adam Smith, *An Inquiry into the Nature and Causes of the Wealth of Nations*, ed. Edwin Cannan (New York: Modern Library, 1937), bk. 5, chap. 2, pt. 2, art. 2.
[23] Ibid., bk. 5, chap. 2, pt. 2, art. 4.

enormously larger scale. Second, governments almost always have an overwhelming superiority of physical force over the individual citizen. It follows that while I can protect myself from my fellow citizens to a considerable degree by using locks and burglar alarms, I can protect myself from government actors only by keeping from them the information that they need to benefit the government at my expense.[24]

The implications of these differences for the value of privacy depend very much on one's view of government. If, at one extreme, one regards government as the modern equivalent of the Philosopher King, then individual privacy simply makes it harder for government actors to do good. If, at the other extreme, one regards government as a particularly large and well-organized criminal gang supporting itself at the expense of the taxpayers, individual privacy against government becomes an unambiguously good thing. Most Americans appear, judging by their expressed views on privacy, to be close enough to the latter position to consider privacy against government as on the whole desirable, except in cases where they believe that privacy might be used primarily to protect private criminals. Similar views are common among citizens of some, but not all, other countries, a difference that may help explain different national policies with regard to privacy. As a very rough observation, Europeans seem to be more concerned than Americans with privacy vis-à-vis private actors and less concerned than Americans with privacy vis-à-vis their governments. The quotations from Smith—when contrasted with current British practice—suggest that concerns with privacy against government may have declined over time, at least in Britain.

F. The weak case for privacy: a summary

Explaining why individuals wish to have control over information about themselves is easy. Explaining why it is in my interest that both I *and* the people I deal with have such control, or why people believe that this latter state of affairs is in their interest and act accordingly, is more difficult.

We have considered three reasons why privacy might be in the general interest, that is, why it might be efficient in the economic sense. One is that people want to control information about themselves, so the easier that this is to do, the less they will have to spend to do it. People also want information about other people, and the harder it is to get, the less they will spend getting it. As the odd asymmetry of the two sides of the argument suggests—in one case, lowering a price reduces expenditure; in the other, raising a price reduces expenditure—the argument for the efficiency of privacy depends on specific assumptions about the relevant

[24] Of course, I could also protect myself by engaging in political activity—for example, by lobbying Congress or making contributions to the police benevolent fund. For most individuals, such tactics are rarely worth their cost.

demand and supply functions. It goes through rigorously if the demand for one's own privacy is inelastic and the demand for information about others is elastic—which might, but need not, be true.[25]

Put in that form, the argument sounds abstract, but the concrete version should be obvious to anyone who has ever closed a door behind him, loosened his tie, taken off his shoes, and put his feet up on his desk. Privacy has permitted him to maintain his reputation as someone who behaves properly without having to bear the cost of actually behaving properly—which is why there is no window between his office and the adjacent hallway.

The second reason why privacy might be efficient is that property rights permit goods to be allocated to their highest-valued use. If protection of privacy is easy, then individuals have reasonably secure property rights over information about themselves. It makes sense to give such rights to the individual whom the information is about, because he is more likely to be the highest-valued user than any single other person—and if he is not, he can always sell the information to someone else. The problem with this argument is that information, unlike other goods, can be reproduced at almost no cost, making it likely that the highest-valued user is "everybody." Even if the transfer of the information from its subject to everybody produces net benefits, it may not occur, since once a few people have the information, it is hard to prevent them from reselling it, making it impossible for the original owner to collect its value from anyone else, and thus making it less likely that the information will be bought in the first place.[26]

The third reason why privacy might be efficient is that it provides a way in which individuals may protect themselves against government. The strength of that argument depends very much on one's view of the nature of government.

We also saw one argument against privacy—that it permits people to act badly while evading the consequence of having people know that they acted badly. This argument was worked out in the context of arguments for and against legalizing blackmail.

The conclusion so far is that the case for privacy rights—for the claim that it is desirable to lower the cost to individuals of controlling information about themselves—is a weak one. Under some circumstances, privacy produces a net gain, but under others it produces a net loss.

