

Privacy and Information Technology

Judith Wagner DeCew

Associate Professor of Philosophy and Hayden Faculty Fellow

Clark University, Worcester, MA

I. Introduction

In both law and ethics, "privacy" is an umbrella term for a wide variety of interests. Much of the vast literature on privacy has focused on an interest protected in American tort law referred to as the crucial core of privacy, and often described as "having control over information about oneself." Beginning in 1965, the United States Supreme Court also recognized an apparently distinct constitutional right to privacy. Because there is no right to privacy explicitly guaranteed in the Constitution, however, and the constitutional cases invoking this right are so diverse, there has been a great deal of criticism and controversy surrounding the constitutional right of privacy. Despite this confusion, reaction to recent Supreme Court confirmation hearings has made it clear that many in the American public and congress are unwilling to give up the privacy protection they currently enjoy.

I first discuss philosophical origins of privacy, and the historical divergence between privacy protection in tort and constitutional law. Second, I describe areas of technological advance in which informational privacy concerns - both moral and legal - are raised. For each I suggest some responses and possible solutions. I then explain my general approach to privacy concerns arising from technological advance. My view is that new technologies must be managed appropriately, to safeguard privacy vigorously and comprehensively, without sacrificing their technological benefits.

Let me make two preliminary points. First, I shall not place special weight on privacy as a right, as opposed to a claim or an interest. A claim is often described as an argument that someone deserves something. A right is then a justified claim; justified by laws or judicial decisions if it is a legal right, by moral principles if it is a moral right.ⁱ My points are significant, however, independently of whether or not we can ultimately make sense of rights, explain when they are binding, or show that they are reducible to utilitarian claims. The literature on privacy uses rights terminology, and I accommodate that. Yet I begin by referring to privacy more generally as an interest, by

which I mean something it would be a good thing to have, leaving open how extensively it ought to be protected.

Second and more obviously, nothing in my discussion requires assuming one endorse all the decisions in cases I cite. One can appreciate the controversy however one views the actual judgments.

II. Philosophical and Other Origins of Privacy

Some concept (or multiple concepts) of privacy has played a fundamental role in political and religious writings as well as in biological, anthropological, and sociological studies from antiquity to today. There is ample evidence for this, some of which is explicit in written material and some of which derives from customs and social practices.

Consider first two examples from political philosophy. An important and well-known (though sometimes controversial) tenet since the time of Aristotle has been the dichotomy between public and private realms. In his book on politics, Aristotle saw the polis, the concept of a structured body politic and province of political activity, as a public sphere where details of government and the proceedings of the city-state developed.ⁱⁱ Political animals by nature, men (but not women or slaves or children) were intended to participate fully in the polis. In ancient times as well as later, the trend was to set limits on the power of governmental authority by separating from this public sphere various places and activities viewed as illegitimate arenas for public regulation. For Aristotle, the oikos was a private sphere attached to the home, namely the private household. Family life served as a paradigm of the private sphere that defined the role of women.

A second instance in political literature comes from John Locke, who marked off the distinction between public and private property in his Second Treatise on Government (1690). The original state of nature, according to Locke, is for all "a state of perfect freedom to order their actions, and dispose of their possessions and persons as they see fit, within the bounds of the Law of Nature."ⁱⁱⁱ In the state of nature no person has exclusive rights to the earth. The earth and all the bounty produced by nature belong to all in common. Nevertheless, each person possesses himself (or herself) absolutely and has property rights to that with which he mixes his labor. Everyone has a property right to "his own person" and can extend it through sweat and labor. Thus what belongs to and is acquired by the self is private property and is distinctly separate from what is owned publicly or in common with all. In Locke's Treatise there are other contexts in which the separation between public and private remains, yet the

relationship between the two spheres is more complex. Those who freely consent to create a political society thereby establish public means, namely the maintenance of civic order through social contract, to assure private ends, specifically the protection of life, liberty, and property. In contrast to Aristotle's view, the state becomes for Locke a necessary means for public protection of certain private ends.

Political philosopher Jean Bethke Elshtain has argued that a wide array of thinkers "of the Western political tradition assumed and deployed some form of a distinction between the public and the private....As conceptual categories, public and private ordered and structured diverse activities, purposes, and dimensions of human social life and thinking about that life."^{iv} The public/private split has sometimes been taken to reflect differences between the appropriate scope of government, as opposed to self-regulation by individuals. It has also been interpreted to differentiate political and domestic spheres of life. These diverse linguistic descriptions capture overlapping yet nonequivalent concepts. Nevertheless they share the assumption that there is a boundary marking off that which is private from that which is public.

In addition to these philosophical references to a distinction between public and private, consider as well biological and anthropological studies that provide evidence of the fundamental value placed on privacy. Philosopher Alan Westin, has reviewed animal studies demonstrating that a desire for privacy is not distinctively human.^v Such studies show, for example, that virtually all animals seek periods of individual seclusion or small-group intimacy. Usually described as a tendency toward territoriality, such patterns serve various biological purposes, especially that of ensuring propagation of the species. Westin concludes that "the parallels between territory rules in animals and trespass concepts in human society are obvious: in each, the organism lays claim to private space to promote individual well-being and small-group intimacy."^{vi}

Anthropological studies by Margaret Mead and others, as well as social and psychological research, support this view that privacy is a cross-cultural and cross-species universal.^{vii} They have shown that virtually all societies have techniques for setting distances and avoiding contact with others in order to establish physical boundaries to maintain privacy. Although some primitive cultures appear to show no concern for privacy for changing clothes, bathing, birth, death, and so on, anthropologists have found that these cultures use various psychological methods for gaining privacy for the individual or family when communal life makes such physical privacy protection impossible. Withholding feelings and expression, averting one's eyes, facing a wall, for instance, provide more subtle ways of putting up social barriers.^{viii}

This brief survey demonstrates that despite the emphasis placed on privacy in varied contexts, the idea of privacy employed is not always the same. Privacy may refer to the separation of spheres of activity, limits on governmental authority, forbidden knowledge and experience, limited access, and ideas of group membership, to name a few possibilities. Consequently, this background sketch provides evidence that privacy is commonly taken to incorporate different clusters of interests.

