The Death of Privacy?

A. Michael Froomkin

"You have zero privacy. Get over it."
--Sun Microsystems Inc. CEO Scott McNealy

Introduction

Information, as we all know, is power. Both collecting and collating personal information are means of acquiring power, usually at the expense of the data subject. Whether this is desirable depends on who the viewer and subject are—and who is weighing the balance. It has long been believed, for example, that the citizen’s ability to monitor the state tends to promote honest government, that “[s]unlight is . . . the best of disinfectants.” One need look no further than the First Amendment of the U.S. Constitution to be reminded that protecting the acquisition and dissemination of information is an essential means of empowering citizens in a democracy. Conversely, at least since George Orwell’s 1984, if not Bentham’s Panopticon, the image of the

1 Deborah Radcliff, A Cry for Privacy, COMPUTER WORLD, May 17, 1999 available in http://www.computerworld.com/home/print.nsf/all/990517privacy. The comment was in response to a question at a product launch. See also Edward C. Baig, Marcia Stepanek & Neil Gross, Privacy: The Internet Wants Your Personal Info., What’s in It for You?, BUS. WK, Apr. 5, 1999, at 84 (quoting McNealy as saying: “You already have zero privacy. Get over it.”).

2 LOUIS D. BRANDEIS, OTHER PEOPLE’S MONEY AND HOW THE BANKERS USE IT 92 (1914). Brandeis actually intended this comment to include both public and private institutions: “Publicity is justly commended as a remedy for social and industrial diseases. Sunlight is said to be the best of disinfectants; electric light the most efficient policeman.” Id.
all-seeing eye, the Argus state, has been synonymous with the power to exercise repression. Today, the all-seeing eye need not necessarily belong to the government, as many in the private sector find it valuable to conduct various forms of surveillance or to “mine” data collected by others. For example, employers continually seek new ways to monitor employees for efficiency and honesty; firms trawl databases for preference information in the search for new customers. Even an infrequently exercised capability to collect information confers power on the potential observer at the expense of the visible: knowing you may be being watched affects behavior. Modern social science confirms our intuition that people act differently when they know they are on Candid Camera--or Big Brother Cam.\(^3\)

In this article, I will use “informational privacy” as shorthand for the ability to control the acquisition or release of information about oneself.\(^4\) I will argue that both the state and the private sector now enjoy unprecedented abilities to collect personal data, and that technological developments suggest that costs of data collection and surveillance will decrease, while the quantity and quality of data increases. I will also argue that, when possible, the law should facilitate informational privacy because the most effective way of controlling information about oneself is not to share it in the first place.

Most of this article focuses on issues relating to data \textit{collection} and not data \textit{collation}. Much of the best work on privacy, and the most comprehensive legislation,\(^5\) while not ignoring


\(^4\) The definition differs from that used in U.S. constitutional law. The constitutional right to privacy is frequently described as having three components: (1) a right to be left alone; (2) a right to autonomous choice regarding intimate matters; and (3) a right to autonomous choice regarding other personal matters. Laurence H. Tribe, American Constitutional Law § 15-1 (2d ed. 1988); Ken Gormley, \textit{One Hundred Years of Privacy}, 1992 Wis. L. REV. 1335, 1340.

issues of data collection nonetheless focuses on issues relating to the storage and reuse of data. Privacy-enhancing legal and policy analysis often proceeds on the reasonable theory that because the most serious privacy-related consequences of data acquisition happen after the fact, and require a database, the use and abuse of databases is the appropriate focus for regulation. This article concentrates on the logically prior issue of data collection. A data subject has significantly less control over personal data once information is in a database. The easiest way to control databases, therefore, is to keep information to oneself: If information never gets collected in the first place, database issues need never arise. It may be that “[t]hree can keep a secret—if two of them are dead,” but in the world of the living we must find kinder, gentler solutions. Although privacy-enhancing technologies such as encryption provide a limited ability to protect some data and communications from prying eyes and ears, it seems obvious that total secrecy of this sort is rarely a practical possibility today unless one lives alone in a cabin in the woods. One must be photographed and fill out a questionnaire to get a driver's license, show ID to get a job. Our homes are permeable to sense-enhanced snooping, our medical and financial data is strewn around the datasphere, our communications are easily monitored, our lives are an open book to a mildly determined detective. Personal lives are becoming increasingly transparent to governments, interested corporations, and even to one another – as demonstrated by notorious incidents of phone eavesdropping or taping involving as diverse persons as Britain's Prince Charles, House Speaker Newt Gingrich, and White House Intern Monica Lewinsky. This general trend is driven by technological innovation and by economic and social forces creating a demand for privacy-destroying technologies. When solitude is not an option, personal data will be disclosed ‘voluntarily’ for transactions or emitted by means beyond our control. What remains

6 BENJAMIN FRANKLIN, POOR RICHARD’S ALMANAC (July 1735), reprinted in THE OXFORD DICTIONARY OF QUOTATIONS 211 (2nd ed. 1959).

Although the phenomenon of ad hoc surveillance and eavesdropping is an interesting one, this article concentrates on more organized corporate and government surveillance and especially profiling.
to be determined is which legal rules should govern the collection as well as the use of this information.

In light of the rapid growth of privacy-destroying technologies, it is increasingly unclear whether informational privacy can be protected at a bearable cost, or whether we are approaching an era of zero informational privacy, a world of what Roger Clarke calls “dataveillance.” Part I of this article describes a number of illustrative technological developments that facilitate the collection of personal data. Collectively these and others provide the means for the most overwhelming assault on informational privacy in the recorded history of humankind. That surveillance technologies threaten privacy may not be breaking news, but the extent to which these technologies will soon allow watchers to permeate modern life still has the power to shock. Nor is it news that the potential effect of citizen profiling is vastly increased by the power of information processing and linking of distributed databases. We are still in the early days of data mining, consumer profiling, and DNA databasing, to name only a few. The cumulative and accelerating effect of these developments, however, has the potential to transform modern life in all industrialized countries. Unless something happens to counter these developments, it seems likely that soon all but the most radical privacy freaks may live in the information equivalent of a goldfish bowl.

If the pace at which privacy-destroying technologies are being devised and deployed is accelerating, the basic phenomenon is nevertheless old enough to have spawned a number of laws and proposed legal or social solutions designed to protect or enhance privacy in various ways. Part II of this article examines several of these proposed privacy enhancing policies in light of the technologies discussed in Part I. It suggests that some will be ineffective, that others have undesirable or unconstitutional effects, and that even the best protect only a narrow range of privacy on their own.

---


10 So-called “reality” television programming provides a possible foretaste of this world. The popularity of these shows demonstrates the supply of willing watchers; there appear to be many willing subjects also. See, e.g., Associated Press, Actress bares All in Santiago Glass House, CNN, Jan. 26, 2000, available in http://cnn.com/2000/WORLD/americas/01/26/chile.glass.house.ap/ (describing actress “spending two
The relative weakness of current privacy-enhancing strategies sets the stage for the conclusion, which focuses on the latest entry to the privacy debate—the counsel of despair epitomized by Scott McNealy’s suggestion that the battle for privacy was lost almost before it was waged. Although there is a disturbingly strong case for this view, a case made trenchantly by David Brin’s *The Transparent Society,* I conclude by suggesting that all is not (yet) lost. While there may be no single tactic that suffices to preserve the status quo, much less claw back lost privacy, a smorgasbord of creative technical and legal approaches could make a meaningful stand against what otherwise seems inevitable.

A focus on informational privacy may seem somewhat crabbed and limited. Privacy, after all, encompasses much more than just control over a data trail, or even a set of data. It encompasses ideas of bodily and social autonomy, of self-determination, and of the ability to create zones of intimacy and inclusion that define and shape our relationships with each other. Control over personal information is a key aspect of some of these ideas of privacy, and is alien to none of them.

On the other hand, given that we live in an age of ubiquitous social security numbers, not to mention televised public talk-show confessionals and other forms of media-sanctioned exhibitionism and voyeurism, it may seem reactionary to worry about informational privacy. It

---


13 The phenomenon is everywhere, from the Starr Report to confessional talk shows, from mainstream films to the Internet’s 24x7 webcams. Cf. Herbert Marcuse, *One-Dimensional Man: Studies in the Ideology of Advanced Industrial Society* 74-81 (1964) (warning of “repressive desublimation” in which capitalism absorbs sexuality, strips it of threat and danger, drains it of its original meaning, repackages it as a commodity, then sells it back to the masses); see also Anita L. Allen, *Privacy And The Public Official: Talking About Sex as a Dilemma For Democracy,* 67 Geo. Wash. L. Rev. 1165 (1999) (noting that public servants now believe that “what takes place in private, unless dull and routine, is likely to become public knowledge anyway.”); Clay Calvert, *The Voyeurism Value in First Amendment Jurisprudence,* 17 Cardozo Arts & Ent. L.J. 273 (1999) (arguing for First Amendment right to “to peer and to gaze into places from which we are typically forbidden, and to facilitate our ability to see and to hear the
also may be that mass privacy is a recent invention, rarely experienced before the Nineteenth Century save in the hermitage or on the frontier. Perhaps privacy is a luxury good by world standards, and right-thinking people should concentrate their energies on more pressing matters, such as war, famine, or pestilence. And perhaps it really is better to be watched, with the benefits of mass surveillance and profiling outweighing the costs. Nevertheless, in this article I will assume that informational privacy is a good in itself, and a value worth protecting.


The extent to which modern ideas of privacy have historic roots is open to debate. While the distinction between the “private” home and the “public” outside is presumed to be ancient, see JURGEN HABERMAS, THE STRUCTURAL TRANSFORMATION OF THE PUBLIC SPHERE 4 (1962), it is clear the conception of the home has changed. Peter Ackroyd’s description of the home of Sir Thomas Moore, for example, with its numbers of servants, retainers, and even a fool, bears little relation to the home life of even the modern rich. See PETER ACKROYD, THE LIFE OF THOMAS MORE (1998). And, of course, one would not expect a concern with informational privacy in its modern form to predate the privacy-destroying technologies, mass data storage or modern data-processing to which it is a reaction.

This article thus does not consider suggestions arising from law and economics that privacy is best understood as a mere intermediate good. See Richard A. Posner, The Right of Privacy, 12 GA. L. REV. 393, 394 (1978); Richard A. Posner, Privacy, Secrecy, and Reputation, 28 BUFF. L. REV. 1 (1979). Treating privacy as an intermediate good, then-Professor Posner concluded that personal privacy is generally inefficient, since it allows persons to conceal disreputable facts about themselves and to shift costs of information acquisition (or the cost of failing to acquire information) to those who are not the least-cost avoiders. Data concealment by businesses is generally efficient, however, since allowing businesses to conceal trade secrets and other forms of intellectual property will tend to spur innovation. Id. Useful correctives to Posner’s views include KIM LANE SCHEPPELE, LEGAL SECRETS: EQUALITY AND EFFICIENCY IN THE COMMON LAW 43-53 & 111-126 (1988), James Boyle, A Theory of Law and Information: Copyright, Spleens, Blackmail, and Insider Trading, 80 CAL. L. REV. 1413 (1992), and Edward J. Bloustein, Privacy Is Dear at Any Price: A Response to Professor Posner’s Economic Theory, 12 GA. L. REV. 429 (1978).


“In a Wall Street Journal/NBC News poll last fall, Americans were given a list of eight concerns that might face them in the new century and were asked to rank the ones that worry them the most. Loss of personal privacy ranked at the top of the list, cited by 29%.” Glenn R. Simpson, E-Commerce Firms Start to Rethink Opposition to Privacy Regulation as Abuses, Anger Rise, WALL ST. J., Jan. 6, 2000, at. A24. Eighty percent of U.S. residents, sixty eight percent of Britons, and seventy nine percent of Germans polled agreed strongly or somewhat with the assertion that “consumers have lost all control over how personal information is collected and used by companies”; however fifty nine percent, sixty three percent and fifty five percent of Americans, Britons and Germans respectively also agreed that existing laws and organization
although not at all costs.\textsuperscript{17}

Privacy-destroying technologies can be divided into those which facilitate the acquisition of raw data and those which allow one to process and collate that data in interesting ways. Although both real and useful, the distinction can be overstated because improvements in information processing also make new forms of data collection possible. Cheap computation makes it easy to collect and process data on the keystrokes per minute of data entry clerks, secretaries, and even executives. It also makes it possible to monitor their web browsing habits.\textsuperscript{18} Cheap data storage and computation also makes it possible to mine the flood of new data, creating new information by the clever organization of existing data.

Another useful taxonomy would organize privacy-destroying technologies by their social context. One could focus on the fact about persons that makes them data subjects (e.g. citizen, employee, patient, driver, consumer). Or, one could focus instead on the different types of observers (e.g. - intelligence agencies, law enforcement, tax authorities, insurance companies, mall security, e-commerce sites, concerned parents, crazed fans, ex-husbands, nosy neighbors).

At the most basic level, initial observers can be broadly categorized as being either

\textsuperscript{17}Due to limitations of space- and of my knowledge-- this article also adopts an artificially U.S.-centric focus, although the problems discussed here are of global importance.

\textsuperscript{18}Employers’ concern about “cyberslackers” is fanned by consultants’ reports that “employees who surf the Web from their office PCs are costing Corporate America more than $1 billion a year.” Michele Masterson, \textit{Cyberveillance at Work: Surfing the Wrong Internet Sites on the Job Could Get You Fired}, CNN, Jan. 04, 2000, available in http://www.cnnfn.com/2000/01/04/technology/webspy/. Cf. Eugene Volokh, \textit{Freedom Of Speech, Cyberspace, Harassment Law, And The Clinton Administration} (forthcoming LAW & CONTEMP. PROBS. 2000) (arguing that sexual hostile environment harassment law is now so pervasive and potentially hair-trigger that prudent employer must carefully monitor workplace, including Internet use, for employee access of sexually themed materials).
governmental or private, although here too the importance of the distinction can be overstated because private parties often have access to government databases, and governments frequently purchase privately collected data. There are some types of data collection that only the government can undertake, for example, the capture of information on legally mandated forms such as the census, driver's licenses, or tax returns. But even these illustrate the danger of being too categorical: some states make driver's license data and even photographs available for sale or search, and many tax returns are filed by commercial preparers (or web-based forms), giving a third party access to the data.

Databases multiply the effects of sensors. For example, camera data has far less effect on privacy if its only use is to be monitored in real time by camera operators watching for commission of crimes. The longer the tapes are archived, the greater their potential effect. And, the more that the tapes can be indexed according to who and what they show rather than just where and when they were made, the more easily the images on those tapes can searched or integrated into personal profiles. Equally importantly, databases make it possible to create new information by combining existing data in new and interesting ways. Once created or collected, data is easily shared and hard to eradicate; the data genie does not go willingly--if ever--back into the bottle.

Realms of data organized into either centralized or distributed databases can have substantial consequences beyond the simple loss of privacy caused by the initial data collection, especially when subject to advanced correlative techniques such as data mining.19 Among the

19 See Ann Cavoukian, Ontario Info. & Privacy Comm's Data Mining: Staking a Claim on Your Privacy (1985), available in http://www.ipc.on.ca/web_site.eng/matters/sum_pap/PAPERS/datamine.htm:

Data mining is a set of automated techniques used to extract buried or previously unknown pieces of information from large databases. Successful data mining makes it possible to unearth patterns and relationships, and then use this “new” information to make proactive knowledge-driven business decisions. Data mining then, “centres on the automated discovery of new facts and relationships in data. The raw material is the business data, and the data mining algorithm is the excavator, sifting through the vast quantities of raw data looking for the valuable nuggets of business information.”

Data mining is usually used for four main purposes: (1) to improve customer acquisition and retention; (2) to reduce fraud; (3) to identify internal inefficiencies and then revamp operations; and (4) to map the unexplored terrain of the Internet. The primary types of tools used in data mining are: neural networks, decision trees, rule induction, and data
possible harmful effects are various forms of discrimination, ranging from price discrimination to more invidious sorts of discrimination. Data accumulation enables the construction of personal data profiles. When the data are available to others, they can construct personal profiles for targeted marketing, and even, in rare cases, blackmail. For some, just knowing that their

visualization.

_Id._ (footnotes omitted) (quoting JOSEPH P. BIGUS, _DATA MINING WITH NEURAL NETWORKS_ 9 (1996)).


See Kang, _Supra_ note 16, at 1239.

You can buy lists of people who have bought skimpy swimwear; college students sorted by major, class year, and tuition payment; millionaires and their neighbors; people who have lost loved ones; men who have bought fashion underwear; women who have bought wigs; callers to a 900-number national dating service; rocket scientists; children who have subscribed to magazines or have sent in rebate forms included with toys; people who have had their urine tested; medical malpractice plaintiffs; workers’ compensation claimants; people who have been arrested; impotent middle-aged men; epileptics; people with bladder-control problems; buyers of hair removal products or tooth whiteners; people with bleeding gums; high-risk gamblers; people who have been rejected for bank cards; and tenants who have sued landlords. There are lists based on ethnicity, political opinions, and sexual orientation.

Jeff Sovern, _Opting In, Opting Out, or No Options at All: The Fight For Control of Personal Information_, 74 WASH. L. REV. 1033, 1033-34 (1999).


Go to a part of town where your kind isn’t thought to belong and you’ll end up on a list somewhere. Attend a political meeting and end up on another list. Walk into a ritzy boutique and the clerk will have your credit report and purchase history before even saying hello. . . . The whole culture will undergo convulsions as taken-for-granted assumptions about the construction of personal identity in public places suddenly become radically false. . . .

And that’s just the start. Wait a little while, and a market will arise in “spottings”: if I want to know where you’ve been, I’ll have my laptop put out a call on the Internet to find out who has spotted you. Spottings will be bought and sold in automated auctions, so that I can build the kind of spotting history I need for the lowest cost. Entrepreneurs will purchase spottings in bulk to synthesize spotting histories for paying customers. Your
activities are being recorded may have a chilling effect on conduct, speech, and reading. Customers may find it discomfiting to discover that a salesperson knows their income or indebtedness, or other personal data.