[25] Privacy might also be on net efficient if one of the two functions met the required condition and produced gains that more than outweighed the loss from the function that did not.

[26] This problem suggests a further point relevant to the issue of blackmail. The information that I am a swindler is worth more to my potential victims than it is to me. But since it is much easier to sell a single piece of information to one person than to many, the blackmailer can collect most of its value to me from me and has no way of collecting any significant fraction of its value to them from them. So he sells it to me instead of to them, which is an inefficient outcome—and one that may be prevented by laws against blackmail.

G. Other privacies

So far we have been talking only about informational privacy. The link between this sort of privacy and physical privacy is fairly obvious; if there is someone else in the room with you, he will probably notice when you loosen your tie and take off your shoes. Physical privacy is, among other things, a means to maintain informational privacy.

The link between informational privacy and attentional privacy is also obvious, but the implications are less clear. When someone sends me a message, such as a phone call or an e-mail, it costs me something to examine the message and determine whether it is of interest. In a world of uncertainty, some messages are of interest to me and some are not; neither I nor the sender knows for certain whether I am interested in a particular message until I have examined it.

Both the sender and I would prefer that the sender send me messages that are of interest to me; there is no point to calling someone up in order to sell him something that he has no interest in buying. Where we differ is in where we draw the line between messages that are or are not worth their cost. The sender wants to send messages if and only if the probability that I will be interested—and will respond in a way that benefits him—is sufficient to justify the cost to him of sending the message.[27] I want him to send messages if and only if that probability is sufficient to justify the cost to me of examining and evaluating the message. In a world where sending messages is expensive and evaluating them is inexpensive, I will receive inefficiently few messages, so I will buy additional messages by (for example) subscribing to magazines. In a world where sending messages is cheap and evaluating them is expensive, I will receive more messages than I want. Resolving that problem requires a negative subscription price, that is, a mechanism by which I can charge people for sending me messages.

The connection between attentional privacy and informational privacy exists because the sender needs information about me in order to decide whether sending a message to me is worth the cost to him. The implication of this is ambiguous because increasing the amount of such information available to him may make the outcome better or worse for me. In the limiting case of a world with complete information, potential senders know for certain whether I want to buy what they are selling, so I receive all the offers that I would want to receive and do not have to waste time

[27] Throughout this discussion, I am assuming that the purpose of messages is to propose voluntary transactions. I am, thus, ignoring cases such as harassment, where the benefit to the sender does not depend on the buyer deciding that the message is of value. I am also ignoring cases of e-mail bombing (flooding someone's mailbox in order to prevent him from using it), where the purpose of the message is to impose a cost on the recipient.

examining any that I do not want to receive.[28] In the limiting case of a world with no information (and in which the cost of sending messages is significant), it is never worth it to send a message. This latter outcome cannot be an improvement on other alternatives, since the other alternatives give me more choices, yet still permit me the option of ignoring all messages—cutting the bottom out of my mailbox and putting a waste basket underneath it.

More generally, increasing the information other people have about you can benefit you by making it easier for those who have offers that you are interested in to find you, and easier for those whose offers you are not interested in to discover your lack of interest and save themselves the cost of making the offers. If only all the world knew that I did not have a mortgage on my house, I would no longer be annoyed by phone calls from people offering to refinance it.

As this example suggests, one way of getting the best of both worlds is to have control over information about yourself and to use that control to make some information public while keeping other information private. I will return to that possibility in Section III, after discussing technologies that facilitate that approach.

Finally, it is worth noting that different societies have had different norms with regard to privacy, some of which surely reflect the differing value that individuals place on having information about themselves widely known. Consider the English upper class at the beginning of the nineteenth century, as depicted by Jane Austen. Every gentleman's income appears to have been a matter of public knowledge. One reason for this may have been that the information was crucial to families with daughters on the marriage market. A gentleman who went to some trouble to conceal his financial situation would be signaling not a taste for privacy, but an income below his pretended status.[29]

We are now finished with our theoretical discussion of privacy. One thing this discussion has made clear is that whether it is desirable for individuals to be able to control information about themselves depends on a variety of technologies—in the economist's sense, in which a technology is simply a way of transforming inputs to outputs. In particular, it depends on technologies for obtaining, concealing, and transmitting information—which will be the subject of the next part of this essay.