Anthropological literature documents the increased physical and psychological opportunities in modern societies to gain privacy through more anonymity, mobility, and economic autonomy. At the same time, however, greater population density, technological advances, and increased governmental power all undermine an individual's ability to maintain a private space within a broader social community.

III. Legal History of Two Privacy Interests

It is likely that technological advance was a major impetus for the codification of privacy protection in written law in the United States. American law has evolved to protect two apparently different rights to privacy--one developed in the last ninety years in tort and Fourth Amendment law, the other first announced as a constitutional right in 1965. Taken within the context of the influence of common law, both are relatively recent developments in U.S. law.

One of the most influential law review articles ever written was "The Right to Privacy" by Samuel Warren and Louis Brandeis. Arguing that "political, social, and economic changes entail recognition of new rights" and "the common law...grows to meet the demands of society,"^{xix} Warren and Brandeis urged that protection we already had against actual bodily injury (battery), attempts (assault), nuisances (offensive noises and odors), slander, and even alienation of a wife's affections (which was held remediable!)^x should be supplemented with a right to privacy protecting a person even if the injury is merely to individual feelings. Relying on Judge Cooley's phrase, the right "to be let alone,"^{xi} and cases they felt were already precedents, they argued that the law should "protect the privacy of private life"^{xii} by securing for an individual the right of determining the extent to which his or her written work, thoughts, sentiments, or likeness could be given to the public. Citing recent inventions and numerous mechanical devices such as high-speed cameras and presses for mass production of newspapers that "have invaded the sacred precincts of private and domestic life,"^{xiii} they urged the law to offer a remedy for protection from such invasions.

One story holds that Warren was upset about newspaper publicity concerning his daughter's wedding. That

has been disputed. If correct, however, it makes clear the early link between technological advance, namely the rise of large-scale media coverage through newspapers, and growing worries about protecting individual privacy.

Up until 1890 when Warren and Brandeis' paper appeared, American law had been extremely cautious about protecting emotional harms for at least two reasons: (i) the difficulty of assessing damages for emotional harms and (ii) the subjectivity of the findings based on a state of mind, especially where there is no parallel or concomitant physical injury. While the second is perhaps a reasonable concern, the first is a poor excuse for denying recovery. Surely it is no less difficult to fix a dollar value on a finger lost, an arm, or a life. But Warren and Brandeis were arguing that existing law already recognized a principle of privacy derived from common law in such cases as breach of trust and defamation, which, when applied to new facts, could protect individuals from the press, photographers, or anyone with devices for recording or reproducing sounds or scenes. Thus they claimed not to be advocating judicial activism, that is, judicial legislation or the addition of legal principles by judges.^{xiv}

While the earliest test cases failed to protect the right Warren and Brandeis argued for,^{xv} both the American public and subsequent cases^{xvi} soon endorsed and expanded it in tort and Fourth Amendment cases. What I am referring to as "tort privacy" now covers interests individuals have in protection from unwarranted observations of themselves and their activities, materials, and conversations, whether these occur in person or through electronic surveillance. Owing to the growth of computer technology and capacities for rapid recording and retrieval of vast amounts of data, protection has also been increased against having one's communications reproduced or misused without authorization, and against having information about oneself appropriated and exploited. Such abuse of information includes attacks on one's reputation, disclosure of embarrassing facts, and use of one's name or likeness without permission.^{xvii} Alternatively, the protected data may be relevant to the Privacy Act of 1974 which covers employment, academic, and medical records.

The second legal right to privacy protected in the United States is even more difficult to describe. It was first recognized by the Supreme Court in 1965 when it overturned convictions for violating Connecticut statutes which banned disbursement of contraceptive-related information, instruction, and medical advice to married persons.^{xviii} Controversy began almost immediately because there were four opinions written in defense of the judgment, each offering a different justification. In a subsequent case, Justice Brennan argued, ... if the constitutional right to privacy means anything, it is the right of the individual, married or single, to be free from unwarranted intrusion into matters so fundamentally affecting a person as the decision whether to bear or beget

a child.^{xix}

This paved the way for using the constitutional right to privacy as a defense for the famous and controversial Roe v. Wade^{xx} abortion decision the following year. Then in Moore v. City of East Cleveland privacy was extended to decisions concerning family composition and living arrangements.^{xxi} Furthermore, constitutional privacy was cited as one major reason for overturning mandatory sterilization laws,^{xxii} and for allowing "possession of obscene matter" in one's home,^{xxiii} interracial marriage,^{xxiv} and attendance at public schools.^{xxv}

Many commentators have defined the tort interest in privacy as "control over information about oneself," and that interest is referred to as the classic notion of privacy. Given this intuitive characterization of tort and Fourth Amendment privacy concerns, it is possible to see a conceptual difference between privacy interests protected in tort and Fourth Amendment law and in constitutional privacy. Paradigmatically, tort privacy cases involve concerns with information--either conveyed by an individual (e.g. in private conversation or activity) or about an individual (e.g. records, newspaper stories). We should take care to note, however, that tort privacy is not as univocal as this description indicates. In tort and Fourth Amendment law, intrusive behavior such as snooping or spying can violate privacy even if no information is gathered or disseminated. It now protects one as well from harassment from bill collectors and stomach pumping for evidence.^{xxvi} The constitutional privacy cases are even more diverse, ranging over issues related to one's body, family relations, life style, and child rearing.