When the government has access to the data, it not only gains powerful investigative tools allowing it to plot the movements, actions and financial activities of suspects, but new techniques for detecting crimes and identifying suspects. Ultimately, if data is collected on everyone’s location and on all transactions, it should be possible to achieve perfect law enforcement; a world in which no transgression goes undetected and, perhaps, unpunished. At daily routine will be known to anyone who wants to pay five bucks for it, and your movement history will determine your fate just as much as your credit history does now... Then things will really get bad. Personal movement records will be subpoenaed, irregularly at first, just when someone has been kidnapped, but then routinely, as every divorce lawyer in the country reasons that subpoenas are cheap and not filing them is basically malpractice. Then, just as we’re starting to get used to this, a couple of people will get killed by a nut who been predicting their movements using commercially available movement patterns.

Id.

Data mining can be used to generate lists of political preferences. Senator John McCain and Texas Governor George W. Bush each contracted with Aristotle Publishing, a firm that offered to target web users by matching web browsing habits and web site signup data with voter registration records. Lauren Weinstein, Web Tracking and Data Matching Hit The Campaign Trail, PRIVACY FORUM DIGEST (08:22), Dec. 23, 1999, available in http://www.vortex.com/privacy/priv.08.22

Of course, disclosure also helps prevent evils which can hide behind the veil of anonymity. See A. Michael Froomkin, Flood Control on the Information Ocean: Living with Anonymity, Digital Cash, and Distributed Databases, 15 J.L. & COM. 395, *** (1996).


See FinCEN, Helping Investigators Use the Money Trail, available in http://www.treas.gov/fincen/follow2.html; see also FinCEN, supra note 26, at 5 (stating that analysts may provide information through FinCEN’s Artificial Intelligence System on previously undetected possible criminal organizations and activities so that investigations can be initiated).

that point, the assumptions of imperfect detection, the need for deterrence, and the reliance on police and prosecutorial discretion on which our legal system is based will come under severe strain.

A further danger is that the government or others will attempt to use the ability to construct personal profiles to attempt to predict dangerousness or antisocial activities before they happen. People whose profile meets the criteria will be flagged as dangerous and perhaps subjected to increased surveillance, searches, or discrimination. Profiling is currently used to identify airline passengers whom the profilers think present an above-average risk of being terrorists. In the wake of the tragedy at Colombine, schools are turning to profiling to assess school children for potential violence. In a world where such profiling is common, who will dare to act in a way that causes red flags to fly?

In a thorough survey, Roger Clarke suggested that the collection and collation of large [data mining] technology . . . being developed for the I.R.S. . . . will be able to feed data from every entry on every tax return, personal or corporate, through filters to identify patterns of taxpayer conduct. Those taxpayers whose returns suggest . . . that they are highly likely to owe more taxes could then quickly be sorted out and their tax returns audited."


amounts of personal data creates many dangers at both the individual and societal levels, including:

- **Dangers of Personal Dataveillance**
  - lack of subject knowledge of data flows
  - blacklisting

- **Dangers of Mass Dataveillance**
  - To the Individual
    - witch hunts
    - ex-ante discrimination and guilt prediction
    - selective advertising
    - inversion of the onus of proof
    - covert operations
    - unknown accusations and accusers
    - denial of due process
  - To Society
    - prevailing climate of suspicion
    - adversarial relationships
    - focus of law enforcement on easily detectable and provable offences
    - inequitable application of the law
    - stultification of originality
    - increased tendency to opt out of the official level of society
    - weakening of society’s moral fibre and cohesion
    - repressive potential for a totalitarian government

There is little reason to believe that the fundamental propensity for nosiness of neighbors, employers, or governments has changed recently. What is changing, very rapidly, is the cost and variety of tools available to acquire personal data. The law has done such a poor job of keeping pace with these developments that some people have begun to suggest privacy is becoming impossible.

---

31 Clarke, *supra* note 9.
Large quantities of personal data are routinely collected in the U.S. today without the involvement of any high-tech equipment. Examples include the collection of personal data by the Federal Government for taxes and the census, data collected by states as a condition of issuing driver’s licenses, and the vast amounts of data collected by the private sector in the course of selling products and services.

By the United States Government.

The most comprehensive, legally mandated, U.S. Government data collections are the annual collection of personal and corporate tax data, and the decennial census. Both of these data collection activities are protected by unusually strict laws designed to prevent the release of personally identifiable data. Other government data collection at the federal and state level is either formally optional, or aimed at subsets of the population. Some of these subsets, however, are very large.

Anyone who takes a new job must be listed in the “new hires directory” designed to

---

32 See 13 U.S.C.A. §§ 8-9 (West Supp. 1999) (census); 26 U.S.C.A. § 6103 (West Supp. 1999) (tax return data). Despite these rules, however, there have been suggestions that because census information is detailed, it could be cross-indexed with other data to pinpoint individuals. For example, if one knows that there is only one person in a particular age group, of a particular ethnicity, or with some other distinguishing characteristic within the census tract, and one can extract the “aggregate” data for all individuals with the characteristic in the area, one has individualized data. Cf. Robert G. Schwartz, Jr., Privacy In German Employment Law, 15 Hastings Int'l & Comp. L. Rev. 135, 146 (1992) (describing 1983 decision of German Federal Constitutional court striking down census questions that it believed would allow identification of respondents).

support the Federal Parent Locator Service.\textsuperscript{34} This growing national database of workers exists to enable courts to enforce court-ordered child support against working parents who are not making their support payments. Each state has its own database, which is coordinated by the Office of Child Support Enforcement within Health and Human Services.\textsuperscript{35} Anyone on public assistance is likely to be in state maintained database of aid recipients. Federal, state and local governments also collect data from a total of about fifteen million arrestees each year.\textsuperscript{36} The government continues to collect (and publish) data about some convicts even after they served their sentence.\textsuperscript{37}

Formally optional data collection with wide application includes license applications—licenses are optional, although the questions are mandatory if one wants the license. Perhaps the most widespread data collection comes from driver’s license applications, as most of the U.S. adult population holds a driver’s licenses, at least outside a few major cities with efficient mass transportation networks. In addition to requesting personal data such as address, telephone number, and basic vital statistics, some states collect health-related information, and all require a (frequently digitized) photograph.

Any personal transaction involving money, be it working, buying, selling, or investing, tends to create a data set relating to the transaction. Unless the payment is in cash, the data set usually includes some personal data about the individual(s) in the transaction.

\begin{itemize}
\item \textsuperscript{34}42 U.S.C. § 653 (1996).
\item \textsuperscript{35}See Department of Health and Human Services, What is NECSRS?, available in http://oese.acf.dhhs.gov/necsrspub/Navigation/Questions/Ques.htm#NECSRS1 (stating “National Electronic Child Support Resource System . . . is used to identify and electronically index Federal, State, and local resource materials.”).
\end{itemize}
Financial data collection is an interesting example of the private sector collecting data from mixed motives. A single firm, Acxiom, now holds personal and financial information about almost every U.S., U.K., and Australian consumer. In many cases, banks and other financial service providers collect information about their clients because the data have commercial value. In other cases, they record data because the government requires them to make routine reports to assist law enforcement objectives. In effect, private banks often act as agents of state data collection efforts.

Until machines for tracking bills by their serial numbers are much more common than today, cash payment remains relatively anonymous. In their quest to capture personal data about customers, merchants have turned to loyalty reward programs, such as frequent shopper cards and grocery club cards. Depending on the sophistication of the card, and of the system of which it is a part, these loyalty programs can allow merchants to amass detailed information about their customers.

Large amounts of cash trigger reporting requirements, which in turn mean that financial intermediaries must collect personal data from their customers. Anti-money laundering laws (and, sometimes, tax laws) require financial service providers to file reports on every suspicious transaction and every time a client deposits, withdraws, or transfers $10,000 or more. Some firms, often chosen on the basis of location in neighborhoods thought by law enforcement to be high drug trading zones, must report transactions involving as little as $750 in cash.

Alternatives to cash, such as checks, debit cards, and credit cards, each create a data trail that identifies the purchaser, the merchant, the amount of the sale and, sometimes, the goods or services sold.

Whether replacing paper cash with electronic cash would make transactions more securely anonymous or create a digital data trail linking every transaction to the parties involved depends entirely on how the electronic cash system is designed. Both extremes are possible, as

---


are intermediate designs in which, for example, the identity of the payer is not recorded (or even identifiable), but the payee is known to the bank that issued the electronic cash.\textsuperscript{40} As there is currently no standard for electronic cash and relatively little e-cash in circulation; anything remains possible.

Large quantities of medical data are generated from any sustained interaction with the United States health care system. In addition to being shared between the various persons involved in providing the care, the information is shared with the various entities that administer the care.\textsuperscript{41} Under the “Administrative Simplification” provision of the Health Insurance Portability and Accountability Act of 1996 (HIPAA),\textsuperscript{42} standards are being developed to facilitate the electronic transfer of health-related personal data. HIPPA requires that all health information be kept in electronic form and that each individual be given a unique health identifier to index the data.

Thus, even without high technology, substantial amounts of personal data are routinely

\textsuperscript{40} See Froomkin, \textit{supra} note 25, at 449-79.


collected about almost everyone in the country. The introduction of new technologies, however, promises to raise the quantity and nature of the information that could be collected about people to new, somewhat dizzying, heights.

=S2B. Ubiquitous Surveillance@

Unless something social, legal, or technical intervenes, it is now possible that there will be no place on earth where an ordinary person will be able to be certain to avoid surveillance. In this possible future, already discernable from the present, public places will be watched by terrestrial cameras and even by satellites. Facial and voice recognition software, cell phone position monitoring, smart transport, and other science-fiction-like developments will together provide full and perhaps real time information on everyone’s location. Homes and bodies will be permeable to sense-enhanced viewing. All communications, save perhaps some encrypted messages, will be scannable and sortable. Copyright protection “snitchware”\(^\text{43}\) and Internet-based user tracking will generate full dossiers of reading and shopping habits. The move to web-based commerce, combined with the fight against money laundering and tax evasion, will make it possible to assemble a complete economic profile of every consumer. All documents, whether electronic, photocopied, or (perhaps) even privately printed will have invisible markings making it possible to trace the author. Workplaces will not only be on camera, anything involving computer use will be subject to detailed monitoring, analyzed for both efficiency and inappropriate uses. As the cost of storage continues to drop, enormous databases will be created, or disparate distributed databases linked, allowing all these data to be cross-referenced in increasingly sophisticated ways.

In this very possible future, indeed perhaps in our present,\(^\text{44}\) there may be nowhere to hide and little that can stay hidden.

\(^{43}\) See infra at text & note 109.

\(^{44}\) Cf. Tina Kelley, An Expert in Computer Security Finds His Life Is a Wide-Open Book, N.Y. TIMES, (Dec. 13, 1999, at C4 (describing how a group of “security experts” were able to dig up vast amounts of information on a self-described “average citizen”).
Moving about in public is not truly anonymous: someone you know can always recognize you; anyone can write down the license plate number of your car. Nevertheless, at least in large cities, one enjoys the illusion, and to a large extent the reality, of being able to move about without anyone knowing one's whereabouts. That freedom is soon to be a thing of the past, as the “privacy commons” of public spaces becomes subject to the enclosure of privacy-destroying technology.

Fear of crime, and the rapidly declining cost of hardware, bandwidth, and storage, are combining to foster the rapid spread of technologies for routinely monitoring public spaces and identifying all who show themselves there. Monitoring technologies include cameras, facial recognition software, and various types of vehicle identification systems. Related technologies some of which have the effect of allowing real-time monitoring and tracking of individuals include cell-phone location technology, and various types of biometric identifiers.

Perhaps the most visible way in which public spaces are monitored is the increasingly ubiquitous deployment of Closed Circuit Television (CCTV) cameras and video recorders. Monitoring is a mix of public and private. Generally, private spaces such as shopping malls are monitored by private security, while public spaces are monitored by law enforcement. Although public cameras are common in the U.S., they are in even more widespread use abroad. Perhaps because of fears of IRA terrorism as well as ordinary concerns about crime, the United Kingdom has pursued a particularly aggressive program of blanketing the nation with cameras. Cameras operated by law enforcement “are now a common feature of Britain’s urban landscape. . . . The cameras have also moved beyond the city, into villages, schools, hospitals and even, in

45 See, e.g., Timothy Egan, Police Surveillance of Streets Turns to Video Cameras and Listening Devices, N.Y. TIMES, Feb. 7, 1996, at A2 detailing the methods and equipment of several cities’ police departments).
Bournemouth, covering a coastal path.” Cameras are also commonly used on the roads to enforce speed limits by taking photos of every speeding vehicle’s license plate. Polls suggest that a substantial majority of the British public approves of the cameras because they make them feel safer. And indeed, the evidence suggests that cameras reduce, or at least displace, street crime and perhaps other anti-social behaviors.

Cameras can also be placed in the office, in the school, and in the home. Visible cameras allow parents to check in on junior at day care. Hidden cameras can be concealed in “clocks, radios, speakers, phones, and many other items” to monitor caregivers and others in the home.

Cameras are also an example of how one technology can interact with another to multiply their privacy-destroying effects. All the videotapes in the world are of little use unless there is someone to monitor them, a useful way to index the contents, or a mechanical aid to scan through them. And pictures alone are only useful if there is a means of identifying the people on them. Thus, for example, the London Police captured excellent quality photos of alleged participants in a violent demonstration in the City of London on June 18, 1998, but had to post them on the Internet to ask viewers for help in identifying them—and it worked in some cases.

Human monitors are expensive and far from omniscient. In the near future, however, human observers will become much less important as the task of identifying people on still photos and videos will be mechanized. In some cases, such as schools, offices, or prisons, data subjects can be compelled to wear IDs with bar codes. In public, however, more elaborate

47 See id. at ¶¶ 12-14.
49 See City of London Police, Current Advise, June 18, 1999, available in http://www.cityoflondon.gov.uk/citypolice/j18frame.htm; City of London Police, Identity Parade, June 18, 1999, available in http://www.cityoflondon.gov.uk/citypolice/idparade8.htm (asking viewers to help “identify any of these people photographed during the June 18 incident in the City of London”; as of December 21, 1999, some photos were missing, labeled “now identified”).
50 They may also be racist. See Taylor, supra note 46, at ¶¶ 26-27.
51 See, e.g., Teacher Fired for Not Making Kids Wear IDs, CHARLESTON GAZETTE & DAILY MAIL, Feb. 5, 1999 available in 1999 WL 6710744 (stating that teacher objected to bar code because
effort, such as facial recognition technology, is needed to identify people. Facial recognition technology is becoming better and more reliable every year. Systems are already capable of picking out all the people present in two different pictures, allowing police to identify repeat demonstrators even in large crowds assembled many weeks apart. The London police installed a system called “Mandrake” that matches CCTV photos taken from 144 cameras in shopping centers, parking lots, and railway stations against mug shots of known criminals. (For some reason, the police chose to test the system in the poorest part of London.) The Israeli government plans to use facial recognition technology in the hopes of creating “Basel,” an automated border-crossing system. The U.S. Pentagon is also investigating the utility of facial recognition systems in the hopes of identifying potential terrorists outside military facilities.

Once mated with, say, a database full of drivers license photos, images from a series of ubiquitous cameras could be indexed by name and stored for an indefinite period of time. (Indeed, the U.S. Secret Service and other agencies have expressed interest in a national database of drivers licence photos, and the government has spent at least $1.5 million helping a private corporation amass the data.) Assuming the index and the videos are at least subject to subpoena, not to mention FOIA-able or just routinely placed on the Internet, alibis, mystery

---


54 See Taylor, supra note 46.


novels, and divorce proceedings will never be the same. Even if this prediction proves false, one’s face will become an index marker. It will be possible to carry a device that warns you every time anyone convicted of rape or child molestation comes within 100 feet. Stores will be able to send coupons to window shoppers who browsed but did not enter (“Hi! Next time, wouldn’t you like to see what we have inside?”). Worse, once you enter, the store will be able to determine which merchandise to show you and how much to charge.  

=S4b. Cell phone monitoring.@

Many people can be tracked today without anyone having to deploy cameras or any other device. Cellular phones must communicate their location to a base station in order to carry or receive calls. Therefore, whenever a cell phone is in use, or set to receive calls, it effectively identifies the location of the user every few minutes to an area defined by the tolerance of the telephone. Recently, Maryland and Virginia officials unveiled a plan to use mobile phone tracking information to monitor traffic flows, although their plan does not involve capturing the identities of individual commuters, only their movements.  

The finer the cell phone zone, the more exactly a person’s location can be identified. In the U.S., an FCC regulation due to become effective in 2001 requires all U.S. cellular carriers to ensure that their telephones and networks will be able to pinpoint a caller’s location to within 400 feet, about half a block, at least sixty-seven percent of the time. The original objective of the

*in* [http://www.cnn.com/US/9902/18/license.photos/].


59 Alan Sipress, *Tracking Traffic by Cell Phone: Md., Va to use Transmission to Pinpoint Congestion*, WASH. POST, Dec. 21, 1999, at A1 (stating that Maryland and Virginia will track “anonymous” callers on highways to measure speed of traffic).

60 Compatibility of Wireless Services with Enhanced 911, 61 Fed. Reg. 40,348, 40,349(1996)(codified at 47 C.F.R. pt. 20). The FCC’s approach differs from that adopted by some telephone manufacturers who have designed their phones with Global Positioning Satellite (GPS) receivers. These receivers display the phone’s precise latitude, longitude, and elevation, which the user can then relay to the 911 operator—but only if the user is able to talk. See Steve Ginsberg, *Cell Phones Get a Homing Device*, S.F. BUSINESS TIMES, Sept. 28, 1998, *available in*
rule was is to allow calls to 911 to be traced, but the side-effect will be to turn cell phones into efficient tracking devices. Indeed, in a recent order the FCC confirmed that wireline, cellular, and broadband Personal Communications Services (PCS) carriers would be required to disclose to law enforcement agents with wiretap authorization the location of a cell site at the beginning and termination of a mobile call. This was less than the FBI, the Justice Department, and the New York Police Department wanted; they had argued they should be entitled to all location information available to the carrier.