[28] This result is not quite as rigorous as it sounds, since the cost of evaluating an offer is already "sunk" at the point when you decide whether to accept it. Consider an offer that costs fifteen cents to evaluate and proposes a transaction that would produce a gain of ten cents for the individual receiving the offer. The receiver, having already paid the examination cost, accepts the offer and so produces a gain for the sender sufficient to more than cover the cost of sending. I will ignore such complications since I doubt they are of much real world importance.

[29] In modern-day Israel, judging by my observations, asking someone his salary is considered perfectly normal, whereas in the United States, it is a violation of norms of privacy. I have no good explanation for the difference.

III. The Technology of Privacy

Over the course of the past fifty years, a variety of technologies have been developed that substantially affect the cost of obtaining information about other people, concealing information about oneself, and transacting in information. For our purposes, they may be grouped into three broad categories: information processing, encryption, and surveillance.

A. Information processing

The earliest and best known of these technologies is information processing. Fifty years ago, a firm or government bureau possessing information on millions of individuals faced daunting problems in making use of it. Today, the average citizen can afford, and may well own, computer hardware and software capable of easily dealing with a database of that size.

One implication of this is that organizations that already have large-scale data collections are increasingly able to use them; privacy rights, in the sense in which I have been using the term, are therefore weaker. A second implication is that dispersed information that nobody found worth collecting in the past may be routinely collected in the future.

It is possible to hinder that development through the use of legal rules restricting the collection and sale of data, and such rules exist (for example, the Fair Credit Reporting Act[30]). But doing so is costly, and it is far from clear that it is useful. For the most part, dispersed information is collected in order to be used by private parties to facilitate voluntary transactions with others—an activity that typically produces net benefits.[31] Given that information is collected for this purpose, it is hard to design legal rules that prevent its occasional use for other purposes, such as locating potential targets for criminal activity. Furthermore, as the growth of the Internet makes it easier for individuals to transact with firms and individuals in other countries and, thus, moves more and more of the commercial activity relevant to U.S. citizens outside of the jurisdiction of U.S. courts, regulation of the collection and use of such information will become even more difficult.

An alternative approach is to give individuals control over information about themselves; this could be achieved through a combination of physical privacy and contract. Information about an individual is frequently produced by voluntary transactions, such as purchases of goods and

[30] The Fair Credit Reporting Act, 15 U.S.C. sec. 1681 et seq., regulates firms that produce consumer reports—information about an individual consumer used by a firm to determine whether to extend that consumer credit, to decide whether to hire him, or to accomplish some other legitimate business purpose. The text of the act is available on-line at http://www.ftc.gov/os/statutes/fcra.htm.

[31] Although it might under some circumstances produce net costs associated with attentional privacy.

services, and thus starts out in the possession of both parties to a transaction. If one party wishes that the information should be kept confidential, that party can specify this in the terms of the initial transaction, which is, of course, often done in a variety of settings. The same information-processing technology that makes it relatively inexpensive to keep track of large numbers of facts about vast numbers of people also makes it inexpensive to keep track of the conditions under which various pieces of information can be disclosed.

A more exotic and potentially more secure approach, which may become increasingly practical as a result of technologies to be discussed in the next section, is to engage in transactions anonymously. When an individual does this, relevant information about him is never put in the control of anyone else, not even the other party to the transaction. More generally, one possibility implicit in the combination of technologies for information processing and encryption is a shift to something more like a private property/freedom of contract model for personal information—a point we will return to in the next section.

B. Encryption

Many forms of modern communication, including e-mail and cellular telephony, are physically insecure; intercepting messages delivered via these media is relatively easy. In order to protect the privacy of such communications, it is necessary to make them unreadable to those who might intercept them. This is done by encryption—scrambling a message in such a way that only someone with the proper information—the key—can unscramble it.