In 1977, in Whalen v. Roe, the Court made its most comprehensive effort thus far to define the legal right to privacy, embracing both (i) an "individual interest in avoiding disclosure of personal matters" and (ii) an "interest in independence in making certain kinds of important decisions."^{xxvii} The Whalen case was deemed to involve both aspects of privacy. Nevertheless, the Court upheld New York statutes for maintaining computerized records of prescriptions for certain dangerous but lawful drugs (morphine used by cancer patients, for example) even though the records included the patients' names and addresses. Here was a data base of sensitive information, where access was not controlled. Although Whalen was said to involve both privacy interests, what I have been calling the tort interest in privacy (which still arises, of course, in Supreme Court cases) and the constitutional right to privacy (now often cited in lower court decisions) are still often viewed as separable interests.

One theme of my book, In Pursuit of Privacy: Law, Ethics and the Rise of Technology, focuses on constitutional privacy and the philosophically interesting claim that the line of constitutional cases since Griswold involve rights which have "no basis in any meaningful conception of privacy."^{xxviii} I argue that there is a similarity

of reasons for protection of privacy in varied cases, showing that the close relationship between tort and Fourth Amendment and constitutional privacy claims is philosophically well-motivated, historically accurate, and reflected in ordinary language--all considerations that justify a broad conception of privacy, which I characterize as a multi-faceted cluster concept. Another theme in my book focuses on ways advancing technology threatens tort or informational privacy. I examine privacy issues raised by (i) database information storage and (ii) new telephone and computer services such as caller identification and e-mail.

IV. Database and On-line Information

Consider first a case involving credit bureaus and the U.S. Post Office.^{xxix} We now pay 32 cents in the United States for a first-class postage stamp, more than double its price in 1960, even when adjusted for inflation. But those who are frustrated about paying more money for stamps may be even more concerned that this is not the only step the U. S. Postal Service has considered taking to increase profits. The postal service has also studied plans to sell addresses, as part of the first nationwide electronic address list, to direct-mail companies and other businesses. Unfortunately, this profit-seeking move is potentially very costly to consumers, as it risks major losses of individual privacy.

The problem does not lie solely with the proposed address list. It is what businesses, investigators and government can do by matching such a list with names and other information available for sale. The postal executives have claimed the list will reduce undeliverable mail and that they will strictly control use of the list. We may well wonder why, then, the direct mail industry has become so excited at the prospect.

In America, when you request a store catalogue or file a change of address card or fill a prescription, your name goes on a list. When you apply for a mortgage, a driver's license, or telephone service, you part with private details about yourself and often supply extensive amounts of information. Virtually every transaction today is recorded in a computer, and a recent consequence is the routine collection and transfer of personal information in digitized form. The sale of such data for profit in the American private sector is now a multimillion-dollar business dominated by the leading credit bureaus: TRW in California, Equifax in Atlanta and Trans Union Credit Information in Chicago. The sheer volume of information stored and repeatedly resold is stunning: these information sponges keep more than 400 million records on 160 million individuals. [Consider this data: TRW 1988 revenues: \$ 335,000,000, 155 million individual files; Trans Union 1988 revenues: \$300,000,000, 155 million

files; Equifax 1988 revenues: \$269,000,000, 100 million files, and they are not the only ones in the business.^{xxx]}

At little or no cost, the bureaus make it easy for almost anyone to find out another individual's income, employment status, marital status, driving record, real estate holdings, credit limit, and even civil and criminal court records. Yet it is difficult or impossible for individuals to find out if information about them is being used. A Business Week article described how

...the long arm of American Express Co. reached out and grabbed Ray Parrish. After getting his credit card in January, the 22-year old New Yorker promptly paid bills of \$331 and \$204.39 in February and March. Then he got a surprising call. His credit privileges were being suspended, an American Express clerk informed him, because his checking account showed too small a balance to pay his April charge of \$596. A contrite American Express now says it should have asked before peeking, and it reinstated Parrish after he paid his bill from his savings and cash on hand. But that was beside the point. "I felt violated," says Parrish, who has kept his card because he needs it. "When I gave them my bank account number, I never thought they would use it to routinely look over my shoulder."^{xxxi}

TRW, Equifax, and Trans Union claim to guard their information, but they actually sell it readily. As a test, one of the editors of Business Week

signed up with two superbureaus, identifying himself as an editor at McGraw-Hill Inc. He told one fib: that he might be hiring an employee or two and would need their credit reports. After a perfunctory check, both bureaus gave him carte blanche--and revealed the surprising breadth of their files....Provided with just the names and addresses of two of his colleagues, one superbureau produced their credit reports--including their social security numbers that the editor didn't have--for \$20 apiece. The superbureau manager warned that one colleague's mortgage was ominously large, then offered to fax the reports.

The second arrangement was more open-ended. For a \$500 initial fee, the editor got access via his home computer to the superbureau's data base. Free to explore, he again checked on his colleagues, at about \$15 per report. Then he ran two names whose prominence might have set off alarms if the credit agency audited use of its files. One was Representative Richard J. Durbin (D-Ill.), the other Dan Quayle [who was vice-president at the time.]

There were no alarms....There was nothing juicy.^{xxxii}

The editor learned that Quayle charges more at Sears, Roebuck than at Brooks Brothers and has a big mortgage; he

was also given all Quayle's credit card numbers. When told of the search, Quayle was not amused.

There are at least four sets of privacy problems generated by these huge credit bureau databases: (1) First, once one is in a database in the United States, one loses access to and control over the information. There are few legal restrictions at present, and a great deal of money can be made by selling data. Economic and market factors make the information vulnerable to exposure. What one may have thought was private, such as shopping and spending habits or medical problems, soon can become public. (E.g. results of genetic testing.)

(2) Second, there are many loopholes in current legal protections. That is, there is a serious lack of protection despite statutory attempts to salvage privacy.