Governments are not the only ones who want to know where people are. Parents could use cell phone tracking to find out where their children are (or where they left the phone). Merchants are also interested in knowing who is in the neighborhood. A U.K. cell phone company is sending “electronic vouchers” to its six million subscribers, informing them of “special offers” from pubs in the area from which they are calling and helpfully supplying the nearby address.

The privacy-destroying consequences of cell phone tracking increase dramatically when the movement data are archived. It is one thing to have police using the data to track someone in real time who is the subject of an arrest warrant or is a suspect in a murder. It is another thing to keep the data around, perhaps even in perpetuity, in case police or others wish to reconstruct someone’s movements later. In 1997, a Swiss newspaper revealed that a local phone company kept information on the movement of one million subscribers, accurate to with a few hundred meters, and that the data was stored for more than six months. Swiss police described the data as a treasure trove. However atypical the collection and retention of cellular phone subscriber movements may be, the Swiss phone company’s actions are clearly not unique. The Swiss


64 See, e.g., Nicole Krau, Now Hear This: Your Every Move is Being Tracked, HA’ARETZ, Mar. 10, 1999, available in 1999 WL 17467375 (stating that Israeli cellular phone records are stored by cellular phone companies and sold to employers who wish to track employees, as well as provided to government when ordered by court); see also Richard B. Schmitt, Cell-Phone
government, at least, so values this locational data that it will go to great lengths to preserve its access to it. Reports in 1998 suggested that the Swiss police felt threatened by the ability of Swiss cell phone users to buy prepaid phone cards which would allow certain types of “easy” telephones to be used anonymously. The Swiss government therefore proposed that citizens be required to register when acquiring “easy” cell phones, arguing that being able to identify who is using a cell phone was “essential” to national security.65

=S4c. Vehicle monitoring.@

Cars are a separate potential target of blanket surveillance. So-called “intelligent transportation systems” (ITS) are being introduced in many urban areas to manage traffic flow, prevent speeding, and in some cases implement road pricing or centralized traffic control.66 Ultimately, ITS promise continuous, real-time information as to the location of all vehicles in motion.67 Less complex systems already create travel records that can stored and accessed later.68 Some countries have also considered putting bar codes on license plates to make it easier to identify vehicles.69 While it is possible to design ITS in a manner that preserves the traveler’s anonymity,70 this has not been the norm.

_Hazard: Little Privacy in Billing Records, WALL ST. J., Mar. 16, 1999_ (stating that AT&T wireless unit fields roughly 15,000 subpoenas for phone records per year).


68 _Id. at 164-65.


70 _See, e.g.,_ ONTARIO INF. AND PRIVACY COMM’R, 407 EXPRESS TOLL ROUTE: HOW YOU CAN TRAVEL THIS ROAD ANONYMOUSLY (1998), available in [http://www.ipc.on.ca/web_site.eng/matters/sum_pap/PAPERS/407.htm](http://www.ipc.on.ca/web_site.eng/matters/sum_pap/PAPERS/407.htm) (“A significant amount of work was required to ensure that the 407 ETR toll and billing system did not compromise personal privacy.”).
Monitoring in the home and office.

Staying home may be no defense against monitoring and profiling. The technology exists today to monitor every electronic communication, be it a telephone call, a fax, or an e-mail. In the U.S., at least, its use by either the government or private snoops is subject to substantial legal restrictions. As voiceprint, voice recognition, and content-analysis technology continue to improve, the tasks of sorting the wheat from the chaff amongst the ever-increasing volume of communications will be subjected to increasingly sophisticated automated processing. Meanwhile, a number of legal technologies are already being deployed to track and archive many uses of the web.

Workplace surveillance.

Outside of restrooms, and of the few laws banning wiretapping and reading e-mail while in transit, there are relatively few privacy protections applicable to every workplace in the nation. Thus, employers may use hidden cameras, monitoring software, and other forms of surveillance more or less at will. A 1993 survey, taken long before surveillance technology got cheap, showed that twenty million workers were subject to monitoring of their computer files,

---


73 See generally Robert G. Boehmer, Artificial Monitoring and Surveillance of Employees: the Fine Line Dividing the Prudently Managed Enterprise from the Modern Sweatshop, 41 DEPAUL L. REV. 739, 739 (1992) (“Except for outrageous conduct and the use of one of a discrete group of techniques that Congress has chosen to regulate, the law supplies employees with precious little protection from the assault on workplace privacy. Similarly, the law provides employers with little guidance concerning the permissible depth of their intrusions.”).

voice and electronic mail and other networking communications. At these prices and sizes, ubiquitous and hidden monitoring is easily affordable. Software designed to capture keystrokes, either overtly or surreptitiously, is also readily available. For example, a program called “Investigator 2.0” costs under $100 and, once installed on the target PC, covertly monitors everything that happens on it and routinely e-mails detailed reports to the boss.

In addition, every technology described below which can be targeted at the home can also be targeted at the office.

According to a report prepared for the European Parliament, the U.S. and its allies maintain a massive worldwide spying apparatus capable of capturing all forms of electronic communications. Known as “Echelon,” the network can “access, intercept and process every important modern form of communications, with few exceptions.” The network is supported by a variety of processing technologies. Voiceprint recognition makes it possible to determine whether any of the participants in a call are on a watch list. If they are, the recording can be routed to a human being for review. Similarly, text messages such as faxes and e-mails can be

---


79 Id. at Technical Annexe § 2.

80 “Contrary to reports in the press, effective ‘word spotting’ search systems automatically to select telephone calls of intelligence interest are not yet available, despite 30 years of research. However, speaker recognition systems—in effect, ‘voiceprints’—have been developed and are
run through so-called dictionary programs which flag messages with interesting references or word patterns. As artificial intelligence improves, these programs should become increasingly sophisticated. Meanwhile, advances in voice recognition (speech to text) promise to transform the telephone monitoring problem into another type of text problem. Further, once the conversation is converted into text, the National Security Agency (NSA) is ready to gauge its importance with semantic forests: The NSA recently received a patent on a computerized means to produce a topical summary of a conversation using a “tree-word-list” to score the text. The patent describes a “pre-processing” phase that will remove “stutter phrases” from a transcript. Then, a computer automatically assigns a label, or topic description, to the text. The method promises to allow computerized sorting and retrieval of transcripts and other documents based on their meaning, not just on keywords.

Not only have the communications intelligence agencies of the U.S. and its major allies “reaffirmed their requirements for access to all the world’s communications,” they have also taken a number of steps in the past two years to ensure they can get it. The NSA installed “sniffer” software to collect traffic at nine major Internet exchange points. On May 7, 1999, the European Parliament passed the Lawful Interception of Communications resolution on new technologies, known as Enfopol. Although the Enfopol resolution is nonbinding, it serves as a declaration of the regulatory agenda of the European law enforcement community. Under the Enfopol proposal, Internet service providers and telephone companies in Europe would be required to provide law enforcement agencies with full-time, real-time access to all Internet transmissions. In addition, wireless communications providers would be required to provide geographical location information on cell phone users. If encryption is provided as part of the cell phone service, the service provider would be required to ensure that it be able to decode the

---

81 “Dictionary computer”--GCHQ monitors all telexes for key words. Id. § 3 ¶ 72.


84 STOA REPORT, supra note 78, ¶ 6.

85 Id. § 2, ¶ 60.
Similarly, in the U.S., the Communications Assistance for Law Enforcement Act of 1994 (CALEA) requires that all new telecommunications networks be engineered to allow lawful wiretaps, although it does not address the issue of encryption. The legislation does not specify how many simultaneous wiretaps the network should be able to handle, leaving this to the implementing regulations. In its initial estimate of its “capacity requirements,” the FBI proposed requiring carriers in major urban areas to install a maximum surveillance capacity of one percent of “engineered capacity,” that is, to make it possible for a maximum of one out of every hundred phone lines to be monitored simultaneously. This proposal was so controversial that the FBI withdrew it and substituted a different capacity projection. Although not free from all ambiguity, the revised rule appears to require very large capacity provisions. For example, the Center for Democracy and Technology calculated that under the formula produced by the FBI, the system would require the capacity to perform 136,000 simultaneous intercepts in the Los Angeles area alone.

Domestic wiretapping without a court order is illegal in the United States, and only law enforcement and counter-intelligence agencies are allowed to apply for warrants. State and federal governments have cooperated with one or more of the world’s largest Internet service providers to design and build the infrastructure of the new global spying system. Nevertheless,Madeleine Acey, Europe Votes for ISP Spying Infrastructure, TECHWEB, May 13, 1999, available in http://www.techweb.com/wire/story/TWB19990513S0009.


Implementation of the Communications Assistance for Law Enforcement Act, 60 Fed. Reg. 53,643, 53-645 (proposed Oct. 16, 1995)(). To be fair, the FBI estimate lumped together wiretap needs along with less-intrusive forms of surveillance such as pen registers and “trap and trace” operations, which reveal information about who is speaking to whom, without disclosing the substance of the conversation. Id.


Warrants are not required abroad, either when the U.S. is wiretapping foreigners, see, e.g., or
federal courts authorized 1329 wiretaps in 1998, an increase of eighty over the 738 authorized a
decade earlier.92 These statistics are somewhat misleading, however, as a single wiretap order
can affect hundreds phone lines and up to 100,000 conversations.93 They are also difficult to
square with reports attributed to the FBI that on peak days up to 1000 different telephone lines
are being tapped in the Los Angeles area.94 Even so, although the number of wiretap orders is
increasing, and the number of persons subject to legal eavesdropping is also increasing, the
total number, however large, is still small compared to the enormous volume of
telecommunications. One reason why wiretaps remain relatively rare may be that judges have to
approve them (although the number of wiretaps refused annually is reputed to be near zero);
another, perhaps more important reason, is that they are expensive. The average cost of a
wiretap is over $57,000,95 with much of the expense being paid to the people who listen to the
calls. However, as the technologies developed by intelligence agencies trickle down to domestic
law enforcement, the marginal cost of telephone, fax, and e-mail surveillance should decline
considerably. Even if domestic law enforcement agencies remain scrupulously within the law,96
the number of legal wiretaps is likely to increase rapidly once the cost constraint is reduced.97

http://www.uscourts.gov/wiretap98/contents.html; Associated Press, State Authorities’

93 See Marc Cooper, Wired, NEWSTIMESLA.COM., Jan. 23, 1998, available in
authorization that produced the Gastelum-Gaxiola case, a mind-boggling 269 phone lines,
including an entire retail cellular phone company, were monitored. Taps on just three pay
phones at the L.A. County jail in Lynwood, for instance, yielded about 100,000 conversations in
six months, according to the Public Defender’s office.”).

94 See id.

95 Administrative Office of the U.S. Courts, supra note 92 at Table 5.

96 There is reason to doubt whether they do. See, e.g., Cooper, supra note 93 (describing LAPD
officers’ testimony of hundreds of illegal “hand offs” of information learned in one wiretap via
fictitious informants to initiate new cases); Los Angeles Public Defenders Office, State Wiretap
Related Cases, available in http://pd.co.la.ca.us/cases.htm (listing known and suspected cases
affected by illegal LAPD use of wiretap information).

97 There are also powerful commercial incentives for private harvesting of call information. For
example, British Telecom searched its records to find people who were regularly calling

999 alleging that “a loophole in the 1985 Interception of Communication Act means intelligence officials can put individuals and
organisations under surveillance without a specific ministerial warrant”).
The world wide web is justly celebrated as a cornucopia of information available to anyone with an Internet connection. The aspects of the web that make the Internet such a powerful information medium (its unregulated nature, the flexibility of browsing software and flexibility of the underlying protocols, plus being a blend of the world’s largest library, shopping mall, and chat room), all combine to make the web a fertile ground for harvesting personal data about web surfers. The more that people rely on the web for their reading and shopping, the more it becomes likely that data about their interests, preferences, and economic behavior will be captured and become part of a personal profile.

The baseline level of user monitoring is built into the most popular browsers and operates by default. Clicking on a link instructs a browser to automatically disclose the referring page to the new site. If a person has entered a name and email address in the browser’s email software that too will be disclosed automatically. These features cannot be turned off—they are part of the hypertext transfer protocol—although one can delete one’s name and e-mail address from the software. Web surfers can, however, employ privacy-enhancing tools such as the anonymizer to mask their personal information.

The default setting on both of the most popular browsers (Internet Explorer and Netscape Navigator) allows web sites to set and read all the “cookies” they want. Cookies are a means by which a browser allows a web site being viewed to write data to the user’s hard drive. Often this works to the user’s advantage—stored passwords eliminate the need to memorize or retype competing Internet service providers, and had its sales staff call to encourage them to switch to BT. See Office of Telecomm’s, OFTEL Acts to Ensures Fair Competition in Marketing of BT Click Internet Services, Sept. 24, 1998, available in http://www.worldserver.pipex.com/coi/depts/GOT/coi6043e.ok (announcing OFTEL had forced BT to cease practice after complaints).

To find out what your browser says about you, visit Privacy Analysis of Your Internet Connection at http://privacy.net/anonymizer/.

passphrases. Preference information allows the web designer to customize the web page to match individual users' tastes. But the process is usually invisible; and even when made visible is not transparent since few cookies are user-readable.

Cookies present a number of potential privacy problems. Any user data disclosed to a site, such as an address or phone number, can be embedded in a cookie. That information can then be correlated with user ID numbers set by the site to create a profile which. If taken to the limit, this would permit a particularly intrusive site to build up a dossier on the user. An online newspaper might, for example, keep track of which articles each reader looked at, allowing it over time to build up a picture of the reader's interests. Cookies can be shared between web sites, allowing savvy web designers to figure out what other web sites their visitors patronize, and (to the extent the other sites store information in cookies) what they have revealed to those other sites. Pieced together, this "clicktrail" can quietly reveal both personal and commercial details without the user ever being aware of it. A frequent visitor to AIDS sites, a regular purchaser of anticancer medicine, even someone who has a passion for Barry Manilow, all may have reasons for not wanting third parties to know of their interests or actions.

Complicating matters, what appears as one page image in a browser may actually be made up of multiple parts originating from multiple servers. Thus, it is possible to embed visible or even invisible content in web page which provides an occasion for setting a cookie. Doubleclick, an Internet advertising company, serves ads that appear on a large number of commercial and advertising-supported web pages. By checking for the doubleclick cookie, the company acquires the capability to assign a unique identifier to each surfer and trace which doubleclick affiliated web sites they visit, when, how often, and what they choose to view while they are there.\footnote{See Chris Oakes, Doubleclick Plan Falls Short, WIRED NEWS, Feb. 2000, available in http://www.wired.com/news/business/0,1367,34337,00.html.}

Cookies, however, are only the tip of the iceberg. Far more intrusive features can be built into browsers, into software downloaded from the Internet,\footnote{E.g., Chris Oakes, Mouse Pointer Records Clicks, WIRED NEWS, Nov. 30, 1999, available in http://www.wired.com/news/technology/0,1282,32788,00.html; Real Networks.} and into viruses or Trojan horses.\footnote{103} In the worst case, the software could be configured to report every keystroke to an
interested party.

The United States Government briefly floated the idea that Congress should authorize law enforcement and counter-intelligence agencies to remotely access computers and plant a back door in suspects’ computers.\textsuperscript{104} Using a back door potentially would give the government access to every keystroke, allowing it to learn passwords and decrypt files otherwise protected with strong, otherwise uncrackable, cryptography.\textsuperscript{105} The proposal in the original draft of the Cyberspace Electronic Security Act was sufficiently ambiguous to allow some to imagine that the government might even contract with makers of popular software to plant back doors which could then be activated remotely as part of an investigation. Whatever the facts, the clause in question, § 2713, was quickly dropped in the face of furious opposition from civil liberties groups and others.\textsuperscript{106} Other countries have considered similar plans. For example, according to the uncensored version of the Australian Walsh Report,\textsuperscript{107} Australian intelligence agencies sought authority to alter software or hardware so that it would function as a bugging device, capturing all user keystrokes, when activated by law enforcement authorities.\textsuperscript{108}

\textsuperscript{103} A trojan horse is a “malicious, security-breaking program that is disguised as something benign, such as a directory lister, archiver, game, or … a program…..” FOLDOC, Trojan Horse,” available in http://wombat.doc.ic.ac.uk/foldoc/foldoc.cgi?query=trojan+horse.


\textsuperscript{107} For the strange saga of the attempts to censor the Walsh report, see THE WALSH REPORT: REVIEW OF POLICY RELATING TO ENCRYPTION TECHNOLOGIES at http://www.efa.org.au/Issues/Crypto/Walsh/.

Monitoring also promises to figure in automated intellectual property rights management. Proposals abound for “copyright management technologies,”\textsuperscript{109} (sometimes unkindly dubbed “snitchware,”) which would be designed to record and in some cases disclose every time the user accessed a document, article, or even page of licensed material in order to finely meter the charges. Similarly, digital watermarking systems,\textsuperscript{110} which insert invisible customized tags into electronic documents, allow those documents to be tracked. Using various forms of these technologies, owners of valuable proprietary data can sell it with less fear that the information will be copied without payment. If the information is sold in encrypted form, along with a program or device that performs the decryption every time the licensee wishes to view part of the content, one of the important avenues of accessing plain text.