The most important modern development in this field is public-key encryption.[32] An individual generates a pair of keys, two long numbers having a particular mathematical relation to each other. If one key is used to scramble a message, the other is required to unscramble it. In order to make sure that messages sent to me remain confidential, all I have to do is to make sure that one of my keys (my "public key") is widely available, so that anyone who wants to send me a message can find it. The other key (my "private key") is my secret, never revealed to anyone. Anyone who has my public key can use it to encrypt a message to me. If someone else somehow steals a copy of the public key, he can send me secret messages too. But only someone with my private key, which I need never make available to any other person, can read the messages.

The same technology solves a related problem: how to prove to the recipient of my message that it is really from me. In order to sign a

[32] For a much longer discussion, see David Friedman, "A World of Strong Privacy: Promises and Perils of Encryption," *Social Philosophy and Policy* 13, no. 2 (Summer 1996): 212–28.

message digitally, I encrypt it with my private key.[33] The recipient decrypts it with my public key. The fact that what he gets is understandable text rather than gibberish demonstrates that the message was encrypted with the matching private key, which only I have.

A digital signature not only demonstrates, more securely than an ordinary signature, that I really sent the message, it also demonstrates it in a way that I cannot later deny. You now possess a digitally signed message—the original, before decryption—which you could not have created yourself. Thus, you can prove to interested third parties that I actually sent the message, whether or not I am willing to admit it. Furthermore, since there is no way of changing the digitally signed message without making the signature invalid, a digital signature, unlike a physical signature, demonstrates that the message has not been altered since it was signed.

Encryption technology also has two other privacy-enhancing applications. One is an anonymous remailer. If I wish to communicate with someone without the fact of our communication being known, I send the message through a third party who is in the business of relaying messages. In order to preserve my privacy from both the remailer and potential snoops, I encrypt my message with the recipient's public key, add to it the recipient's e-mail address, encrypt the whole package with the remailer's public key, and send the package to the remailer. The remailer uses his private key to strip off the top layer of encryption, permitting him to read the e-mail address and forward the message. If I am concerned that the remailer himself might want to keep track of who I am communicating with, I can bounce the message through multiple remailers, providing each with the address of the next. Unless all of them are jointly spying on me, my secret is safe.

The second important application is anonymous digital cash. Using encryption, it is possible for an issuer of money to create the digital equivalent of currency. This permits a person, by sending a message to someone else, to transfer claims against the issuer without either person having to know the other's identity and without the issuer having to know the identity of either of the two parties.

Consider a world in which all of these technologies exist and are in general use. In such a world, it is possible to do business anonymously, but with a reputation. Your cyberspace identity is defined by your public key. Anyone who can read messages encrypted with that public key must have the matching private key—which is to say, must be you. The same

[33] The process used for digital signatures in the real world is somewhat more elaborate than this, but the differences are not important for the purposes of this essay. A digital signature is produced by using a hash function to generate a message digest—a string of numbers much shorter than the message it is derived from—and then encrypting the message digest with the sender's private key. The process is much faster than encrypting the entire message and almost as secure.

is true for anyone who can sign messages with the private key that matches that public key.

One disturbing implication of this, which I have discussed elsewhere,[34] is the possibility of criminal firms operating anonymously, but with brand-name reputation. A more attractive implication is that, in such a world, the private property model of personal information becomes a practical possibility. If, when I buy something from you, neither of us knows the identity of the other, then neither of us can obtain the relevant transactional information—the fact that a certain other person bought or sold a particular good—without the cooperation of the other person. Hence, transactional information starts as the sole property of the person whom the information is about; that person is then free to suppress it, publish it, or sell it, whichever best serves his interests.

A second feature of this world relevant to the issues we have been discussing comes from a different use of the technology of encryption: technological protection of intellectual property.[35] It may soon become practical to distribute intellectual property in a cryptographic container, that is, as part of a computer program which controls access to its contents; IBM refers to this as a "cryptolope." Use of the contents will then require a payment, perhaps in digital cash, with the container regulating the form of use. Combining such technologies with the use of intelligent software agents that can negotiate on-line contracts, we have the possibility of a world where it will be practical to treat information as something close to ordinary property. One could, for example, sell or give away transactional data about oneself in a form that could only be used for specified purposes, or only in association with specified payments.