The Fair Credit Reporting Act of 1970 is a case in point. It sounds good. It gives individuals the right to see and correct their credit reports and limits the rights of others to look at them. But it has five exceptions, including a big one: Anyone with a "legitimate business need" can peek. Legitimate isn't defined.

Then there's the Right to Financial Privacy Act of 1978. It forbids the government to rummage through bank-account records without following set procedures. But it excludes state agencies, including law enforcement officials, as well as private employers. And more exceptions are tacked on every year.^{xxxiii}

These loopholes minimize the effectiveness of the legislation. Moreover, the patchwork of legal protections is peculiar and difficult to justify. Rental records from a video store are protected, for example, while medical insurance records, which often contain more important and more personal information, are not. This is especially disturbing since Blue Cross/Blue Shield and other health care providers now require detailed explanations of treatment before granting even partial reimbursement, thus creating new medical data files for each payment.

(3) Third, private individuals can now use personal computers and Internet services to gain access to database information. New software developed by TRW, Lotus Development Corporation and others, magnifies access to this information because of its low cost, ease of use, and lack of safeguards. What is more, these computer programs allow unlimited use of the information purchased. Similar information is now available on-line, through privately held CDB Infotek in Santa Ana, California, and Information America in Atlanta. Both can be called on voice lines, and searches conducted through these companies can yield information such as divorce records; mortgage, IRS, and other financial data; and even individual social security numbers.^{xxxiv} It is unnerving to learn that a public agency such as the U.S. Postal Service would consider profiting from such efforts, by providing a national address directory with no "unlisted" option. One can, of course, ask that one's name be removed from

mailing lists. One can decline to provide information on certain forms. But there is no guarantee that one's name will be removed. Moreover, being added to a database is unavoidable when one applies for credit cards, gets a telephone or enters a hospital, and one cannot dictate where and to whom the information goes.

To be fair, it is important to note that Lotus and Equifax have withdrawn some of their prospective programs from the market--namely, "Lotus Marketplace: Households," and "Lotus Marketplace: Businesses," which anyone could tap into with a personal computer. These programs gave personal information on names broken down by categories that included gender, age, marital status, dwelling unit type, and shopping habits, on about 120 million households. After a storm of protest from 30,000 consumers, the products were recalled. Equifax has also said it is giving up its controversial practice of selling target lists drawn from confidential credit files to purveyors of junk mail.^{xxxv}

These are clearly major concessions to the growing public sentiment that electronic databases and on-line services providing access to sensitive information are used in ways that threaten personal privacy. Yet other data bureaus and Internet data services insist they have no plans to reduce access to their information banks. And the store of data continues to increase. Information from the U.S. census taken in 1990 was considerably more detailed than in the past. The most recent census data on house values, family membership, ethnicity, elderly needs, transportation habits, and educational level are now available on CD-ROM and floppy disk, providing information easily and inexpensively to direct marketers and others who can access and convert into more usable formats.

(4) Fourth, data once recorded rarely disappears. Yet obsolete information can be misleading or incriminating out of context. Moreover, in any database, the information may be erroneous. Surveys in 1988 and 1991 found errors in 43 - 48 percent of credit reports, including as many as 19 percent with inaccuracies that could lead to denial of credit.^{xxxvi} Errors may not be the fault of the credit bureaus. Sometimes an original public record is itself inaccurate. Regardless of an error's source, however, there are no clear or established procedures for correcting it. Simply finding out if the information given out about oneself is inaccurate may not be difficult. In 1996, TRW provided one free copy per year of any individual's own credit file on request, and Equifax and Trans Union charged a fee of only \$8.00 for each report.^{xxxvii} Despite easy access to files, however, many people have horror stories about what happens after they discover an error. Correcting an error may be nearly impossible. One man reportedly contacted a credit bureau repeatedly to correct erroneous information. Soon after, he was denied credit for a loan on the grounds that computer records of his frequent inquiries concerning his credit rating indicated

he may well have been "tampering" with the information, and thus his high credit rating was viewed as unreliable!

V. Caller Identification

My second illustration of developing technology clashing with privacy is caller identification.^{xxxviii} For several years, telephone companies have been offering a service to businesses with "800" or "900" telephone numbers that routinely provides marketers with end-of-the-month lists of the phone numbers of all their callers, with no restrictions on the use of the information. Those lists are often sold to others seeking to target new customers. The service is rapidly expanding: thanks to technology now being developed, all callers can be identified by their phone numbers to whomever they call, even if their numbers are unlisted in a telephone directory. It is simple: for as little as \$6.50 a month as a service fee, plus a one-time equipment charge of \$29 - \$80, customers can install on their phone an electronic screen that flashes every incoming number while the phone is still ringing. Telephone companies can also deliver the name, as well as the number, of the incoming caller, and that is quickly becoming the service norm. Caller ID was first introduced in the United States in New Jersey in 1987. By 1991 it was approved in over 20 states and under consideration in 13 others.^{xxxix}

Some legal theorists have argued that the caller ID technology does not raise significant privacy concerns.^{xl} Justice Stewart's comments in his dissent in Smith v. Maryland (1979) express the contrary opinion: It simply is not enough to say, after Katz, that there is no legitimate expectation of privacy in the numbers dialed because the caller assumes the risk that the telephone company will disclose them...Most private telephone subscribers may have their own numbers listed in a publicly distributed directory, but I doubt that there are any who would be happy to have broadcast to the world a list of the local or long distance numbers they have called. This is not because such a list might in some sense be incriminating, but because it easily could reveal the identities of the persons and the places called, and thus reveal the most intimate details of a person's life.^{xli}

Privacy issues surrounding caller ID are magnified because the telephone companies offering the service are, in an almost Orwellian fashion, becoming increasingly powerful keepers and purveyors of information most of us consider private. Recent court decisions have cleared the way for the Baby Bells to enter the electronic information services business, using phone lines to provide news reports and stock quotes, as well as long-term storage of business and medical records.^{xlii} Now they have the power to package and publish electronic information for sale across business and home phone lines in ways we cannot control, to everyone from prospective employers to

telemarketers, making the phone companies ever more powerful as the scope of telecommunications grows.