\textit{Id.}

The opportunity may present itself to the AFP, NCA or ASIO to alter software located in premises used by subjects of intensive investigation or destined to be located in those premises. The software (or more rarely the hardware) may relate to communication, data storage, encoding, encryption or publishing devices. While some modifications may have the effect of creating a listening device which may be remotely monitored by means of the telecommunications service, for which purposes extant warranting provisions would provide, others may create an intelligent memory, a permanent set of commands not specified in the program written by the manufacturer or a remote switching device with a capacity to issue commands at request. The cooperation of manufacturers or suppliers may sometimes be obtained by agencies. When manufacturers or suppliers are satisfied the modification has no discernible effect on function, they may consent to assist or acquiesce in its installation. It will not always be possible, however, to approach manufacturers or suppliers or the latter may be in no position to consent to modification of proprietary software. When agencies are investigating a high priority target, practising (SIC) effective personal and physical security, moving premises and changing telephone/fax regularly, an opportunity to access the target’s computer equipment may represent not only the sole avenue but potentially the most productive.

\textit{Id.} § 6.2.10.


\textsuperscript{110} See, e.g., Digimark Corp., available in http://www.digimarc.com/.
charging can be on a pay-per-view basis rather than requiring a large fee in advance. Leaving aside the issue of the effect on fair use, monitoring for pricing purposes is only a privacy issue if the details are recorded (and thus discoverable or subject to search and seizure) or if they are reported to the licensor. If all that is reported is the quantity of use, rather than the particular pages viewed or queries run, user privacy is unaffected. When the metering is conducted in real time, however, it is particularly difficult for the user to be confident about what is being reported. If a copyright management system is connected to the Internet in order, say, to ensure billing or even payment before access, then only the most sophisticated user will be able to determine how much information is being transmitted in order to get decryption authorization, and the temptation to build up user profiles for marketing purposes may be quite great.

Already, programs that quietly report in real time on every URL viewed to a central registry are common. Click on “what’s related” in the default configuration of Netscape 4.06 or above and every URL visited in that browser session will be reported back to a server at Netscape/AOL. Alone, this information only tells Netscape which sites people consider related to others; it helps them build up a database they can use to guide future surfers. But the logs of this data, in conjunction with cookies that recorded personal data, could be used to build extensive dossiers of individual web users. There is no reason to believe this is what Netscape does, but there is no technical obstacle to it.112

111 See Cohen, supra note 109, at .

Hardware manufacturers are also deploying privacy-compromising features in a wide variety of devices.
The General Motors corporation has equipped more than six million vehicles with (until recently) secret devices able to record crash data akin to airplane flight data recorders known as “black boxes.” First introduced in 1990, the automobile black boxes have become progressively more powerful. The 1994 versions “record 11 categories of information, including the amount of deceleration, whether the driver was wearing a seat belt, whether the airbag was disabled, any system malfunctions recorded by the on-board computer at the time of the crash and when the airbag inflated. A more sophisticated system installed in some 1999 models also records velocity, brake status and throttle position for five seconds before impact.” Other manufacturers also include less elaborate data recorders in their cars.

Makers of computer chips and ethernet cards adapters used for networking and for high-speed Internet access routinely build in unique serial numbers into their hardware, numbers which can then be accessed easily over the web.

The Intel Pentium III has a unique identification number on every chip. Intel originally designed the chip ID to be always on and accessible to software such as web browsers. The intention appears to have been to make electronic anonymity impossible. Anonymous users might, Intel reasoned, commit fraud or pirate digital intellectual property. With a unique, indelible ID number on each chip, software could be configured to work only on one system, and the ability of users to mask their identity would be reduced to cases where many people used a single machine, or one person used several machines. The unique ID could also serve as an index number for web sites, cookie counters, and others trying to track users across the Internet.

---


The revelation that Intel was building unique serial numbers into Pentium III chips caused a small furor.\textsuperscript{117} Intel therefore announced that it would commission a software program that would turn off the ID function.\textsuperscript{118} However, it appears that Intel’s software can be circumvented by a sufficiently malicious program and the ID number surreptitiously broadcast in a cookie or by other means.\textsuperscript{119}

Intel is not the only company to put unique serial numbers into its communication-related products. For many years, all ethernet cards, the basis for networks and most DSL\textsuperscript{120} connections, had a “Media Access Control” (MAC), a six-byte (usually represented as twelve alphanumeric characters) ID number built into them. This unique, unchangeable, number is important for networks, as it forms part of each device’s address, ensuring that no two devices on the network get confused with each other, and that no data packets get misdelivered. The privacy issues become most acute when the card is part of a computer that is used on the Internet or other communications networks, because the number can be used to identify the computer to which the ethernet card is attached.

Indeed, the new communications protocol Internet Protocol version 6 (IPv6),\textsuperscript{121} which will gradually replace the current Internet protocol, contemplates using an ethernet card’s unique number to create globally unique identifiers (GUIDs). The IPv6 standard requires software to include a GUID in the header of every Internet communication (e-mail, web browsing, chat, and others). Computers with an ethernet card would create a GUID by combining the unique ID

\begin{itemize}
\item \textsuperscript{118}See \textit{Big Brother Inside Homepage}, \textit{available in} \url{http://www.bigbrotherinside.com/#notenough}.
\item \textsuperscript{120}DSL stands for “Digital Suscriber Line.” See generally John Kristoff, comp.dcom.xdsl Frequently Asked Questions, \textit{available in} \url{http://homepage.interaccess.com/~jkristof/xdsl-faq.txt}.
\item \textsuperscript{121}See generally \textit{STEVIE KING, RUTH DIMITRY HASKING, WEAKEN LING, TOM MEEHAN, ROBERT FINK & CHARLES E. PERKINS, THE CASE FOR IPv6 4} (1999), \textit{available in} \url{http://www.ietf.org/internet-drafts/draft-ietf-iab-case-for-ipv6-05.txt} (touting IPv6’s “enhanced features, such as a larger address space and improved packet formats”); \textit{Ipv6: The Next Generation Internet!}, \textit{available in} \url{http://www.ipv6.org}.
\end{itemize}
number assigned to the card’s manufacturer and a unique number assigned to the card in the factory. 122 Thus, “[e]very packet you send out onto the public Internet using IPv6 has your fingerprints on it. And unlike your IP address under IPv4, which you can change, this address is embedded in your hardware. Permanently.” 123 In response to criticism, the standards-making bodies have revisions in the works to allow users--optionally, and if they are savvy enough to do so--to pick a random number to replace the GUID, and to change it from time to time. 124 But this modification is still wending its way through the standards process and would not, apparently, be the default.

Even before IPv6 was introduced, some software products, notably Word 97, Excel 97, and Powerpoint 97 routinely embed a unique ID number into every document. If the author’s computer had an ethernet card, the programs used its MAC, much like IPv6. 125 As a result, it became possible for law enforcement and others to trace the authorship of seemingly anonymous documents if they could match the MAC to a computer. This matching task was made easier by another Microsoft product: the initial version of the Windows 98 registration wizard transmitted the unique ID number to Microsoft; visitors to the Microsoft web site who had previously registered were then given a cookie with the ID number. 126 As a result, the Microsoft

122 See King et al., supra note 121, at 34 (defining IPv6 required header to include “a generic local address prefix to a unique token (typically derived from the host’s IEEE LAN interface address)”; see also IEEE, Guidelines for 64-bit Global Identifier (EUI-64) Registration Authority, available in http://standards.ieee.org/regauth/oui/tutorials/EUI64.html (explaining ID numbers).

123 Bill Frezza, Where's All the Outrage About the IPv6 Privacy Threat?, TECH WEB, Oct. 4, 1999 available in http://www.internetwk.com/columns/frezz100499.htm


125 See Yusef Mehdi, Microsoft Addresses Customers’ Privacy Concerns, PRESS PASS, Mar. 8, 1999, available in http://www.microsoft.com/presspass/features/1999/03-08custletter2.htm: “The unique identifier number inserted into Office 97 documents was designed to help third parties build tools to work with, and reference, Office 97 documents. The unique indentifier generated for Office 97 documents contains information that is derived in part from a network card . . . .” Until the most recent revisions, these numbers were then transmitted during the Windows 98 registration process. See Mike Ricciuti, Microsoft Admits Privacy Problem, Plans Fix CNET NEWS, Mar. 7, 1999, available in http://news.cnet.com/news/0-1006-200-339622.html?st.ne.160.head.

ID not only identified a computer, but it tied it directly to an individual’s personal data. These features were not documented.  Although there is no reason to believe that Microsoft used the information for anything more than tracking use of its website, there are powerful financial and commercial incentives for corporations to collect this information. A filing in a recent lawsuit claims that user information collected by Yahoo was worth $4 billion.  Not surprisingly, other companies, including RealNetworks and Amazon.com, have been shown to be collecting, or considering collecting, similar personal information. Indeed, it is possible that Microsoft’s data collection activity was a dry run for something more elaborate. Documents disclosed during the Microsoft antitrust case revealed that Microsoft had considered switching to an “annuity model” by which users would pay an annual fee for a Windows license in future versions of the operating system. Annual billing would most likely have required registering and identifying users.

Hardware with built-in device ID numbers are not yet ubiquitous, but proposals for expanding their use are increasingly common in part because law enforcement and others fear that anonymous activities lead to criminality and antisocial behavior.  For example, the fear the people may use color copiers to counterfeit U.S. currency has spurred makers of color copiers to put invisible unique ID numbers in each machine so that counterfeits can be traced to the originating machine.  The ID number appears in all color copies, making every copied document traceable to the originating machine. Because the quality of personal color printers


127 Associated Press, Microsoft Promises a Patch for ID Feature, Mar. 9, 1999, available in http://search.nytimes.com/search/daily/homepage/bin/fastweb?getdoc+cyber-lib+cyber-lib+4112+0+wAAA+micr0soft%7EID%7Eprivacy (“the company also acknowledged it may have been harvesting those serial numbers from customers--along with their names and addresses even when customers had explicitly indicated they didn’t want the numbers disclosed.”).

128 Kathleen Murphy, $4B Sought from Yahoo for Not Sharing Customer Data, INTERNET WORLD NEWS, Dec. 27, 1999, available in DisplayText cannot span more than one line!


131 See Froomkin, supra note 40, at 402-11.

continues to increase, the Treasury has become increasingly concerned that common inkjet color printers may become good enough for counterfeiters. As a result, the Treasury has begun to investigate the possibility of requiring tracing information be inserted into each color printer.\textsuperscript{133}

Ubiquitous hardware ID numbers are probably around the corner because they will enable smart homes and offices. Consider, for example, the smart fridge: “The fridge computer can automatically display a shopping list of what is running short. The list can then automatically be sent to a shop over the Internet. . . . can also incorporate cookbook functionality, i.e. the fridge can suggest suitable recipes depending on the contents of the fridge”\textsuperscript{134} When every food is tagged,\textsuperscript{135} and the fridge knows its expiration date, the fridge can even be programmed to nag you to throw out milk that outlasts its sell-by date. Smart home and office applications such as the smart fridge or the smart office supply cabinet will provide a cornucopia of marketing data, and the information officers of food suppliers and others are already making plans on how to get and use that information.\textsuperscript{136} Ultimately the information may be of interest to many others as well. Insurance companies, for example, might like to know if there are any cigarette packages in your home, whether you snack regularly, and how often you eat fatty foods.


\textsuperscript{135} Joseph Kaye, Niko Matsakis, Matthew Gray, Andy Wheeler & Michael Hawl, PC Dinners, Mr. Java and Counter Intelligence: Prototyping Smart Appliances for the Kitchen (Nov. 1, 1999) (unpublished paper submitted to IEEE for publication), available in http://www.media.mit.edu/ci/ieee.cga.jofish/ieee.cga.jofish.htm). (“We predict--even assume, in many of our scenarios--that all products sold will have a digital ID.”)

\textsuperscript{136} See Alice LaPlante, The Battle for the Fridge: The Food Industry is Looking to Hook Up Your Home to the Supply Chain, COMPUTERWORLD, Apr. 5, 1999, at 52(1), available in http://www.chic.sri.com/library/links/smart/fridge.html ("CIOs in the grocery industry are putting in the proper technical infrastructure to collect and consolidate customer data.").
The technology for identifying people is advancing at least as quickly as the technology for identifying machines. With technologies for distinguishing human irises, fingerprints, faces, or other body parts improving quickly, it seems increasingly attractive to use the “body as password” rather than base security on a passphrase, a PIN, or a hardware token such as a smart card. Biometrics can be used for identification (who is this) or authentication (what permissions does this person have).

To the extent that reliance on biometric identifiers may prevent information from being stolen or improperly disclosed, it is a privacy-enhancing technology. Some banks now use iris scans to determine whether a person is entitled to take money from an ATM. The U.S. government uses biometric identifiers in the border crossing identification cards issued to aliens who frequently travel to and from the U.S. on business, as do several states seeking to prevent fraudulent access to welfare and other benefits.

---

137 For a list of possibilities, see Java Card Special Interest Group, *Introduction to Biometrics*, available in http://www.sjug.org/jcsig/others/biometrics_intro.htm.


Despite their potential to enhance privacy, biometrics pose a two-pronged threat to privacy. First, a biometric provides a unique identifier that can serve as a high-quality index for all information available about an individual. The more reliable the biometric identifier, the more it is likely to be used, and the greater the amount of data likely to be linked to it. Because the biometric is a part of the person, it can never be changed. It is true that current indexes, such as social security numbers, are rarely changed, which is why they make good indexes, but in extreme cases one can leave the country or join the witness protection program. As far as we know, changing an iris or a fingerprint is even more difficult. Second, some biometrics, particularly those which involve DNA typing, disclose information about the subject, such as race, sex, ethnicity, propensity for certain diseases and (as the genome typing improves) more. Others may provide the capability to detect states of mind, truthfulness, fear, or other emotions.

DNA is a particularly powerful identifier. It is almost unique and (so far) impossible to change. A number of state and federal databases already collect and keep DNA data on felons and others. Attorney General Janet Reno recently asked the National Commission on the Future of DNA Evidence whether a DNA sample should be collected from every person arrested in the United States. Under this proposal, DNA information would become part of a permanent, permanent,

---


145 See Cavoukian supra note 144, at § 4. In addition, some people for religious or personal reasons find submitting to a biometric testing to be unacceptable. Even if the scan does not require a blood sample or other physical invasion, it may encroach on other sensibilities. See WOODWORD, supra note 140, text accompanying note 168 (“Having to give something of themselves to be identified is viewed as an affront to their dignity and a violation of their person. Certain biometric techniques require touching a communal reader, which may be unacceptable to some, due to cultural norms or religious beliefs.”).

146 See Dutch Data Protection Authority (Registratiekamer), supra note 139, §§ 2.1-2.3.

147 See DNA Fingerprinting, Encyclopedia Britannica Online, available in http://search.eb.com/bol/topic?eu=31233&sctn=1&pm=1 (noting that DNA is usually unique with “the only exception being multiple individuals from a single zygote (e.g., identical twins)

148 The FBI Combined Index DNA Indexing System (CODIS) alone currently contains information on 38,000 people. Approximately 450,000 samples await processing. See EPIC, supra note 36. Compare id. with Ng Kang-Chung, SOUTH CHINA MORNING POST, Feb. 12, 1999, Legislators Fear DNA Test Plans Open to Abuse, available at 1999 WL 2520961 (describing Hong Kong legislature’s fears of “allowing police to take DNA samples from suspects too easily”).
and sizable, national database: more than fifteen million people were arrested in the U.S. in 1997 alone. Such a plan is far from unthinkable--the Icelandic government considered a bill to compile a database containing medical records, genetic information, and genealogical information for all Icelanders.

Sense-enhanced searches rely on one or more technologies to detect or make visible that which ordinarily could not be detected or seen with un-aided human senses. These searches differ from surveillance in public places in that, with a few exceptions (such as airport body searches), sense enhanced searches are not yet routine, perhaps because of the rarity or expense of the necessary equipment. Instead, the typical sense-enhanced search is targeted at someone or something specific, or carried out at specific and usually temporary location. Unlike home or office monitoring, which usually requires equipment inside the place to be monitored, many sense-enhanced searches allow someone outside to see what is happening inside a building, or inside a package, or even clothing. Because there is no “entry” as the term is commonly defined, nor a physical intrusion, and because many of the technologies rely on emanations which are not coerced by the observer, there is room for dispute as to whether the use of these technologies constitutes either a Fourth Amendment “search” or a private law trespass. Because the technology for sense-enhanced searches is changing rapidly, there is also room for confusion as to what constitutes a reasonable expectation of privacy in a world where we are all increasingly effectively naked in transparent homes.

Governments appear to be the primary users of sense-enhanced searches, but many of the technologies are moving into private sector as prices decrease.

Looking down: satellite monitoring.

---

See EPIC, supra note 36.

Once the sole property of governments, high-quality satellite photographs in the visible spectrum are now available for purchase. The sharpest pictures on sale today are able to distinguish objects two meters long, with a competing one-meter resolution service planned for later this year.

Meanwhile, governments are using satellites to regulate behavior. Satellite tracking is being used to monitor convicted criminals on probation, parole, home detention, or work release. Convicts carry a small tracking device which receives coordinates from global positioning (GPS) satellites and communicates them to a monitoring center. The cost for this service is low, about $12.50 per target per day.