This set of possibilities represents one part of a more general pattern. The combination of encryption, information processing, and on-line communications will permit a much more detailed control over information flows—at least on-line information flows or flows of information that originate on-line—than has been possible in the past. Thus, to take an entirely different example, there is no technical barrier preventing the creation of an e-mail program that would permit someone who wished to protect his attentional privacy to charge a price for receiving e-mail—and to simply trash, without human intervention, any messages that came without an associated payment. Nor is there any barrier to making such software distinguish among senders, receiving messages for free if they are digitally signed by people from whom the owner of the software wants to receive messages.

For a less exotic example, consider the marketing of magazine subscription lists. With current transactional technology, the fact that a

[34] Friedman, "A World of Strong Privacy."

[35] See David Friedman, "In Defense of Private Orderings: Comment on Julie Cohen's 'Copyright and the Jurisprudence of Self-Help,'" *Berkeley Technology Law Journal* 13, no. 3 (Fall 1998): 1151–72.

transaction took place is known to both parties. Therefore, I cannot directly control access to the fact that I am a subscriber to a magazine—as I could if the transaction had taken place on-line between anonymous parties. But a magazine may, and some do, restrict its use of that information by contract, by promising not to make its mailing list available to others or by giving the customer the choice of whether or not to have his name and address sold to other merchants. Such contractual arrangements will become easier as more and more transactions shift to digital forms, where individualized contract terms are considerably less expensive to implement than they are under conventional contracting technology.

Suppose a magazine that you subscribe to lets you decide whether or not to be on the mailing lists that it provides to others. One option is to keep your name and address private; another is to permit it to be freely sold. A third option, which many might find more attractive than either of the others, is for the magazine to sell merchants access to its subscribers without revealing the subscribers' identities. This could be done easily enough by having the magazine operate its own remailer. Information about each subscriber would be provided to merchants interested in communicating with him. Merchants would get information about what the subscriber had purchased, and any other information the magazine had that was relevant to what the subscriber would want to buy; however, merchants would not get any information that could be used to identify the subscriber. The merchant would then send a message directed at that particular unnamed subscriber, which the magazine would forward to him.

Currently, mailing lists are usually not sold, but rented for a fixed number of uses. Modern technology makes possible a more sophisticated version of such a transaction. Ultimately, we could have third-party remailers holding large amounts of information on unidentified individuals in ways that would permit merchants to search for individuals possessing combinations of characteristics that make them attractive targets for specific offers; this could be done without permitting any outsiders to link this information with a particular identity. The same result could be produced even more securely—without having to trust the remailer—by having individuals interact via anonymous on-line personas. This would make the facts of transactions public, which would help customers attract desirable offers, but would keep the identity of the realspace person corresponding to a particular cyberspace persona private.[36] One thus abandons privacy sufficiently to permit voluntary transactions, which can

[36] For an early and still interesting fictional exposition of the idea of separating realspace and cyberspace identities, see Vernor Vinge's novelette "True Names," included (among other places) in Vinge, *True Names and Other Dangers* (New York: Simon and Schuster, 1987). A more recent fictional effort, picturing something much closer to what we are actually likely to see in a few decades, is Marc Stiegler, *Earthweb* (New York: Simon and Schuster [Baen Books], 1999).

take the form of an offer to an unknown identity, but retains it for protection against involuntary transactions. It is hard to burgle the house of a cyberspace persona when the only identifying information you have about him is his public key and a remailer address.

With the exception of fully anonymous e-cash (which we know how to do but which nobody has so far done[37]) and cryptolopes (which are still mostly in the development stage), the fundamental technologies I have described above already exist. Public-key encryption has been implemented in a variety of forms, including a widely distributed free program.[38] Anonymous remailers currently exist. Digital signatures are widely used. But for the most part, these technologies have been applied only to *text, and so have affected only that part of private and commercial life* that is embodied in text messages.