Protecting individual privacy without losing the benefits of caller ID is a difficult challenge. On one hand, proponents of the technology argue it provides a valuable service to people pestered by obscene or harassing phone calls or persistent telemarketers, as well as to delivery services such as florists who need verification for orders or who are plagued by pranksters. The benefits are obvious: caller ID lets them know who is calling before they answer the phone. On the other hand, privacy advocates for callers vehemently disagree, maintaining that callers have privacy rights, too, and should be able to choose anonymity. They worry that the prospect of identification will deter anonymous police informants or callers to hot lines for drug abusers, people with AIDS, or runaways, for instance. They believe Caller ID can threaten the safety of those trying to find refuge from batterers or child abusers and will discourage doctors and other professionals from returning emergency calls from their homes, fearing release of their private numbers.

Opponents of caller ID believe few of us want our names and numbers automatically available for direct callbacks, and they know information about who calls a number can easily be used to compile and update telemarketing lists and data banks. They recognize that the cost of caller ID puts it beyond the reach of low-income customers, further aggravating inequalities of power. As Pennsylvania ACLU Executive Director Barry Steinhardt has argued, "Not only does the use of Caller ID go against public policy, but it is one more blatant example of how emerging technology is stripping away individual privacy rights layer by layer."^{xliii} Generally, when people see themselves as receivers of phone calls, they are eager for caller ID. But as callers, most want the power to block display of their numbers and names. Ironically, the privacy interests compete within the same people: those who both make and receive telephone calls.

The privacy problems of caller ID are amplified in part by a similar telephone service called ANI (automatic number identification) geared to businesses, including those with toll-free numbers. Like caller ID, ANI passes a telephone number along with each call, and then matches the number with a customer's corporate database in a personal computer, making it possible for a caller's file to be displayed before anyone answers the phone.^{xliv} Beginning with just a phone number, a whole host of information becomes common property.

Most caller ID systems automatically release the caller's phone number and name. To prevent this information from being divulged for a particular call, the caller must enter a code (typically *67) before dialing the number. In other words, callers must take an extra step each time they want to retain the privacy they had

previously taken for granted. This is called "per-call" blocking. Some phone systems allow "per-line" blocking: the caller's number is kept private by default and is released only when the caller enters an "unblocking" code for a single call. A serious difficulty is that for most caller ID systems, automatic supply of phone numbers is routine. Blocking, if available at all, is usually allowed only on a per-call basis. With these systems the burden for blocking is always on the caller. Callers must know that their numbers are being released, must learn how to block the release, and must remember to enter the special code every time they want to block automatic transmission of their names and numbers. Hence callers cannot avoid "assuming the risk" of privacy loss without careful self-discipline.

Bell Atlantic, among other providers, have been fighting all blocking on the grounds that it will devalue their service.^{xlv} In 1992, New England Telephone chose not to offer caller ID rather than be forced to provide a blocking option. Under pressure, New England Telephone reversed its policy, but at first offered per-call blocking as the only option. For other telephone companies as well, per-line blocking is either unavailable or must be specially requested by the customer.^{xlvi}

In a preposterous example of the profit motive at work, New York Telephone, in a full-page letter in The New York Times, defended caller ID with blocking on a single-call basis as a public service valuable for consumers, society, and the telephone companies.^{xlvii} It insisted that caller ID can help deter crime such as bomb threats and kidnapping, arguing that per-call blocking by code adequately protects the privacy of callers as well as those subscribing to the service. New York Telephone maintained, furthermore, that per-line blocking increases false alarms and compromises the effectiveness of emergency response agencies such as police, fire, and ambulance services by impeding quick determination of call sources. It claimed that children and others would either forget or not know how to disengage the blocking in an emergency.

This appeal to public policy is both self-serving and deceptive. The phone companies are well aware that the technology is available to override blocking for "911" calls and other emergency numbers. Moreover, with the responsibility on the caller to safeguard privacy on every call, privacy is lost by default. Experts say that so far, few people are blocking release of their numbers. That is no surprise. Even careful readers can overlook or misunderstand inserts in phone bills that describe blocking, and consequently much of the public is unaware of the option to block.

VI. Suggestions and Possible Solutions

A) Consider first massive databases and on-line dispersal of information. The move by Lotus and Equifax to recall software allowing access to files via personal computer is encouraging. Apparently concerned with its image, Equifax has also hired Professor Alan Westin, a philosopher and privacy expert from Columbia University, to review its privacy protections. Thus it is clear that public pressure can have an effect and must be continued.

In addition, we need better legislative controls over access to information. The European Union has proposed privacy guidelines to restrict carefully the collection and dissemination of personal data. These guidelines require companies to register all databases containing personal information, require that subjects be told and give consent for their personal data to be collected or used, and require that any information gained for one purpose not be used for any other purpose unless the individual consents after being given an opportunity to refuse to allow the information sharing. The guidelines also prevent transfer of information from one country to another unless the latter country also has adequate protection of records, and they do not allow collection of data on race, ethnic origin, political or religious affiliation, health status or sexual orientation.^{xlviii} Europeans are astounded there is no comparable protection or similar plan pending in the United States. Unfortunately American corporations, far from embracing these sound ideas, are fearful that the rules will hinder their routine use of computer data. However, many European countries are threatening to prohibit business transactions with American companies that cannot ensure similar protection. Consequently, the profit motive may actually boost privacy protection in this area.