Meanwhile, the United Kingdom is considering the adoption of a GPS-based system, already field tested in the Netherlands and Spain, to prevent speeding. Cars would be fitted with GPS monitors that would pinpoint the car’s exact location, liaise with a computer built into the car containing a database of the national road map, identify the speed limit for the road on which the car was driving, and instruct a governor built into the vehicle to stop the fuel supply if the car passes a certain speed. GPS systems allow a receiver to work out its location by reference to satellites, but do not actually transmit the recipient’s location to anyone. The onboard computer could, however, permanently record everywhere the car goes, if sufficient

---

154 Gary Fields, Satellite “Big Brother” Eyes Parolees, Apr. 8, 1999, USA TODAY, at 10A.
155 Satellites in the Driving Seat, BBC NEWS, Jan. 4, 2000, available in http://newsvote.bbc.co.uk/hi/english/uk/newsid_590000/590387.stm (reporting that half of the users in the test said they would be willing to adopt system voluntarily).
storage were provided. The U.K. proposal also calls for making speed restrictions contextual, allowing traffic engineers to slow down traffic in school zones when needed, after accidents, or during bad weather.\textsuperscript{158} This contextual control requires a means for updates to be loaded to the computer; indeed, unless the U.K. wished to freeze its speed limits for all time, some sort of update feature would be essential. Data integrity validation usually relies on two-way communication. Once there is two-way communication between the speed control system and a central authority, the routine downloading of vehicle travel histories becomes a real possibility. And even without two-way communication, a satellite-controlled valve on a vehicle’s fuel supply opens the possibility of immobilizing vehicles for purposes other than traffic control. For example, cars could be stopped for riot control or if being chased by police; parents would have a new way of “grounding” children – and hackers would have a new target.

That a government can track a device designed to be visible by satellite does not, of course, necessarily mean that any individual without one could be tracked by satellite in the manner depicted by the film \textit{Enemy of the State}. However, even a one-meter resolution suggests that it should be possible to track a single vehicle if the satellite were able to provide sufficient images, and satellite technology seems to be improving rapidly.

The public record does not disclose how accurate secret spy satellites might be, nor what parts of the spectrum they observe other than visible light. The routine privacy consequences of secret satellites is limited, because governments tend to believe that using the results in anything less than extreme circumstances tends to disclose their capabilities. As the private sector catches up with governments, however, technologies developed for national security purposes will gradually become available for new uses.

\textit{Watching Me, Watching You, supra note \textsuperscript{62}}\textsuperscript{157} See Hibbs, \textit{supra} note 156.\textsuperscript{158}
defence against injury and violence, as for his repose,” but the walls of that fortress are far
more permeable than ever before. Suitably equipped observers can now draw informed
conclusions about what is going on inside a house without having to enter it. Most of these
technologies are passive, that is they do not require the observer to shine a light or any other
particle or beam on the target; instead they detect preexisting emanations.

Thermal imaging, for example, allows law enforcement to determine whether a building
has “hot spots.” In several cases, law enforcement agencies have argued that heat concentrated
in one part of a building tends to indicate the use of grow lights, which in turn (they argue)
suggests the cultivation of marijuana. The warrantless discovery of hot spots has been used to
justify the issuance of a warrant to search the premises. Although the courts are not unanimous,
the trend is decidedly towards holding that passive thermal imaging which does not reveal details
about the inside of the home does not require a warrant.160

The telephone is not the only electronic devices that makes new forms of monitoring
technically feasible. Computer monitors broadcast signals that can be replicated from a

---


160 See United States v. Robinson, 62 F.3d 1325, 1328-29 (11th Cir. 1995) (thermal imager
search does not violate the Fourth Amendment), United States v. Ishmael, 48 F.3d 850, 853-55
(5th Cir. 1995) (same), United States v. Myers, 46 F.3d 668, 669-70 (7th Cir. 1995) (same),
United States v. Ford, 34 F.3d 992, 995-97 (11th Cir. 1994) (same), United States v. Pinson, 24
F.3d 1056, 1058-59 (8th Cir. 1994) (same), United States v. Kyllo, 190 F.3d 1041 (9th Cir. 1999)
(holding that use of thermal imager did not require warrant because it “did not expose any
intimate details” of inside of home, and therefore privacy interest in waste heat was not one that
society would accept as “objectively reasonable”); but see State v. Young, 867 P.2d 593, 594
(Wash. 1994) (holding that a warrantless thermal image search violates State and Federal
Constitutions); United States v. Cusumano, 67 F.3d 1497, 1500-01 (10th Cir. 1995), vacated en
banc, 83 F.3d 1247 (10th Cir. 1996) (raising the possibility that thermal scans without a warrant
violate the Fourth Amendment and arguing that other circuit courts have “misframed” the Fourth
Amendment inquiry). For a more detailed analysis of the circuit courts’ thermal imaging cases,
see Lisa Tuenge Hale, Comment, United States v. Ford: The Eleventh Circuit Permits
Unrestricted Police Use of Thermal Surveillance on Private Property Without A Warrant, 29 GA.
L. REV. 819 (1995); Susan Moore, Does Heat Emanate Beyond the Threshold?: Home Infrared
Emissions, Remote Sensing, and the Fourth Amendment Threshold, 70 CHI.-KENT L. REV. 803
(1994); Lynne M. Pochurek, From the Battlefront to the Homefront: Infrared Surveillance and the
War on Drugs Place Privacy Under Siege, 7 ST. THOMAS L. REV. 137, 151-59 (1994); Matthew L.
Zabel, A High-Tech Assault on the “Castle”: Warrantless Thermal Surveillance of Private
considerable distance. Computer programs and viruses, can use this capability to surreptitiously broadcast other information besides what is displayed on the screen. The emissions are so powerful that one of the academics who first documented them suggested that Microsoft might want to use it to have its licensed programs “radiate a one-way function of its license serial number. This would let an observer tell whether two machines were simultaneously running the same copy of Word, but nothing more.” Microsoft, however, apparently was not interested in a copy protection scheme that would have required it to employ a fleet of piracy detection monitors cruising the world’s highways or hallways. Users can protect against the crudest types of distance monitoring of their computer displays by employing “Tempest fonts.” These special fonts will protect the user’s privacy by displaying a different text to any eavesdropper from the one actually displayed on the users’ screen.

=S4c. Seeing through clothes.@

Passive millimeter wave imaging reads the electromagnetic radiation emitted by an object. Much like an X-ray, passive millimeter wave imaging can specifically identify the radiation spectrum of most objects carried on the person, even those in pockets, under clothes, or in containers. It thus allows the user to see through clothes, and conduct a “remote frisk” for concealed weapons, or even dry powders or liquids. Imagers are available as a

---

162 E-mail from Ross Anderson to ukcrypto mailing list (Feb. 8, 1998) (available in http://www.jya.com/soft-tempest.htm).
handheld scanner, a visible gateway scanner, or in a hidden surveillance model.\footnote{168}

A similar product, which is not passive, uses low levels of X-rays to screen individuals for concealed weapons, drugs and other contraband. The makers of “BodySearch” boast that two foreign government agencies are using it for both detection and head-of-state security, and that a state prison is using it as a substitute for strip searching prisoners. The U.S. customs service is using it as a substitute for pat-down searches at JFK airport, prompting complaints from the ACLU. According to the ACLU, “BodySearch” provides a picture of the outline of a human body, including genitals: “If there is ever a place where a person has a reasonable expectation of privacy, it is under their clothing.”\footnote{169} And in fact, the sample photo provided by BodySearch makers American Science and Engineering, Inc. is fairly revealing.\footnote{170} Still newer devices such as a radar skin scanner can distinguish all anatomical features over one millimeter, making it possible to “scan someone standing on the street . . . [and] see through a person’s clothing with such accuracy that it can diameter of a woman’s nipples, or whether a man has been

\begin{quote}
(“As an imaging system, millimeter wave sensors cannot determine chemical composition, but when combined with advanced imaging software, they can provide valuable shape and location information, helping to distinguish contraband from permitted items.”).
\end{quote}

\footnote{168 See id. (containing links to various models).}

\footnote{169 Deepti Hajela, \textit{Airport X-Ray Device Spurs Concerns}, AP ONLINE, Dec. 29, 1999 (quoting testimony of ACLU legislative counsel Gregory T. Nojeim).}

\footnote{170 See http://216.149.33.140/images/pic_body02lg.jpg (reproduced below).}

\textbf{[note: copyright permission not yet secured]}
Perhaps the ultimate privacy invasion would be ubiquitous miniature sensors that would float around in the air. Amazingly, someone is trying to build them: The goal of the “smart dust” project is “to demonstrate that a complete sensor/communication system can be integrated into a cubic millimeter package” capable of carrying any one of a number of sensors. While the current prototype is seven millimeters long (and does not work right), the engineers hope to meet their one millimeter cube goal by 2001. At that size, the “motes” would float on the breeze, and could work continuously for two weeks, or intermittently for up to two years. A million dust motes would have a total volume of only one liter.  

Although funded by the Pentagon, the project managers contemplate a large number of potential civilian as well as military applications if they are able to perfect their miniature sensor platform. Among the less incredible possibilities they suggest are: battlefield surveillance, treaty monitoring, transportation monitoring, scud hunting, inventory control, product quality monitoring, and smart office spaces. They admit, however, that the technology may have a “dark side” for personal privacy.

The prospect of “smart dust,” of cameras too small to see with the naked eye, evokes David Brin’s and Neal Stephenson’s vision of a world without privacy. As the discussion above


172 See KRIS PISTER, JOE KAHN, BERNHARD BOSER & STEVE MORRIS, SMART DUST: AUTONOMOUS SENSING AND COMMUNICATION IN A CUBIC MILLIMETER, available in http://robotics.eecs.berkeley.edu/~pister/SmartDust/.

173 See id.

174 See NEAL STEPHENSON, THE DIAMOND AGE (1995) (imagining a future in which nanotechnology is so pervasive that buildings must filter air in order to exclude nanotechnology spies and attackers).
demonstrates, however, even without ubiquitous micro-cameras tomorrow, governments and others are deploying a wide variety of privacy-destroying technologies today. These developments raise the immediate question of the appropriate legal and social response.

One possibility is to just “get over it” and accept the emerging realities. Before adopting this counsel of defeat, however, it seems prudent to explore the extent to which the law offers strategies for resistance to data collection. The next part of this Article thus offers a survey of various proposals for a legal response to the problem of ubiquitous personal data collection. Because any legal reform designed to protect informational privacy arises in the context of existing law, the discussion begins by outlining some of the major constraints which must shape any practicable response to privacy-destroying technologies.

=S2A. The Constraints@

An effective response to privacy-destroying technologies, in the U.S. at least, is constrained by three factors: First, market failure caused by myopia among imperfectly informed consumers; second, by a clear, correct, vision of the First Amendment; and third, by fear.

=S31. The economics of privacy myopia.@

Under current ideas of property in information, consumers are in a poor position to complain about the sale of data concerning themselves. The original alienation of personal data may have occurred with the consumer’s acquiescence or explicit consent. Every economic transaction has at least two parties; in most cases the facts of the transaction belongs equally to both. As the existence of the direct mail industry testifies, both sides to a transaction generally

175 For an extreme example, see Moore v. Regents of California, 793 P.2d 479, (Cal. 1990) (holding a patient had no cause of action against his physician or others who used the patient’s cells for medical research without his permission).

176 See Spiros Simitis, From the Market to the Polis: The EU Directive on the Protection of Personal Data, 80 IOWA L. REV. 445, 446 (1995) (noting traditional view, now retreating in Europe, that "data . . . were perfectly normal goods and thus had to be treated in exactly the same way as all other products and services").
are free to sell the facts of the transaction to any interested third party.

There are exceptions to the default rule of joint and several ownership of the facts of a transaction, but they are relatively minor. Sometimes the law creates a special duty of confidentiality binding one of the parties to silence. Examples include fiduciary duties and a lawyer’s duty to keep a client’s confidence. Overall, the number of transactions in which confidentiality is the legal default appears relatively small compared to the total number of transactions in the US economy.

In theory, the parties to a transaction can always contract for confidentiality. It seems to me that in fact this is unrealistic due to seemingly rational economic behavior by consumers who in fact suffer from privacy myopia: consumers will sell their data too often and too cheaply. Modest assumptions about consumer privacy myopia lead one to the conclusion that even Americans who place a high value in information privacy will sell their privacy bit by bit for frequent flyer miles. Explaining this requires a brief detour into stylized microeconomics.

Assume that a representative consumer engages in a large number of transactions. Assume further that the basic consumer-related details of these transactions—consumer identity, item purchased, cost of item, place and time of sale—are of roughly equivalent value across transactions for any consumer and between consumers, and that the marginal value of the data produced by each transaction is low on its own. In other words, assume we are limiting the discussion to ordinary consumer transactions, not extraordinary private ones, such as the purchase of anticancer drugs. Now assume that aggregation adds value: once a consumer profile reaches a given size, the aggregate value of that consumer profile is greater than the sum of the value of the individual data standing alone. Most heroically, assume that once some threshold has been reached the value of additional data to a potential profiler remains linear and that there are not declining returns from another datum. Finally, assume that data brokers or profile compilers are able to buy consumer data from merchants at low transactions costs because these are repeat transactions between repeat players in which substantial amounts of data change hands. Consumers, however, are not aware of the value of their aggregated data to a profile compiler. With the possible exception of the assumption that profilers cannot overdose on data about a given consumer, these all seem to me to be very tame and reasonable assumptions.

177 MODEL CODE OF PROFESSIONAL RESPONSIBILITY Cannon 4 (1999); MODEL RULES OF PROFESSIONAL CONDUCT Rule 1.6. (1999)
assumptions.

In an ordinary transaction, a consumer will value a datum at its marginal value in terms of lost privacy. In contrast, the merchant, who is selling it to the profiler, will value it at or near its average value as part of a profile. Since on these assumptions the average value of a single datum is greater than the marginal value of that datum (remember, aggregation adds value), a consumer will always agree to have the data released at a price the merchant is willing to pay.

The ultimate effect of consumer privacy myopia depends on a number of things. First, it depends on how intrusive it is to be profiled. If the profile creates a privacy intrusion that is noticeably greater than an occasional individual fact would do -- that is, if aggregation not only adds value but aggravation -- then privacy myopia is indeed a problem. I suspect that this is in fact the case and that many people share my intuition that it is considerably more intrusive to find strangers making assumptions about me, be they true or painfully false, than it is to have my name and address residing in a database restricted to the firms from which I buy. On the other hand, if I am just weird, and aggregation does not usually cause additional harm to privacy, the main consequence of privacy myopia is greatly reduced. For some, it is only distributional. Consumers who place a low value on their information privacy--people for whom their average valuation is less than the average valuation of a profiler--would have agreed to sell their privacy even if they were aware of the long-run consequences. The only harm to them is that they have not extracted the highest price they could get. But consumers who place a high value on their information privacy will be more seriously harmed by their information myopia. Had they been aware of the average value of each datum, they might have preferred not to sell their data.

Unfortunately, if the marginal value\textsuperscript{178} to the consumer of a given datum is small, then the value of not disclosing that datum will in most cases be lower then either the cost of negotiating a confidentiality clause (if that option even exists), or the cost of forgoing the transaction of which it is a minor part.\textsuperscript{179} Thus, in the ordinary case, absent anything terribly revealing about the datum, privacy clauses are unlikely to appear in standard form contracts, and consumers will accept

\textsuperscript{178} Or even the average value to a well-informed consumer.

\textsuperscript{179} See Joel R. Reidenberg, Setting Standards for Fair Information Practice in the U.S. Private Sector, 80 IOWA L. REV. 497, 519-23 (1995); Jeff Sovern, Opting In, Opting Out, or No Options at All: The Fight For Control of Personal Information, 74 WASH. L. REV. 1033 (1999) (arguing that “businesses have both the incentive and the ability to increase consumers’ transaction costs in protecting their privacy and that some marketers do in fact inflate those costs”).
this. Furthermore, changing the law to make consumers the default owners of the fact of their economic activity is unlikely to produce large numbers of confidentiality clauses in the agora. In most cases, all it will do is move some of the consumer surplus from information buyers to information producers or sellers as the standard forms change to include a term in which the consumer conveys rights to the information in exchange for a frequent flyer mile or two.

In short, if consumers are plausibly myopic about the value of a datum--focusing on the marginal value of a datum rather than the average value, which is difficult to measure--but profilers are not myopic in this way and the data are more valuable in aggregate, then there will be substantial over-disclosure of personal data even when consumers care about their informational privacy.

If this stylized story is even somewhat congruent with reality, it has unfortunate implications for many proposals to change the default property rules regarding the ownership of personal data in ordinary transactions because the sale will tend to happen even if the consumer starts out with the sole entitlement to the data. It also suggests that European-style data protection rules would have only a limited effectiveness, primarily for highly sensitive personal data. The E.U.’s data protection directive allows personal data to be collected for reuse and resale if the data subject agrees; the privacy myopia story suggests that customers will ordinarily agree except when disclosing particularly sensitive personal facts with a high marginal value.

On the other hand, the privacy myopia story also suggests several profitable questions for further research. For example, the myopia story suggests that we need to know how difficult it is to measure the value of privacy and, once that value has been calculated, how difficult it is to educate consumers to value data at its average rather then marginal value. Can information provide corrective lenses? Or, perhaps consumers already have the ability to value the privacy interest in small amounts of data in the context of the long run consequences of disclosure.

Consumers sometimes have an interest in disclosure of information. For example, proof


\[181\] For an innovative, if slightly cute, attempt to teach children about privacy, see Media Awareness Network, Privacy Playground: The First Adventures of the Three Little Cyberpigs,
of credit-worthiness tends to improves the terms on which lenders offer credit. The myopia story assumes this feature away. It would be interesting to try to measure the relative importance of privacy and disclosure as intermediate and final goods. If it turned out that the intermediate good aspect of informational privacy and disclosure substantially outweighed their final good aspect, this would suggest that the focus on blocking disclosure advocated in this article was misguided, and that European data-protection rules--which focus on requiring transparency regarding the uses to which data will be put--might be the best strategy.

It would also be useful to know much more about the economics of data profiling. In particular, it would be helpful to know how much data it takes to make a profile valuable--at what point does the whole exceed the sum the data parts. Additionally, it would be important to know whether profilers regularly suffer from data overload, and to what extent there are diminishing returns to scale for a single person’s personal data. Furthermore, it could be useful to know to what extent there might be increasing returns to scale as the number of consumers profiled increases. If there are increasing returns to scale over any relevant part of the curve, the marginal consumer is worth extra. It might follow that in an efficient market, profilers would be willing to pay more for data about the people who are most concerned about their informational privacy.