As computers become more powerful and the bandwidth of digital networks increases, that situation will change. Using wide-bandwidth networks and virtual-reality software, it will eventually be possible to create the illusion of any transaction that involves only the senses of sight and sound. Further in the future, we may succeed in cracking the "dreaming problem," figuring out how our nervous system encodes the information that reaches us as sensory experience. At that point, we will no longer be limited to reproducing only two senses. We will be able to create, by the transmission of information in digital form, the illusion of any interaction that could take place in realspace.

As more and more of our activity shifts into cyberspace, encryption and related technologies make possible a degree of control over both the creation and the transfer of information that is very much greater than that which we now have. Given this, the property justification for privacy, rejected in Section II, comes back into the argument.

What about the argument against privacy—that one reason I may wish to conceal information about myself is in order to defraud my trading partner? This becomes a less serious problem on-line, where encryption technology restricts parties to voluntary transactions. You can, of course, conceal information about yourself if that information is under your control, and you can attempt to defraud me with false information. But I can refuse to transact with you unless you agree to reveal the relevant information in verifiable form; if you decline, that fact signals something about the information that you are keeping private.

[37] There have been experiments with e-cash. Most notable of these experiments was that performed by the Mark Twain Bank of St. Louis, which worked with David Chaum, the cryptographer responsible for many of the fundamental ideas in the field. The currency was semianonymous, meaning that the issuing bank could identify one party to the transaction if it had the cooperation of the other.

[38] PGP (Pretty Good Privacy) is a freeware program (also available in a commercial version) for doing public-key encryption and decryption, and for keeping track of other people's public keys. It is available from, among other places, http://web.mit.edu/network/pgp.html.

C. Surveillance devices—toward a transparent society

While technological developments in on-line communication are moving us toward a high level of privacy in cyberspace, developments in surveillance technology may be moving realspace in precisely the opposite direction, for two reasons. One is that surveillance devices provide an inexpensive and effective way of reducing crime, one that is becoming increasingly popular. The other is that, as these devices become smaller and cheaper, it becomes more difficult to prevent surveillance. We may be moving toward a world in which video cameras with the size and aerodynamic characteristics of a mosquito are widely available.

Physicist and science fiction author David Brin, on whose book *The Transparent Society*[39] this section is largely based, argues that in the future, privacy will no longer be an option for most people. We will be limited to two choices: a world in which those in power know everything that they want to know about everyone, and a world in which everyone knows everything he wants to know about everyone. Brin, not surprisingly, prefers the latter. He envisages a future with video cameras everywhere—including every police station—all generating images readily accessible, via some future equivalent of the World Wide Web, to anyone who is interested.

If Brin is correct, physical privacy in realspace will vanish. Individuals will protect their informational privacy in the same ways in which people in primitive societies without physical privacy protect their informational privacy: by adopting patterns of speech and behavior that reveal as little as possible of what they actually believe and intend. This will represent a substantial rent-seeking cost, which must be added to the rent-seeking cost of individuals processing enormous quantities of public information in order to learn things about all those with whom they expect to interact.

Two qualifications are worth making to Brin's picture. The first is that he is assuming that the technology of surveillance is going to outrun the technology of physical privacy, that the bugs will beat the screens, that video mosquitoes will not fall victim to automated dragonflies. While he may be correct, it is hard to predict in advance how the balance will turn out. We might end up in a world where legal surveillance is cheap and easy, but where illegal surveillance is difficult; this would give us the choice of how much privacy we would have.

One possible compromise is for people to have privacy in private spaces, but not in public spaces. This would represent a further development along the same lines as computerized databases. What you do in public spaces, like the public records produced by your life,[40] has always been

[39] David Brin, *The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?* (Reading, MA: Addison-Wesley, 1998).

[40] There are a few exceptions created by the law, such as the rules under which a record of the criminal conviction of a minor may sometimes be expunged. (In Florida, for example, such a record may be expunged when the minor reaches twenty-six years of age. See Fla. Stat. chap. 943.0515, on the World Wide Web at http://www.leg.state.fl.us/citizen/documents/statutes/1994/CHAPTER_943.html.)

public in a legal sense. A video surveillance network, coupled to computers running pattern-recognition software and sorting and saving the resulting data, would simply put that public information in a form that would permit other people to find and use it.