We should note that this American fear of regulating data may be unwarranted. Some argue that Germany's experience with careful control of electronic databases undermines U.S. marketers' claims that strict privacy laws will place unacceptable burdens on businesses. Today Germany is cited as having Europe's most successful direct marketing industry, despite laws that forbid collecting personal information on anyone without prior notification and withholding that information if the individual wants to review it. The German system requires businesses of twenty or more employees to name an official to oversee gathering of personal data. There are state and federal data directors as well.^{xlix}

Sweden, which in 1973 was the first country to pass a national privacy law, provides a somewhat different example. It has a centralized government file with the information that marketers want, and the file is used by about 9 percent of Sweden's direct mail companies.¹ The worry with this centralization is that it places too much power in a single public agency. Advocates of the system reply that the constitutional right for any individual to see what is in the archives or files places a check on the government. Having access to information does not guarantee control

over the information, however, and it is not clear what procedures Sweden has for those who find erroneous information or want data eliminated from their file.

Another proposal worth considering is the formation of national privacy boards staffed with experts who have considered the issues from consumer, business, political, philosophical, and economic viewpoints. These boards could oversee regulations such as those suggested by the European Union. They might also implement and supervise additional protective measures, such as provision of free annual credit reports to consumers and regular mandatory updates, audits, and corrections in reports.

Note, however, the common theme in these different approaches by the European Union, Germany, Sweden, and others. Each echoes a dominant thesis of my book: the initial presumption must be that privacy protection is important and guidelines are essential. Moreover, each plan helps individuals retain control over information about themselves by providing knowledge about the data banks and access to the information, and by requiring permission and consent for collection or transfer of data.

B) For the second case, caller ID, it is unfortunate that most parties to the debate have taken extreme positions. They either recommend that the service be legally prohibited, revoked, or heavily regulated to protect privacy, or they defend caller ID as a service that should be available without limitations. It seems clear that like computer databases, the service must be regulated at the federal rather than local level, perhaps with worldwide guidelines to follow. This is necessary in part to coordinate the interstate calling patterns of consumers and businesses, as well as to harmonize the competing claims of individual privacy and commercial viability. Local or state regulations do not protect privacy uniformly, and will undoubtedly lead consumers to become frustrated or annoyed with a patchwork of different rules and options. Such frustration will only hinder the success of the technology. There is, moreover, a better alternative for satisfying both parties in the privacy debate over caller ID: namely to provide per-line blocking as the standard service, with a choice to revert to per-call blocking. This can be accomplished in a way that allows people dynamically to negotiate the degree of privacy they wish to sacrifice or maintain.^{li}

Consider how such a system would work with caller ID. Initially, all phone subscribers' lines would, by default, block the release of the caller's number. Subscribers could choose to release their number on a per-call basis by dialing an unblocking code (other than *67). Thus far, this is just per-line blocking. But phones with caller ID displays could also be set up automatically to refuse calls when the number has not been provided by the caller.

When an anonymous call is attempted, the phone does not ring. The thwarted caller hears a short recorded message explaining that to complete the call, the originating phone number must be furnished. This message then instructs the caller what code to dial to give out the number. Otherwise, the call is incomplete and the caller is not charged. Thus, a caller has the chance to decide whether a call is important enough that it is worth surrendering anonymity. This solution preserves choice and ensures privacy. Callers can control when to give out their numbers; call recipients can screen and refuse anonymous calls. The system remains voluntary. Through a dynamic and interactive process, both callers and call recipients are allowed to determine the extent to which their privacy is compromised.

Most callers, of course, will want to release their number when calling friends and associates. And if such calls dominate their use of the phone, they might choose to change the default on their line so that it automatically releases their number unless they dial in a blocking code. Thus, a dynamic negotiation system may well lead many people to change from per-line to per-call blocking-- precisely what the phone companies and the Federal Communications Commission favor. But when these customers change their default setting, they will know what they are choosing and why; they will be actively consenting to give out their numbers as a matter of course.

Some display units that can be purchased for use with caller ID are already able to reject anonymous calls, but they are a far cry from the dynamic negotiation system described. With these caller ID units, every call, whether accepted or not, is considered to have been answered and is charged to the caller. But a call that is rejected because of its anonymity should entail no charge. This requires that the call be intercepted by the phone company's central office switchboard before it reaches the recipient's line. The technology for implementing dynamic negotiation for caller ID is already available. The FCC need only amend its recent ruling and mandate per-line blocking as the default, requiring the necessary recordings and call interceptions described.

Although inspired by the debate over caller ID, the concept of dynamic negotiation of privacy can apply to other telecommunications technologies. One likely candidate is electronic mail. With traditional paper mail, people have always had the right, and the ability, to send anonymous correspondence. Delivery of the envelope requires neither that the letter be signed nor that a return address be provided. On the receiving end, people similarly have the right to discard anonymous mail unopened. Applying the principles of dynamic negotiation, senders of electronic mail would have the option to identify or not identify themselves. Recipients could reject as undeliverable any e-mail with an unidentified sender. The sender would then have the option to retransmit the

message, this time with a return address. As with caller ID, the users negotiate among themselves. The system itself remains privacy neutral.

The fundamental presumption is that privacy must be viewed as important from multiple perspectives; its protection should be assumed to be necessary at the outset, and technology should be so adapted that its use does not automatically require that one forfeit one's privacy. Several criteria guide the approach I have defended: (i) the need to protect individual privacy for all parties to a communication, (ii) the importance of letting new technologies flourish, and (iii) the need for national guidelines to provide consistency in system use and privacy protection where we now have a conglomeration of conflicting state guidelines. Since technological innovation proceeds rapidly, we must continually examine how best to make possible new features while preserving or enhancing our existing privacy.