There has already been considerable work on privacy-enhancing technologies for electronic transactions.\textsuperscript{182} There seems to be scope for more research, however, on which types of transactions are best suited to using privacy-enhancing technologies such as information intermediaries. The hardest work, however, will be finding ways to apply privacy-enhancing technologies to those transactions that are not naturally suited to them.

Perhaps the most promising avenue, however, is designing contracts and technologies that falsify the assumptions in the myopia story. For example, one might seek to lower the transaction costs of modifying standard form contracts, or of specifying restrictions on reuse of disclosed data. The lower the cost of contracting for privacy, the greater the chance that it will be less than the marginal value of the data (note that merely lowering it below average cost does

not solve the underlying problem, as sales will still happen in that price range). If technologies such as P3P\textsuperscript{183} are able to reduce the marginal transactions costs involved in negotiating the conditions attaching to the release of personal data to near-zero, even the privacy myopic will be able to express their privacy preferences in the P3P-compliant part of the marketplace.

\textsuperscript{183} P3P is the Platform for Privacy Preferences Project, a set of standards, architecture and grammar to allow complying machines to make requests for personal data and have them answered subject to predetermined privacy preferences set by a data subject. See Joseph M. Reagle, Jr., \textit{P3P and Privacy on the Web FAQ, available in http://www.w3.org/P3P/P3FAQ.html} ("P3P [allows] [w]eb sites to express their privacy practices and enable users to exercise preferences over those practices. P3P products will allow users to be informed of site practices (in both machine and human readable formats), to delegate decisions to their computer when appropriate, and allow users to tailor their relationship to specific sites.").

The First Amendment intersects the quest for privacy-enhancing rules in at least three ways: (1) most prohibitions on private data-gathering (i.e.- surveillance) in public places risk violating the First Amendment (similarly, most government surveillance in public appears unconstrained by the Fourth Amendment\textsuperscript{184}); (2) the First Amendment may also impose limits on the extent to which legislatures may restrict the collection and sale of personal data in connection with commercial transactions; and (3) the First Amendment right to freedom of association imposes some limits on the extent to which the government may observe and profile citizens, if only by creating a right to anonymity in at least some cases.\textsuperscript{185}

One of the arguments advanced most strenuously in favor of the proposition that the privacy battle is now lost to ubiquitous surveillance is that "information wants to be free," and that once collected, data cannot in practice be controlled. Although the most absolutist versions of this argument tend to invoke data havens or distributed database technology, the argument also draws some force from the First Amendment--although perhaps a little less than it used to.

\textsuperscript{184} "[I]f police are lawfully in a position from which they view an object, if its incriminating character is immediately apparent, and if the officers have a lawful right of access to the object, they may seize it without a warrant." Minnesota v. Dickerson, 508 U.S. 366, 375 (1993); \textit{see also} Michigan v. Long, 463 U.S. 1032, 1049-50 (1983).

\textsuperscript{185} See A. Michael Froomkin, \textit{Legal Issues in Anonymity and Pseudonymity}, 15 The Information Society
Perhaps the critical question shaping the legal and social response to new technologies of surveillance is the extent to which the one can limit the initial collection of personal data in public. Once information is collected, it is hard to control and almost impossible to erase once it gets into distributed databases. Legal rules prohibiting data collection in public are not the only possible response; defenses against collection might include educating people as to the consequences of disclosure or the deployment of countertechnologies such as scramblers, detectors, or masks. Unlike a legal solution, however, most technological responses involve shifting costs onto the data subject. The cost of compliance with any laws restricting data collection is likely to fall on the observer, at least initially. The difficulty is writing rules that are consistent with the First Amendment and with basic policies of freedom.

Professor Jerry Kang recently proposed and defended a statute banning the collection of personal information in cyberspace. As seen from the discussion in part I, there is no doubt that the collection of personal information in cyberspace is already a serious threat to information privacy, and that this threat will continue to grow by leaps and bounds. Professor Kang’s statute would be a valuable contribution to information privacy if it were adopted. But even if its economic importance is growing, cyberspace is only a small part of most daily lives. Part I also demonstrates that a great deal of the threat to information privacy is rooted firmly in “meatspace” (the part of life which is not cyberspace). The problem is considerably more general, and indeed cyberspace privacy and meatspace privacy are related, since the data drawn from both will be matched in databases. The Kang proposal, already unlikely to be adopted by a legislature, would need to be radically generalized to meatspace just to protect the status quo ante. Even if a legislature could be persuaded to adopt such a radically pro-privacy initiative, it is not at all clear that such an ambitious attempt to create privacy rights in public places would be constitutional.

113 (1999).
186 On masks, however, see text accompanying notes 280-296 infra (discussing anti-mask laws in several states).
187 See Kang, supra note 16.
In peacetime, the First Amendment allows only the lightest restrictions on ordinary gathering information in public places or on repeating information gathered in a public place. Other than cases protecting bodily integrity, the constitutional right to privacy is anemic, especially when compared to the First Amendment’s protection of the rights to gather and disseminate information. This is not necessarily a bad thing, especially when one considers that most rules designed to protect privacy in public places would probably have a very substantial harmful effect on newsgathering and public debate. Nevertheless, there are a few areas where light privacy-enhancing regulation might be possible without impinging on core first amendment values. There are also areas where laws actively hindering privacy might be reformed.

Gathering Information in Public. The First Amendment protects the freedom of speech and of the press, and does not mention the right to gather information. However, both the Supreme court and appellate courts have interpreted the First Amendment to encompass a right to gather information. The right is not unlimited. It does not, for example, create an affirmative duty on the government to make information available.

As a general matter, if a person can see it in public, she can write about it and talk about it. It does not inevitably follow that because she may share her natural sense impressions, or her written recollection, she can also photograph it or videotape it and then publish the

---

188 In Kleindienst v. Mandel, 408 U.S. 753 (1972), the Court acknowledged a First Amendment right to receive information, but said that their right must bow to Congress’ plenary power to exclude aliens. See also Lamont v. Postmaster General, 381 U.S. 301 (1965) (invalidating a statutory requirement that foreign mailings of "communist political propaganda" be delivered only upon request by the addressee); Martin v. City of Struthers, 319 U.S. 141 (1943) (invalidating a municipal ordinance forbidding door-to-door distribution of handbills as violative of the recipients’ First Amendment rights); Note, The Rights of the Public and the Press to Gather Information, 87 Harv. L. Rev. 1505, 1506 (1974) ("[w]hen the public has a right to receive information, it would seem to have a First Amendment right to acquire that information.").

189 See Los Angeles Police Dep’t. v. United Reporting Publ’g Corp., -U.S.-, 120 S.Ct. 483, 489-90 (1999); Zemel v. Rusk, 381 U.S. 1, 16-17 (1965).

190 Fourth Amendment rules are similar. It has long been held that no warrant is required to view objects in plain sight. Courts have similarly been reluctant to say that technologically assisted viewing implicates the warrants clause. Sometimes this is justified on the theory that the viewing is passive rather than invasive; other times it is justified by the court’s idea of what constitutes a reasonable expectation; still other times the focus seems to be on whether the surveillance revealed “intimate details.” Bernstein, supra note ‘165’, at 600-03. Certainly, it is clear that not every use of technology requires a warrant: A policeman using a flashlight to see into a parked car in the dark is not engaged in a “search” requiring a warrant. Texas v. Brown, 460 U.S. 730 (1983). On the other hand, the Supreme court has suggested that using a beeper to track a person might violate the Fourth Amendment if it were used to track movements in the defendant’s home. United States v. Karo, 468 U.S. 705 (1984).
mechanically recorded images and sounds. Most courts that have examined the issue, however, held that she may, subject only to very slight limitations imposed by the privacy torts.¹⁹¹ “[C]ourts have consistently refused to consider the taking of a photograph as an invasion of privacy where it occurs in a public fora.”¹⁹² Thus, in order for an invasion of privacy to occur, “[t]he invasion or intrusion must be of something which the general public would not be free to view.”¹⁹³

Perhaps it might be constitutional to prohibit devices that see through clothes only on the theory that there is a limited First Amendment exception allowing bans on outrageous assaults on personal modesty.¹⁹⁴ On the other hand, the government’s use of passive wave imaging, which does see through clothes pretty well, suggests either that one branch of the government thinks that there is no constitutional problem, or that the problem is solved by offering subjects the alternative of an (equally intrusive?) patdown search.¹⁹⁵ Or, perhaps, the government’s

¹⁹¹ See generally Phillip E. Hassaman, Annotation, Taking Unauthorized Photographs as Invasion of Privacy, 86 A.L.R.3d 374 (1978). The classic case is Daily Times Democrat v. Graham, 162 So. 2d 474 (Ala. 1964), reflected in the Restatement (Second) of Torts: (“Even in a public place, however, there may be some matters about the plaintiff, such as his underwear or lack of it, that are not exhibited to the public gaze; and there may still be invasion of privacy when there is intrusion upon these matters.” RESTATEMENT (SECOND) OF TORTS § 652B cmt. c


¹⁹³ Vazquez, 31 F. Supp. 2d at 90 (quoting Mark, 618 P.2d at 519).

¹⁹⁴ See, e.g., York v. Story, 324 F.2d 450, 455 (9th Cir. 1963) (holding that police violated privacy right of assault victim by forcing her to disrobe, pose nude in indecent positions, taking photographs, and distributing the photographs); Bowling v. Enomoto, 514 F. Supp. 201, 203 (N.D. Cal. 1981) (holding that male prisoners’ right to privacy requires limits on viewing and supervision by female guard); see also Rebecca Jurado, The Essence of Her Womanhood: Defining the Privacy Rights of Women Prisoners and the Employment Rights of Women Guards, 7 AM. U.J. GENDER SOC. POL’Y & L. 1, 35-40 (1999) (discussing person’s privacy interest in his/her own naked body).

¹⁹⁵ The U.S. Customs offers travelers the option of choosing a pat down search instead of the X-
ability to ban intrusive monitoring sweeps more broadly. Which is the correct answer doctrinally is unclear because as yet there have been no privacy-enhancing statutes seeking to block systematic data collection in public places. Ultimately, the answer may turn on just how outrageous high tech surveillance seems. Meanwhile, however, one must look to privacy tort cases in which the First Amendment was raised as a defense for what indications they offer as to the possible sweep of the First Amendment in public view cases.

Tort-based attempts to address the use of privacy-destroying technologies in public places tend to focus either on the target, the type of information, or whether a person might reasonably expect not to be examined by such a technology. Unless they seek to define the personal data as belonging to the data subject, approaches that focus on the person targeted tend to ask if there is something private or secluded about the place where person was which might create a reasonable expectation of privacy. If there was not, the viewing is usually lawful, and the privacy tort claim fails either because of the First Amendment or because the court says that the viewing is not a tort. Cases that focus on this type of information are usually limited to outrageous fact situations, like looking under clothes. Cases that focus on reasonable expectations are the most likely to find that new technologies can give rise to a privacy tort, but these expectations are notoriously unstable: the more widely a technology is deployed and used, the less reasonable it becomes to expect not to be subjected to it. Thus, for example, absent statutory change, courts would be unlikely to find a reasonable expectation not to be photographed in public, although it does not necessarily follow that there is no reasonable expectation against being on camera all the time.

Therefore, the core question of whether a legislature may constitutionally change the default, and make it an offense to use a particular new technology to view or record others in public, remains unanswered by current doctrine. Prohibiting the use of technologies that are not already commonplace prevents the public from becoming desensitized to them, and ensures that it is reasonable to expect to be able to walk in public without being scanned by them. Similarly, prohibiting the use of commonplace technologies also creates a (legally) reasonable expectation that others will follow the law, and that the technologies will not be used.

...ray, arguing plausibly that some might find the imaging to be less of an intrusion.

196 See note 192 supra.
General regulation of new technologies such as thermal imaging or passive wave imaging seems unproblematic on First Amendment grounds so long as the regulation applies to all uses.\textsuperscript{197} The legislature can ban a technology that happens to be useful for news gathering because that is a law of general application, so long as the ban is reasonably tailored to achieve some legitimate objective, among which privacy is surely found. There are limits: It is doubtful, for example, that a ban on pens and pencils ostensibly designed to prevent note-taking in public would survive very long. On the other hand, it might well be constitutional to prohibit using, or even possessing, some devices that enhance natural sensory perceptions on privacy grounds.\textsuperscript{198} Indeed, federal regulations already criminalize the sale of various types of spy gear.\textsuperscript{199}

Whether the ban could be crafted to apply only to use or possession in public places is more dubious as this cuts more closely against the First Amendment. Pragmatically, the results in court may depend on the currency of the technology. It is inconceivable, for example, that a ban on capturing all photographic images in public could possibly be squared with the First Amendment any more than could a ban on carrying a notebook and a pencil. Photography and television have become so much a part of ordinary life, and of news gathering and reporting, that such a ban would surely be held to violate the freedom of the press, and of speech, no matter how weighty the public interests in privacy.\textsuperscript{200} Possibly, however, a more limited ban might be

\textsuperscript{197} A similar calculation applies to the Fourth Amendment cases. As the Supreme Court noted in dicta in \textit{Dow Chemical}, “surveillance of private property by using highly sophisticated surveillance equipment not generally available to the public . . . might be constitutionally proscribed absent a warrant.” Dow Chemical Company v. United States, 476 U.S. 227, 106 S. Ct 1819, 1827 (1986). See Christopher Slobogin, \textit{Technologically-Assisted Physical Surveillance: The American Bar Association’s Tentative Draft Standards}, 10 HARV. J.L. & TECH. 383, 394-95 (1997) (noting that courts often find “the commonness of the surveillance technique to be dispositive” in Fourth Amendment cases).

\textsuperscript{198} Cf. Andrew Jay McClurg, \textit{Bringing Privacy Law Out of the Closet: A Tort Theory of Liability for Intrusions in Public Places}, 73 N.C. L. REV. 989, 1063 (1995) (making similar distinction in connection with privacy tort and proposing that “most situations involving actionable public intrusions would involve the defendant using some form of technological device (e.g., video camcorder, single-frame camera, audio recording device, binoculars, telescope, night vision scope) to view and/or record the plaintiff”).

\textsuperscript{199} See 18 U.S.C. § 2512(1)(a) (1986) (prohibiting mailing, manufacturing, assembling, possessing, or selling of “any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications,” so long as there is a connection with interstate commerce). The section also bans advertising such devices unless for official use only. \textit{Id.} §2512(c).

\textsuperscript{200} Cf. Forster v. Manchester, 189 A.2d 147, 150 (1963) (rejecting invasion of privacy claim
crafted to allow news gathering but not 24-hour surveillance. Such a rule might, for example, limit the number of images of particular place per hour, day or week, although lines will inevitably be difficult to draw. A more practical rule, perhaps easier to enforce, would distinguish between technologies.

_Disseminating Accurate Information._ Data collection becomes much less attractive if because “all of the surveillances took place in the open on public thoroughfares where appellant's activities could be observed by passers-by. To this extent appellant has exposed herself to public observation and therefore is not entitled to the same degree of privacy that she would enjoy within the confines of her own home.”); Daily Times Democrat v. Graham, 162 So.2d 474, 478 (Ala. 1964) (relying on Foster v. Manchester for proposition that it is not “such an invasion to take his photograph in such a place, since this amounts to nothing more than making a record, not differing essentially from a full written description of a public sight which anyone present would be free to see.”).

The constitutionality of limits of data gathering in public places may be tested by anti-paparazzi statutes. The statute recently adopted in California suggests what such a law might look like, although the California statute artfully avoids the interesting constitutional issues. The key parts of the statute state:

b) A person is liable for constructive invasion of privacy when the defendant attempts to capture, in a manner that is offensive to a reasonable person, any type of visual image, sound recording, or other physical impression of the plaintiff engaging in a personal or familial activity under circumstances in which the plaintiff had a reasonable expectation of privacy, through the use of a visual or auditory enhancing device, regardless of whether there is a physical trespass, if this image, sound recording, or other physical impression could not have been achieved without a trespass unless the visual or auditory enhancing device was used.

_CAL. CIV. CODE_ § 1708.8(b) (West 1999).

(e) Sale, transmission, publication, broadcast, or use of any image or recording of the type, or under the circumstances, described in this section shall not itself constitute a violation of this section, nor shall this section be construed to limit all other rights or remedies of plaintiff in law or equity, including, but not limited to, the publication of private facts.

_Id. § 1708.8(b)(e)(West 1999). By limiting the offense to invasions offensive to a reasonable person, where there was already a reasonable expectation of privacy, and exempting republishers, the statute avoids the hard issues. See generally Note, _Privacy, Technology, and the California “Anti-paparazzi” Statute_, 112 HARV. L. REV. 1367 (1999); Andrew D. Morton, _Much Ado About Newsgathering: Personal Privacy, Law Enforcement, and The Law of Unintended Consequences for Anti-paparazzi Legislation_, 147 U. PA. L. REV. 1435 (1999).
there are fewer buyers. One way to reduce the number of buyers is to make it illegal to buy, use, or reveal the data. Although the issue is not free from doubt, there are good reasons to believe that the First Amendment would forbid most legislation criminalizing the dissemination or use of accurate information. While good for free speech, it makes any ban on types of data collection much more difficult to enforce. Conversely, if is also constitutional to penalize downstream uses of certain data, and even retention or publication, then enforcement of a collection ban becomes easier, and the incentives to violate the rule become smaller.