A second qualification is that although the technology that Brin anticipates will produce information, it might not always be verifiable information. Suppose I am conducting an adulterous affair. My suspicious wife can use a video mosquito to obtain video footage of me in flagrante delicto with my paramour. That footage may be of very limited use in court, though, since it could have been produced just as easily if I were not conducting an affair—using video-editing software instead of a camera. To the extent that modern technology makes it easy to forge evidence, evidence without a provable pedigree becomes worthless. It may be easy to get a mosquito camera into my bedroom, but it is somewhat more difficult to also get a reliable witness in there to prove that that camera really took that film.[41]

Encryption technology provides one approach to solving this problem. Conceivably, a manufacturer could build a sealed, tamperproof camera, complete with its own private key. The camera would digitally sign and time-stamp[42] its films as it produced them, making it possible to prove at a later date that those particular films were created by that camera, at that time, and have not since been edited.

One difficulty with this approach is that a camera records not facts about the outside world, but facts about the pattern of light that comes into its lens. To defeat such a camera, I could build a lens cap capable of generating computer-synthesized holographic images. I would then put the lens cap on the camera and play whatever I want the camera to see; it would see the images and sign them, making them appear authentic. As this example suggests, figuring out the implications of technologies that do not yet exist, or that exist only in primitive forms, is not a trivial problem.

IV. Conclusion

In Section II of this essay, I sketched out an economic analysis of privacy. The conclusion was that increasing the ability of individuals to

[41] A human solution to the problem of forged data was proposed by Robert Heinlein in *Stranger in a Strange Land*: a body of specially trained "fair witnesses," whose job it was to observe accurately and report honestly. See Heinlein, *Stranger in a Strange Land* (New York: Putnam, 1961).

[42] One way of time-stamping a digital document is to calculate a *hash* of that document—a much shorter string of digits derived from the document in a fashion that is difficult to reverse—and post the hash in some publicly observable place. The document is still secret, since it cannot be derived from the hash. The existence of the hash at a given date can later be used to prove that the document from which it was derived—in our case, a digital video—existed at the time that the hash was posted. The fact that the hash function cannot easily be reversed means that one cannot post a random hash and then later create a suitable document that would be a source of that particular hash.

control information about themselves had both desirable and undesirable effects, making it unclear whether, on net, we were better off with more or less privacy. One argument that I considered and rejected was that increased privacy rights—at least over information that originates with the person that it is about—are efficient because they make it possible to convert such information into private property and then allocate it efficiently through market transactions.

That argument is harder to reject when applied to the information technology of a few decades hence. It may become possible to create transactional information in such a way that each piece of information originates in the possession of a single person. It may also become possible, given the much lower transaction costs of on-line transactions, to then use private transactions to allocate information to its highest-valued users. If these things occur, we would end up with a world in which information that is generated by cyberspace events—on-line transactions—is characterized both by a high degree of control by those whom the information concerns and by an efficient market for its creation and allocation.

There is no reason to expect the same to be true in realspace. If anything, the combination of improved surveillance technology and improved information-processing technology is likely to make increasingly large amounts of realspace information about everyone inexpensively available to everyone else. We then have both the advantages and the disadvantages of a low-privacy environment. Individuals cannot hide unattractive facts about their doings in realspace from those whom they transact with, which makes many forms of commercial and social fraud impractical. The cost of privacy becomes the cost of behaving in a way that reveals as little as possible about oneself.

If realspace is public and cyberspace is private, the amount of privacy that individuals have depends critically on the importance of each type of space, and on the links between the two. It does me no good to protect my messages with strong encryption if a mosquito camera is watching me type the unencrypted original. In extreme versions of this scenario, versions where both Brin's vision of realspace and my vision of cyberspace are realized in full, privacy depends critically on mechanisms for computer input that cannot be observed from the outside. The low-tech version of this is touch-typing under a very secure hood; the high-tech version is a link directly from mind to machine. If some such method makes it possible to protect cyberspace privacy from realspace prying, the balance between public and private then depends on how much of what we do is done in cyberspace and how much in realspace. It is going to be an interesting century.

Law, Santa Clara University