The challenge is to protect privacy comprehensively, but not at the expense of technological services. For Caller ID as well as the European proposals for data bases, the key idea is to begin with maximal privacy protection, and then ensure that people are educated, consulted, and allowed to give consent or refusal before information is gathered or disseminated. They may then choose whether or not it is worthwhile for them to release personal database information or their phone numbers, etc. Consumers must demand that the government make it possible easily to protect the privacy of both the caller and the called, the e-mail sender and receiver. Individuals, not the telephone or communications companies, should determine the manner and extent to which the inevitability of new information technologies pervade our nation.

VII. Conclusion

In conclusion, I have focused on only two instances where information technology and privacy collide. Many other cases arise where there is a need to balance access to information and privacy. For example: Should doctors know when patients have AIDS or are HIV positive? Should patients be told the HIV status of doctors? Who, for what reasons, should be allowed access to the results of genetic testing? How much employment monitoring, through closed-circuit television, phone tapping, e-mail and computer files, is acceptable? Are tracking and surveillance systems for criminal suspects justified? Surely there are many others.

There are a number of moral issues that arise from conflicts between privacy and information technology. First, technological advances without restrictions often erase one's ability to maintain privacy and control

information about oneself. Second, competing claims between public access and individual privacy are sometimes compounded by concerns over the coercive power of the state. We want to live in an open and accountable society, yet we also want to preserve our right to be let alone. Third, one person's or one group's right to know often collides with another's right to keep information private. It is difficult to make broad generalizations about how to balance these interests. Individuals may make different choices based on their evaluation of the context of each case, and it is essential to involve them in the decisions wherever possible.

Legal issues are rapidly increasing in this area as well. In some cases, there are as yet no legal guidelines to help answer questions about how much is private, as with doctors who are HIV positive and want to withhold that information. In other cases, there is a patchwork of local regulations that conflict, as in different U.S. state laws concerning the telephone companies and caller ID. Finally, there are cases where national regulations and legislation have been proposed and passed, but where there are loopholes or escape clauses that vitiate the intended effects of the legislation, as is the case with U. S. statutes on databases and information storage.

There are many good reasons to keep public records open and accessible. It is important for society to monitor illegal activities, to capture criminals, and to preserve public safety. Oliver North's e-mail messages helped lead to major revelations in the Iran-Contra scandal, and organized crime leaders have been detected through phone taps and surveillance. Yet personal data can be collected and used to blackmail people, as was done by J. Edgar Hoover and the FBI in the 1960s and 1970s, ruining innocent lives.^{lii}

Clearly individual privacy must be balanced against other rights and values such as public safety. It is sometimes difficult to separate trivial irritations arising from privacy intrusions, such as extra junk mail, from more damaging privacy invasions. But it is also worth remembering that technology and privacy need not be incompatible and antagonistic. Airport X-ray machines can make hand searches of luggage less frequent. Magnetic markers in books and on merchandise make searches of briefcases and bags in libraries and stores largely unnecessary. Our goal should be to manage new technologies appropriately, not impede or destroy them.

My approach requires first that we specify which types of matters are private. Surely aspects of one's medical history may legitimately be viewed as private, in contrast to one's publicly listed telephone number. Second, we must maintain a presumption in favor of privacy and then develop criteria for deciding whether a violation of privacy is justified. Random drug testing for airline pilots may be a clear invasion of privacy, but it may be justified on the basis of public safety if there is strong evidence of drug abuse related to accidents and reasonable

likelihood the testing can alleviate the problem. In contrast, random testing of clerical workers is not legitimate when their work can be monitored in other ways without violating their privacy. In the case of address lists and phone numbers, local firehouses or ambulance services may need this information to respond immediately to emergencies and save lives. And financial institutions clearly have legitimate uses for credit histories in an era of economic stress and increased bankruptcies. But free-flowing information on interconnected public or private databases that can be sold without restrictions is not only highly questionable, but extremely intrusive.^{liii}

i. Joel Feinberg, Social Philosophy, (Englewood Cliffs, N.J.: Prentice-Hall, 1973), 64 - 67.

ii. Aristotle, The Politics, translated by Benjamin Jowett, in The Basic Works of Aristotle, ed. Richard McKeon (

iii. John Locke, The Second Treatise on Government, ed. Thomas P. Peardon, (New York: Macmillan, Library of

iv. Jean Bethke Elshtain, Public Man, Private Woman: Women in Social and Political Thought (Princeton: Prince

v. Alan Westin, "The Origins of Modern Claims to Privacy" in Ferdinand David Schoeman, ed., Philosophical D
(Cambridge: Cambridge University Press, 1984), 56-74.

vi. Ibid., p. 57. See also Peter H. Klopfer and Daniel I. Rubenstein, "The Concept Privacy and Its Biological Bas
Behavioral Phenomenon, 33, 3 (1977), 52-65.

vii. See Journal of Social Issues: Privacy as a Behavioral Phenomenon, 33, 3 (1977) for a wide range of essays es

Margaret Mead, Coming of Age in Samoa (New York: New American Library, 1949).

viii. Westin, "Origins of Modern Claims to Privacy," 59ff.

ix. Samuel Warren and Louis Brandeis, "The Right to Privacy," 4 Harvard Law Review 193 (1890), reprinted in Privacy, 75-103.

x. Winsmore v. Greenbank, Willes, 577 (1745).

xi. Thomas C. Cooley, Law of Torts, (1st ed. 1880, 2nd. ed. 1888).

xii. Warren and Brandeis, "The Right to Privacy," 215.

xiii. Ibid., 195.

xiv. Ibid., 213n.

xv. Roberson v. Rochester Folding Box Company, 171 N.Y. 538 (1902). The defendant had admittedly used lithography with the defendant's consent to advertise its flour. But the New York Court of Appeals refused to recognize legal protection of privacy.

xvi. In Pavesich v. New England Life Insurance Company, 122 Ga. 190 (1905), the Georgia Supreme Court declared the law.