The case for the constitutionality of a ban on the dissemination of some forms of accurate collected personal data is not negligible. It has long been assumed that sufficiently great government interests allow the legislature to criminalize the publication of certain special types of accurate information. Even prior restraint, not to mention subsequent criminal prosecution, might be a constitutionally acceptable reaction on the publication of troop movements in wartime, or other similar information that might aid an enemy during armed conflict. In peacetime, copyright protections are justified by a specific constitutional derogation from the general principle of freedom of speech. Some highly regulated industries, such as the securities industry, heavily regulate the speech of some persons, such as financial advisors or those with market sensitive information—although the constitutionality of those rules is itself subject to some doubt and debate. Generally, however, most truthful disclosures in the absence of a specific contractual duty to keep silent have usually been considered to have considered to be constitutionally protected.

The Supreme Court’s decisions pointedly do not give blanket First Amendment protection even to the publication of information acquired legally. Instead they have noted “[t]he tension

202 See Near v. Minnesota ex rel. Olson, 283 U.S. 697, 716 (1931) (“No one would question but that a government might prevent actual obstruction to its recruiting service or the publication of the sailing dates of transports or the number and location of troops”).


204 See Taucher v. Born, 53 F.Supp.2d 464, 482 (D.D.C. 1999) (upholding First Amendment challenge to § 6M(1) of the Commodity Exchange Act, as amended, 7 U.S.C. § 6m (1994), as applied to publishers of books, newsletters, Internet websites, instruction manuals and computer software providing information, analysis, and advice on commodity futures trading, because speech may not be proscribed “solely on a fear that someone may publish advice that is fraudulent or misleading”).

205 As Justice Marshall explained in Florida Star v. B.J.F., 491 U.S. 524, 532-33 (1989);
between the right which the First Amendment accords to a free press, on the one hand, and the protections which various statutes and common law doctrines accord to personal privacy against the publication of truthful information, on the other . . . .”

But, other than in cases involving intellectual property rights or persons with special duties of confidentiality, the modern Court has struck down all peacetime restrictions on publishing true information that have come before it. While keeping open the theoretical possibility that a sufficiently compelling government interest might justify penalizing the publication of true statements, even when faced with what might appear to be fairly compelling interests, such as protecting the privacy of rape victims, the Court has found the privacy interests insufficient to overcome the First Amendment. This pattern suggests that a compelling interest would have to be weighty indeed to overcome First Amendment values, and that most, if not all, privacy claims would fail to meet the standard. As the Supreme Court put it in Smith v. Daily Mail Publishing, “state action to punish the publication of truthful information seldom can satisfy constitutional standards.”

Furthermore, “if a newspaper lawfully obtains truthful information about a matter of public significance then state officials may not constitutionally punish publication of the information, absent a need to further a state interest of the highest order.”

Our cases have carefully eschewed reaching this ultimate question, mindful that the future may bring scenarios which prudence counsels our not resolving anticipatorily. See, e.g., Near v. Minnesota ex rel. Olson, 283 U.S. 697, 716, 51 S. Ct. 625, 75 L. Ed. 1357 (1931) (hypothesizing “publication of the sailing dates of transports or the number and location of troops”); see also Garrison v. Louisiana, 379 U.S. 64, 72, n.8, 74, 85 S. Ct. 209, 215, n.8, 216, 13 L. Ed. 2d 125 (1964) (endorsing absolute defense of truth “where discussion of public affairs is concerned,” but leaving unsettled the constitutional implications of truthfulness “in the discrete area of purely private libels”); Landmark Communications, Inc. v. Virginia, 435 U.S. 829, 838, 98 S. Ct. 1535, 1541, 56 L. Ed. 2d 1 (1978); Time, Inc. v. Hill, 385 U.S. 374, 383, n.7, 87 S. Ct. 534, 539-40, n.7, 17 L. Ed. 2d 456 (1967). Indeed, in Cox Broadcasting, we pointedly refused to answer even the less sweeping question “whether truthful publications may ever be subjected to civil or criminal liability” for invading “an area of privacy” defined by the State. Cox Broad. Corp. v. Cohn, 420 v.5. 469, 491 (1975).

=ft

206 Id. At 530.
208 443 U.S. 97, 102 (1979).
In *Cox Broadcasting Corp. v. Cohn*, the Court considered a state statute making it a “misdemeanor to publish or broadcast the name or identity of a rape victim.” The Court held that, despite the very private nature of the information, the First Amendment protected the broadcasting of the name of a deceased, seventeen-year-old rape victim, because the reporter obtained the information from open public records. Relying on the Restatement of Torts § 867 by analogy, the Court noted that “the interests in privacy fade when the information involved already appears on the public record.”

Then, in *Landmark Communications, Inc. v. Virginia*, the Court struck down a state statute that criminalized the publication of the name of a judge subject to confidential judicial disciplinary proceedings. Although the newspaper received the information from someone who had no right to divulge it, the Supreme Court held that the First Amendment barred criminal prosecution of a newspaper for publishing accurate information about a matter of public concern. The Court noted, however, that the case did not involve a person with an obligation of confidentiality: “We are not here concerned with the possible applicability of the statute to one who secures the information by illegal means and thereafter divulges it.” And, in *Smith v. Daily Mail Publishing Co.*, the Court said the First Amendment protected a newspaper that lawfully interviewed witnesses, obtained the names of juvenile offenders, and then published those names in violation of a state statute requiring prior leave of court to publish them.

Although the Court struck down the statute, it left open the possibility that publication of true and lawfully obtained information might lawfully be prohibited “to further an interest more substantial than is present here.” Similarly, in *Florida Star v. B.J.F.*, the Court held that the First Amendment barred damages against a newspaper that published the name of a rape victim that it had lawfully acquired.

More recently, in *Rubin v. Coors Brewing Co.*, the Court struck down a statute preventing

---

211 Id. at 494-95.
213 Id. at 837.
215 443 U.S. at 103.
brewers from stating the alcohol content of beer, even though the Court found that the rule regulated commercial speech and thus was subject to less exacting scrutiny than regulations on other types of speech.\textsuperscript{217}

Thus, prior to 1999, although the Supreme Court “carefully eschewed reaching th[e] ultimate question” of whether truthful publications of news can ever be banned, or even the narrower question of “whether truthful publications may ever be subjected to civil or criminal liability” for invading “an area of privacy,”\textsuperscript{218} its decisions suggested that if a category of truthful speech that can constitutionally be banned exists, it is small indeed, and that “state action to punish the publication of truthful information seldom can satisfy constitutional standards.”\textsuperscript{219}

To put it more bluntly, the Supreme Court’s cases do not make it clear whether illegally acquired information is (1) contraband per se, or (2) contraband so long as a recipient reasonably should know that it was illegally acquired, or (3) whether handing illegally acquired information to another launders it sufficiently to bring publication completely within the protections of the First Amendment.\textsuperscript{220} Which of the these is the law matters enormously to any attempt to regulate technologies of surveillance, as it affects how easily the information can be laundered through innocent, or even (should have been) knowledgeable parties.\textsuperscript{221} A recent

\begin{itemize}
\item \textsuperscript{216} 491 U.S. 524 (1989).
\item \textsuperscript{217} 514 U.S. 476 (1995).
\item \textsuperscript{218} \textit{Florida Star} at 533 (quoting Cox Broadcasting Corp. v. Cohn, 420 U.S. 469, 491 (1975)).
\item \textsuperscript{219} \textit{Daily Mail}, 443 U.S. at 102.
\item \textsuperscript{220} See \textit{Florida Star}, 491 U.S. at 534 n.8, stating, \textit{The Daily Mail} principle does not settle the issue whether, in cases where information has been acquired unlawfully by a newspaper or by a source, government may ever punish not only the unlawful acquisition, but the ensuing publication as well. This issue was raised but not definitively resolved in \textit{New York Times Co. v. United States}, 403 U.S. 713, 91 S. Ct. 2140, 29 L. Ed. 2d 822 (1971), and reserved in \textit{Landmark Communications}, 435 U.S. [at] 837, 98 S. Ct. 1535, 56 L. Ed. 2d 1. We have no occasion to address it here.
\item \textsuperscript{221} Washington is notoriously leaky. Except for the rare prior restraint cases involving national security such as \textit{New York Times v United States}, 403 U.S. 713 (1971) (The "Pentagon papers" case) and \textit{United States v. The Progressive, Inc.}, 467 F. Supp. 990, 997 (W.D. Wis. 1979) (H-bomb case) the government’s unbroken practice is to either ignore leaks, or, occasionally, to seek to impose after-the-fact criminal sanctions on the leakers but not on the press. See L. A. Powe, Jr., \textit{Mass Communications and the First Amendment: An Overview}, 55 LAW & CONTEMPORARY PROB. 53, 57-58 (1992) ("It has been almost twenty years and five administrations since \textit{Branzburg v. Hayes} held that there is no general first amendment privilege for reporters who wish to protect their confidential sources. Yet there has not been a single
divergence between two circuits suggests that the Supreme Court again may be asked to decide whether truthful information, obtained legally by the ultimate recipient, can nonetheless be contraband. Deciding that issue may require deciding the even more important question of when “information” is First Amendment speech, and when it is just a regulated commodity.

The D.C. Circuit and the Third Circuit recently reached opposite conclusions regarding the potential liability of a third party receiver of information illegally acquired by a second party. In both cases the information was an illegally intercepted telephone conversation on a matter of public interest; in both cases the information was ultimately passed to a newspaper. In *Boehner v. McDermott* the D.C. Circuit held that a Congressman who acted as a conduit for a tape between the interceptor and a newspaper could be prosecuted for violating the Wiretapping Act, 18 USC § 2511. The D.C. Circuit held that the prohibition on disclosure by third parties who had reason to know that the information had been illegally acquired was justified because: “Here, the `substantial governmental interest’ `unrelated to the suppression of free expression’ is evident.” The statute, the D.C. Circuit suggested, increases the freedom of speech because “[e]avesdroppers destroy the privacy of conversations. The greater the threat of intrusion, the greater the inhibition on candid exchanges. Interception itself is damaging enough. But the damage to free speech is all the more severe when illegally intercepted communications may be distributed with impunity.” In reaching this conclusion, the court characterized the Congressman’s action in being a conduit from the eavesdropper to the media as being a combination of speech and conduct.

_____________________________________________________

subpoena to trace an inside-the-Beltway leak of information. . . .”) (citation omitted).

222 191 F.3d 463 (D.C. Cir. 1999).

223 *See* 18 U.S.C. § 2511, creating civil and criminal causes of action against anyone who:

(c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;

(d) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection . . . .”

224 *Id.*

225 *Boehner v. McDermott*, 191 F.3d at 468 (quoting Time Warner Entertainment Co. v. FCC, 93 F3d 957, 969 (D.C. Cir. 1996)).

226 *Boehrer* *** (citing United States v. O’Brien, 291 U.S. 267, 376 (1968) for proposition that ‘when ‘speech’ and ‘nonspeech’ elements are combined in the same course of conduct, a sufficiently important governmental interest in regulating the nonspeech element can justify incidental limitations on First Amendment freedoms).
The Third Circuit saw the issue differently. *Bartnicki v. Vopper* involved a tape of a cellular telephone conversation between two members of a teachers' union who were involved in contentious pay negotiations with their school district. Someone recorded a conversation in which they discussed going to the homes of school members and “blow[ing] off their front porches.” That unknown party left the tape in the mailbox of one Jack Yocum, an opponent of the teachers' union, who then took it to the press.

On an interlocutory appeal, the Third Circuit held 2-1 that both Yocum, the conduit, and the subsequent publishers were protected by the First Amendment, even if they knew or had reason to know that the tape was illegally recorded.

Although the *Bartnicki* majority tried to disguise the extent of its disagreement with the D.C. Circuit by focusing its discussion on the media defendants, who had no analogue in the *Boehner* case, the fact remains that the *Bartnicki* majority held that Yocum, the conduit, was protected every bit as much as the media defendants. In so doing, the *Bartnicki* majority characterized Yocum’s conduct as pure speech, rejecting *Boehner*’s conclusion that it was more properly seen as at least partially conduct.

The first difficulty the Third Circuit had to overcome in reaching this conclusion was that in *Cohen v. Cowles Media* the Supreme Court explained that “generally applicable laws do not offend the First Amendment simply because their enforcement against the press has incidental effects on its ability to gather and report the news.” Furthermore, "enforcement of such general laws against the press is not subject to stricter scrutiny than would be applied to enforcement against other persons or organizations.

Despite holding that both Yocum and the media defendants engaged in pure speech, not a mixture of conduct and speech, the majority applied intermediate scrutiny because it found the Wiretap Act to be content-neutral. Intermediate scrutiny requires the court to weigh the

---

227 Bartnicki v. Vopper, 200 F.3d 109, __ (3d Cir. 1999).
228 *Id.* at __.
230 See 191 F.3d at 467 (noting that ultimate publishers of conversation were not defendants in the *Boehner* case).
231 *Cohen*, 501 U.S. at 669.
232 *Id.* at 670.
233 There is no doubt that the Wiretap Act is a general law rather than one directed solely at the press. The majority nonetheless concluded that the actions being regulated – the handing over of a tape containing a recording relating to a matter of public interest, and the dissemination of its content – were pure speech. To the government’s argument that the Wiretap Act separately regulated conduct because it prohibits using or endeavoring to use intercepted material, see 18 U.S.C. § 2511(1)(d), the
government’s interest, and the means selected to effectuate the interest, against the countervailing First Amendment interest. In doing this balancing, the court determined it must ask whether the regulation is “narrowly tailored” to achieve a “significant government interest.” The dissent agreed that this was the right test, but rejected the majority’s application of it to the facts.235

The Government argued that the Act is narrowly tailored. The regulation of third-party use, it said, eliminates the demand for the fruits of the wrongdoer’s labor.236 The majority was not persuaded, calling the connection between the third party provisions Act and the prevention of the initial interception of communications “indirect at best”237; in contrast, the dissent accepted the connection.238

The two sides thus differed on two issues: Whether handing over a tape is pure “speech,” and whether the prophylactic effect of a prohibition on “disclosing” or “using” the contents of a communication would a sufficiently great discouragement to the illicit acquisition of communications as to justify restricting the speech of recipients.

Although there is something distasteful about the idea of accurate information being contraband, even if hedged with a scienter requirement, it seems hard to believe that if Congress can make a law allowing prosecution of the recipients and republishers of personal data, this would have no discernable effect on the incentive to deploy privacy-destroying technologies. Rather, it seems likely that such a law would reduce the incentive to capture the data in the first place, since buyers would become harder to find. The argument is weakest on Bartnicki facts, where the motives for disclosure are political rather than financial, and the matter of is of public interest. The argument is surely stronger when applied to the disclosure of personal profile data.

The more fundamental question of what exactly constitutes speech, a question also raised by Bartnicki and Boeher, is much more difficult, and has considerably greater implications.

---

234 See 200 F.2d at 124.
235 Id. at 130.
236 Id. at 125. The government also argued that the Act would “deny[] the wrongdoer the fruits of his [own] labor,” id., but the majority noted on the facts neither defendant was the “wrongdoer” — the eavesdropper, so that justification did not apply. Id.
237 Id. at 126.
238 Id. at 133-34 (Pollak, J. dissenting).
for regulations designed to increase informational privacy; alas, privacy and free speech are in tension. Questions about what is properly characterized as “speech” dog the regulation of everything digital from the sale of bulk consumer data to the regulation of software.\textsuperscript{239}

The recent and unanimous Supreme Court decisions in \textit{Reno v. Condon}\textsuperscript{240} and the earlier decision in \textit{Los Angeles Police Department v. United Reporting Publishing Corp}\textsuperscript{241} suggest one possible answer. In \textit{Condon}, the Court upheld the Driver’s Privacy Protection Act (DPPA) against claims asserted under the Tenth and Eleventh Amendments. In so doing, the Court agreed with the petitioner that “personal, identifying information that the DPPA regulates is a thin[g] in interstate commerce,” and that the sale or release of that information in interstate commerce is therefore a proper subject of congressional regulation” under Congress’s Commerce Clause powers.\textsuperscript{242}

\textit{Condon} is a decision about federalism. Neither side briefed or argued the First Amendment reuse or republication rights of data recipients,\textsuperscript{243} so the issue remains open.\textsuperscript{244} It remains open even though the \textit{Condon} decision specifically relied on and upheld the part of the DPPA that regulates the resale and redisclosure of drivers’ personal information by private persons who have obtained that information from a state department of motor vehicles.\textsuperscript{245} The

\textsuperscript{239} Cf. Bernstein v. United States, 176 F.3d 1132, 1146 (9th Cir. 1999)(citations omitted), \textit{opinion withdrawn, rehearing en banc granted}, 192 F.3d 1308 (9th Cir. 1999) (deciding that source code is speech).
\textsuperscript{241} 120 S. Ct. 483, 489 (1999).
\textsuperscript{242} Id. (quoting United States v. Lopez, 514 U.S. 549, 558—59 (1995)).
\textsuperscript{243} Neither party briefed or argued the first amendment issue, except that the United States’s reply brief responded to a claim by an amicus that Condon was analogous to government targeting of a particular member of the press for adverse treatment. \textit{See} Reno v. Condon, \textit{Reply Brief for Petitioners, available in} 1999 WL 792145.
\textsuperscript{244} As Eugene Volokh reminded me, “cases cannot be read as foreclosing an argument that they never dealt with.” Waters v. Churchill, 511 U.S. 661, 678 (1994) (plurality opinion) (citing United States v. L.A. Tucker Truck Lines, Inc., 344 U.S. 33, 38 (1952)); see also Miller v. California Pac. Med. Ctr., 991 F.2d 536, 541 (9th Cir. 1993) (“It is a venerable principle that a court isn’t bound by a prior decision that failed to consider an argument or issue the later court finds persuasive.”).
\textsuperscript{245} \textit{See} 18 U.S.C. § 2721(c) (1994 ed. and Supp. III): “An authorized recipient of personal information . . . may resell or redisclose the information only for a use permitted under subsection (b) . . . . Any authorized recipient (except a recipient under subsection (b)(11)) that resells or rediscloses personal information covered by this chapter must keep for a period of 5 years records identifying each person or entity that receives information and the permitted purpose for which the information will be used and must make such records available to the motor vehicle.
DPPA, the Court stated, "regulates the States as the owners of databases" and it follows that similar rules could be applied to any database owner; indeed the Court defended the DPPA against South Carolina’s claim of regulating states exclusively by noting that § 2721(c) regulates everyone who comes into contact with the data.