xvii. William L. Prosser, "Privacy," 48 California Law Review 383 (1960), 389. Prosser's suggested additional tort of one in a false light is rarely invoked because of its overlap with defamation.

xviii. Griswold v. Connecticut, 381 U.S. 479 (1965). The Court stated that the physicians were being prosecuted and therefore had the legal standing to challenge, on behalf of married couples, the features of the law that made

xix. Eisenstadt v. Baird, 405 U.S. 438, 453 (1972).

xx. Roe v. Wade, 410 U.S. 113 (1973).

xxi. Moore v. City of East Cleveland, 431 U.S. 494 (1977).

xxii. Skinner v. Oklahoma, 316 U.S. 535 (1942).

xxiii. Stanley v. Georgia, 394 U.S. 557 (1969).

xxiv. Loving v. Virginia, 388 U.S. 1 (1967).

xxv. Pierce v. Society of Sisters, 268 U.S. 510 (1925).

xxvi. Rochin v. California, 342 U.S. 165 (1952).

xxvii. Whalen v. Roe, 429 U.S. 589, 599, 600 (1977).

xxviii. Judith Wagner DeCew, In Pursuit of Privacy: Law, Ethics, and the Rise of Technology (Ithaca: Cornell U
"Uncertain Protection of Privacy By the Supreme Court," 1979 Supreme Court Review, 173, 214 (1979).

xxix. This case is described in an op-ed piece: Judith Wagner DeCew, "Your Privacy Is Being Threatened," Phila
in The Atlanta Constitution, March 4 1991; the San Francisco Examiner, March 12 1991; and the Chicago Tribu

xxx. Jeffrey Rothfeder, "Is Nothing Private?," Business Week, September 4, 1989, 81.

xxxi. Ibid., 74.

xxxii. Ibid., 74.

xxxiii.Michele Galen, "The Right to Privacy: There's More Loophole Than Law," Business Week, September 4, 1991, 11.

xxxiv.Daniel Akst, "We Know Where You Live...," Boston Globe, October 16, 1995, 11.

xxxv.Michael W. Miller, "Equifax to Stop Selling Its Data to Junk Mailers," Wall Street Journal, August 9, 1991, 11.

xxxvi.Charles Piller, "Privacy in Peril," MacWorld, July 1993, 126.

xxxvii.Saul Hansell, "Keeping Identity Thieves at Bay," New York Times, June 16, 1996, sect. 4, 5.

xxxviii.Part of the following argument appeared in an op-ed piece: Judith Wagner DeCew, "Caller ID a Subtle Threat to Privacy," Washington Post, February 17, 1994, widely reprinted in newspapers under various titles.

xxxix.Richard Lacayo, "Now We've Really Got Your Number," Time, November 11, 1991, 40.

xl.Glenn Chatmas Smith, "We've Got Your Number! (Is it Constitutional to Give it Out?): Caller Identification Threatens Privacy," 37 U.C.L.A. Law Review 145 (1989); Arthur Miller, statement before the Subcommittee on Technology and Information of the U.S. Senate (August 1, 1990), reprinted in M. Ethan Katsh, ed., Taking Sides: Clashing Views on Controversial Issues (1993), 342-344. Miller supports caller ID, arguing that the caller's claim to privacy is weak or nonexistent, whereas the privacy of called parties who have "the superior privacy right" (343).

xli. Smith v. Maryland 442 U.S. 735, 747, 748 (1979). In this case the Court held that law enforcement officials register, a device that records numbers dialed from a telephone. The majority wrote, "All telephone users realize telephone company, since it is through telephone company switching equipment that their calls are completed. A company has facilities for making permanent records of the numbers they dial." (442 U.S. at 742, cited in Miller have anticipated and envisioned the further privacy problems of advanced telephone technology as described below

xlii. Richard Carelli, "Court Clears Baby Bells for Information Fields," Boston Globe, October 31, 1991, 53+. The broadcasting groups, the Supreme Court, without comment, rejected a request to bar the Baby Bell companies from

xliii. Barry Steinhardt is quoted in Charles Edward Anderson, "Night Callers Beware," ABA Journal 75 (May 1991)

xliv. Mary Lu Carnevale, "Caller ID Rings With New Controversies," Wall Street Journal, March 25, 1991, B1-E

xlv. Ibid.

xlvi. Ronald Rosenberg, "New Service for Phones Will Tell Who's Calling," Boston Globe, October 14, 1992, 1+

xlvii. Letter signed by Bailey Geeslin, New York Times, June 20, 1991, D23.

xlvi. John Markoff, "Europe's Plans to Protect Privacy Worry Business," New York Times, April 11, 1991, A1+ Privacy," Boston Globe, September 7, 1993, 10. An excellent summary of the European approach is supplied in Law and Restrictions on International Data Flows," 80 Iowa Law Review 471 (1995). On the domestic approach Regulating Privacy: Data Protection and Public Policy in Europe and the United States (Ithaca: Cornell University Press, 1996), Business Guide to Privacy and Data Protection Legislation (Dordrecht: Kluwer Law International, 1996), where national laws in Europe are summarized and explained, with relevant portions translated.

xlix. Larry Tye, "No Private Lives: German System Puts a Lid on Data," Boston Globe, September 7, 1993, 1+.

l. Ibid., 10.

li. The solution proposed first appeared in Ross E. Mitchell and Judith Wagner DeCew, "Dynamic Negotiation in the Age of Information Technology," Journal of Business Ethics 13 (1994), 70-71.

lii. Piller, "Privacy in Peril," 126.

liii. An early version of this paper was presented on November 11, 1993 at a conference on "Philosophy and Information Technology in the Age of Information Technology," organized by Jeroen van den Hoven, and was written with the support of research grants from the National Endowment for the Humanities at Clark University and the National Endowment for the Humanities. This version is drawn from my book The Rise of Technology (Ithaca: Cornell University Press, 1997).