The Supreme Court’s pre-Condon decisions left open the possibility that the First Amendment might apply more strongly when facts were legally acquired, as opposed to originating in the illegal actions of another. Legally acquired facts have the highest protection: “[I]f a newspaper lawfully obtains truthful information about a matter of public significance then state officials may not constitutionally punish publication of the information, absent a need to further a state interest of the highest order.” Of the cases discussed above, only Landmark Communications involved a leak of information by someone with a legal duty to keep it confidential. That case could be explained, if one chose to, as turning on the heightened First Amendment protection for reporting on important public issues, such as the honesty of judges.

In this light, the key factor in Condon may be the Court’s decision that no one has a right to driver’s license data in the first place because the data belonged to the government. When examining cases involving the regulation of government data use and reuse, the Court adopts what amounts to an informational right/privilege distinction: if access to the data is a privilege, it can be hedged with conditions. The same logic appears in Los Angeles Police Department v. United Reporting Publishing Corp. There, the Court upheld a statute requiring persons requesting arrestee data to declare that the arrestees’ addresses would not be used directly or indirectly to sell a product or service. The Court reasoned that because California had no duty to release arrestee data at all, its decision to impose substantial conditions on how the information would be used would survive at least a facial First Amendment challenge.

---

247 See id. (noting the DPPA is generally applicable). In Travis v. Reno, 163 F.3d 1000, 1007 (7th Cir. 1998), Judge Easterbrook characterized First Amendment arguments against the DPPA as “untenable.” It is clear from the context, however, that Judge Easterbrook was speaking only of the claim that there is a First Amendment right to view driver’s license records, and had not addressed himself to the republishing issue.
250 Id. at 489.
If the Court were to adopt what amounts to a right/privilege distinction relating to
government data, it is hard to see why the government’s ability to impose conditions that run with
its proprietary data should be any less than a private party’s, especially if those conditions
arguably restrict speech. If data are just a commodities, then data usage can be regulated by
contract or license -- a view that may import elements of a property theory of data into what had
previously been the preserve of the First Amendment.

Thus, the Supreme Court faces a choice. One view of the First Amendment, implied by
Bartnicki, suggests governments cannot impose sweeping restrictions on data dissemination in
the name of privacy. The alternate view of the First Amendment, offered by Boeher, is more
likely to allow the government to impose public limits on data dissemination and collection, and
thus enhance privacy.\textsuperscript{251}

The choice between these visions is closely connected to the constitutional status of any
regulation of the initial data collection. If it would be unconstitutional to impose a restriction on
the initial collection, then it will be difficult to impose constitutionally acceptable limitations on
downstream users of the data. When the government is not the data proprietor, the
Constitutional justification for a rule limiting, say, the dissemination of mall camera photos, or the
sale of consumer profiles will be closely tied, and perhaps identical, to whether the data
collection could be banned in the first place. If restrictions on the initial collection could be
imposed constitutionally, then the justification for imposing conditions that run with the data is
easy to see. If the data were lawfully acquired, the justification must depend on labeling the use
or dissemination as somehow the shipment of a data-good in commerce rather than a speech
act.

\textsuperscript{251} Ironically, a vision which makes it possible to restrict the speech of persons who receive
contraband information in the name of privacy is also the most compatible with developments as
diverse as the Uniform Computer Information Transactions Act and the Copyleft license, each of
enunciated in *Central Hudson Gas & Electric Corp. v. Public Service Commission of New York*:

> For commercial speech to come within [the First Amendment], it at least must concern lawful activity and not be misleading. Next, we ask whether the asserted governmental interest is substantial. If both inquiries yield positive answers, we must determine whether the regulation directly advances the governmental interest asserted, and whether it is not more extensive than is necessary to serve that interest.\footnote{\textsuperscript{252}}

Unlike public surveillance data, transactional data is usually collected in private by one of the parties to the transaction.

The government’s ability to regulate privately generated speech about commerce is surprisingly undertheorized, and underlitigated. This may be because there is not (yet) much relevant regulation in U.S. law. Under the common law, and absent a special duty of confidentiality as in an attorney-client relationship, the facts of a transaction belong jointly and severally to the participants. If Alice buys a chattel from Bob, ordinarily both Alice and Bob are free to disclose this fact. (If Alice is famous, however, Bob may not use her likeness to advertise his wares without her permission, although he certainly can tell his friends that Alice was in his shop.)\footnote{\textsuperscript{253}} Current doctrine can be read to suggest that speech about commerce is ordinary speech, if one applies “the ‘commonsense’ distinction between speech proposing a commercial transaction, which occurs in an area traditionally subject to government regulation, and other varieties of speech.”\footnote{\textsuperscript{254}} On the other hand, the two most recent Supreme Court decisions relating to the regulation of personal data seem to tend towards the view that some transactional

which legitimate private conditions on data dissemination.

\footnote{\textsuperscript{252}} 477 U.S. 557, 566 (1980).

\footnote{\textsuperscript{253}} See \textit{Restatement (Second) of Torts} § 652C (1977) (saying that it is an invasion of privacy for someone to appropriate the name or likeness of another); \textit{see also} \textit{Cal. Civ. Code} § 3344.1 (1999) (extending right of protecting one’s name or likeness from publicity to 70 years after death). For a survey of the evolving right of publicity in the U.S., compare Theodore F. Haas, \textit{Storehouse of Starlight: the First Amendment Privilege to Use Names and Likenesses in Commercial Advertising}, 19 U.C. DAVIS L. REV. 539 (1986) (arguing that the Supreme Court has begun a revolutionary reinterpretation of the constitutional status of commercial advertising, creating tension between the right to control the use of one’s name and likeness, and the free speech rights of advertisers) with James M. Treece, \textit{Commercial Exploitation of Names, Likenesses, and Personal Histories}, 51 TEX. L. REV. 637 (1973) (arguing that only those who can show actual injury from the appropriation of their name or likeness should be compensated otherwise holding the First Amendment should prevail).

data is just an information commodity, although the special circumstances of those decisions --
the data was held by state or local governments -- make generalization hazardous.

A very small number of statutes impose limits on the sharing of private transactional data
collected by persons not classed as professionals. The most important may be the Fair Credit
Reporting Act.255 In addition to having rules designed to make credit reports more accurate, the
statute also has a few rules prohibiting credit bureaus from making certain accurate statements
about aged peccadilloes, although even this statute of limitations does not apply to reports
requested for larger transactions.256 More directly federal privacy-oriented commercial data
statutes are rare. The Cable Communications Policy Act of 1984 forbids cable operators and
third parties from monitoring the viewing habits of subscribers. Cable operators must tell
subscribers what personal data is collected and, in general, must not disclose it to anyone
without the subscriber’s consent.257 The “Bork Bill,” formally known as the Video Privacy
Protection Act, also prohibits most releases of customers’ video rental data.258

Neither the privacy provisions of the Cable Act nor those of the Bork Bill appear to have
been challenged in court. Some have suggested that this is evidence of their uncontroversial
constitutionality.259 More likely, this proves only that merchants in two industries that sell a great
deal of sexually themed products have no incentive to do anything that reduces their customers’
beliefs that their viewing habits will not become public knowledge. As a doctrinal matter, the


256 See id. § 1681c (prohibiting reporting of bankruptcies that are more than 10 years old; “[c]ivil
suits, civil judgments, and records of arrest that, from date of entry, antedate the report by more
than seven years or until the governing statute of limitations has expired, whichever is the longer
period;” tax liens paid seven or more years earlier; or other non-criminal adverse information that
is more than seven years old. None of the prohibitions apply if the transaction for which the
report will be used exceeds $150,000, or the job on offer pays more than $75,000 per year.) See
also id. § 1681k (requiring that consumer credit reporting agencies have procedures in place to
verify the accuracy of public records containing information adverse to the data subject).


release customer names and addresses to third parties wishing to market them to customers so
long as there is no disclosure of titles purchased or rented. Customers can, however, be
grouped into categories by the type of film they rent. See id. § 2710(b)(2)(D)(ii).

259 See Kang, supra note 16, at 1282 (arguing that the proposed Cyberspace Privacy Act
Survives First Amendment scrutiny because of its similarity to the Cable Act and the Video
Privacy Protection Act, neither of which have been challenged on First Amendment grounds).
The most important constraint on an effective response to privacy-destroying technologies is fear. While greed for marketing data drives some applications, fear seems far more central, and much harder to overcome. Employers monitor employees because they are afraid workers may be doing unproductive or even illegal things. Communities appreciate cameras in public places because, whether cameras reduce or merely displace crime, one seems to be safer in front of the lens. And law enforcement officials constantly seek new tools to compete in what they see as an arms race with terrorists, drug dealers and other criminals.  

It would be well beyond the scope of this article to attempt to decide which of these fears are wellfounded, but any attempt at a political solution to the problem of personal data collection will have to confront these fears, whether they are wellfounded or not.

In making the case for increased privacy protection, one subtle fear also needs to be considered: Anything that increases a citizen’s reasonable expectation of privacy will, under current doctrine, also increase the scope of Fourth Amendment protections.  

See Equifax Serv., Inc. v. Cohen, 420 A.2d 189 (Me. 1980), (characterizing Equifax’s interest as commercial speech, but nonetheless finding that the First Amendment was violated).


See Morton, supra note 201, at 1470 (noting that current Fourth Amendment law is decided with regard to an individual’s reasonable expectation of privacy).
more that ubiquitous surveillance becomes commonplace, the less the Fourth Amendment will protect.

=S2B. Making Privacy Rules Within the Constraints@

The effect of these constraints on an effective response to privacy-destroying technologies is evident from the relatively limited protection against data acquisition provided by existing privacy rules in the United States. The constraints also suggest that several proposals for improving privacy protections are likely to be less effective than proponents might hope.

=S31. Nonlegal proposals.@

Proposals for nonlegal solutions to the problem of privacy-destroying technologies perforce must focus either on the data collector, or on the data subject. Proposals focusing on the data collector usually invoke some version of enlightened self-regulation. Proposals focusing on the data subject usually invoke the rhetoric of privacy-enhancing technologies or other forms of self-help.

Self-regulation has proved to be a chimera. In contrast, privacy-enhancing technologies clearly have a role to play in combating privacy-destroying technologies, particularly in areas such as protecting the privacy of telecommunications and other electronic messaging systems. It is unlikely, however, that privacy-enhancing technologies alone will be sufficient to meet the multifaceted challenge described in part one above. There may be some opportunities for the law to encourage privacy-enhancing technologies through subsidies or other legal means, but frequently the most important role for the law will be to remove existing obstacles to the employment of privacy-enhancing technologies or not to impose new ones.

=S4a. “Self regulation.”@
United States privacy policy has, until recently, been dominated by a focus on a very limited number of issues and, within those issues, a commitment to ask industry to engage in self-regulation. Since the economic incentive to provide strong privacy protections is either weak, nonexistent, or at least nonuniformly distributed among all participants in the marketplace, most serious proposals for self-regulation among market participants rely on the threat of government regulation if the data collectors fail to regulate themselves sufficiently.

Without some sort of government intervention to encourage self-regulation, “Wolves self-regulate for the good of themselves and the pack, not the deer.” Perhaps the most visible and successful self-regulatory initiative has been TRUSTe.com, a private third party privacy-assurance system. TRUSTe.com provides a privacy “trustmark” to about 750 online merchants who pay up to $5000 per year to license it. In exchange for the fee, TRUSTe verifies the existence of the online merchant’s privacy policy, but does not conduct an audit. TRUSTe does, however, investigate complaints that firms have violated their privacy policies. It currently receives about 375 complaints per year, and deems about twenty percent to be valid, triggering additional investigation. These decisions do not appear to be published save in exceptional circumstances.

---


264 See Joel R. Reidenberg, Restoring Americans’ Privacy in Electronic Commerce, 14 BERKELEY TECH. L.J. 771, 789 (1999) (“During the debate over self-regulation, U.S. industry took privacy more seriously only when government threats of regulation were perceived as credible.”); See also Peter P. Swire, Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information in PRIVACY AND SELF-REGULATION IN THE INFORMATION AGE, supra note 302, at 3, 11 (arguing that industry members might rationally prefer an unregulated market in which they can sell personal information to a self-regulated market, and therefore only the threat of mandatory government regulation can induce them to self-regulate).


266 See http://www.truste.org/webpublishers/pub_join.html#step3 (describing TRUSTe’s services).

267 See id. at Investigation Results, available in http://www.truste.org/users/users_investigations.html (stating that TRUSTe posts results of its investigations “[f]rom time to time.”). The page currently lists the results of only four investigations.
The meaningfulness of the “trustmark” was called into question when TRUSTe confirmed that 13 million copies of trustmark holder Real Networks’ RealJukebox Software created "globally unique identifiers" (GUIDs) and transmitted them to RealNetworks via the Internet every time the software was in use. The GUID could be associated with the user’s registration information to build up a profile of their music listening habits. RealNetworks’ privacy policy disclosed none of these facts. Nevertheless, once they came to light, RealNetworks kept its “trustmark” because the data collection was a result of downloaded software, and not anything on RealNetworks’ web page. Both the company’s web privacy policy and its accompanying “trustmark” applied only to data collection via the web pages, not other Internet-related privacy intrusions. A similar distinction between data collected via a web page and data collected by user-run software let Microsoft keep its “trustmark” after the discovery that its registration software sent a GUID and accompanying user data during windows 98 registration, even when the user told it not to. TRUSTe announced, however, that it was developing a pilot software privacy program with RealNetworks. Although the announcement did not actually say that the program would be expanded to other companies, much less when, it implied that it would.

---

268 See RealNetworks’ Privacy Intrusion, JUNKBUSTERS, available in http://www.junkbusters.com/ht/en/real.html (detailing the controversies surrounding the GUID discovery); TRUSTe, Truste & Realnetworks Collaborate to Close Privacy Gap, available in http://www.truste.org/about/about_software.html (describing TRUSTe's efforts to resolve the GUID situation); RealJukeBox Update, REAL NETWORKS, available in http://www.realnetworks.com/company/privacy/jukebox/privacyupdate.html (announcing Real Network's release of a software update designed to address customer concerns about privacy); Robert Lemos, Can You Trust TRUSTe?, ZDNET NEWS, Nov. 2, 1996, available in http://www.zdnet.com/zdnn/stories/news/0,4586,2387000,00.html (claiming that TRUSTe does not take active measures to assure that its licenseholders do not violate consumer privacy).

269 See TRUSTe & Real Networks Collaborate, supra note 268 (explaining that the GUID incident was outside the scope of TRUSTe’s privacy seal program because it did not involve collection of data on Real Networks’ website); See also TRUSTe FAQ, available in http://www.truste.org/users/users_investigationfaqs.html#offline (stating that TRUSTe does not deal with software or offline privacy practices but any with information collected and used at and by web sites).

270 See Watchdog #1723 -- Microsoft Statement of Finding, TRUSTE, available in http://www.truste.org/users/users_w1723.html (announcing that Microsoft had not violated its TRUSTe license because the manner in which the information was transferred did not fall within the boundaries of the TRUSTe license agreement, but acknowledging that the data transfer did compromise consumer trust and privacy).

271 See TRUSTe and Real Networks Collaborate, supra note 268 (announcing TRUSTe's plan to extend its privacy services to RealNetworks' Software applications and to form a working group of Software and Internet experts to advise TRUSTe how to extend its privacy seal program).
The RealNetworks incident followed an earlier, similar fiasco in which the FTC settled a complaint against GeoCities.\textsuperscript{272} The FTC charged that GeoCities “misrepresented the purposes for which it was collecting personal identifying information from children and adults.”\textsuperscript{273} According to the FTC, GeoCities promised customers that their registration information would be used only to “provide members the specific advertising offers and products or services they requested and that the ‘optional’ information [education level, income, marital status, occupation, and interests] would not be released to anyone without the member’s permission.”\textsuperscript{274} In fact, however, GeoCities created a database that included “email and postal addresses, member interest areas, and demographics including income, education, gender, marital status, and occupation” and disclosed customer data to marketers.\textsuperscript{275} In settling the case, GeoCities issued a press release denying the allegations. GeoCities then changed its privacy policy to disclose that user data might be disclosed to third parties with user consent (the previous policy also implied this; in any event the FTC charge was that disclosures happened without consent). TRUSTe, which had issued a trustmark to GeoCities during the FTC investigation, did not remove it.\textsuperscript{276}

Critics unkindly suggest that TRUSTe’s unwillingness to remove or suspend a trustmark results from its funding structure. Firms license the trustmark; in addition, some corporate sponsors, including Microsoft but neither RealNetworks nor GeoCities, contribute up to $100,000 per year in support.\textsuperscript{277} If TRUSTe starts yanking trustmarks, it loses revenue; if it gets a reputation for being too aggressive towards its clients, they might decide they are better off without a trustmark and the attendant hassle. In the absence of a meaningful way for consumers

\begin{itemize}
  \item \textsuperscript{272} See Jamie McCarthy, \textit{TRUSTe Decides Its Own Fate Today}, SLASDOOT, Nov. 8, 1999, available in \url{http://slashdot.org/yro/99/11/05/1021214.shtml} (detailing several other debacles, in which trustmark holders violated privacy policies or principles but kept their accreditation).
  \item \textsuperscript{274} Id. (quoting GeoCities’ membership sign-up form).
  \item \textsuperscript{275} Id. (quoting FTC statement).
  \item \textsuperscript{277} See TRUSTe Sponsors, TRUSTe, available in \url{http://www.truste.org/about/about_sponsors.htm} (listing TRUSTe’s corporate sponsors). EDS: I think this was right before: TRUSTe is the author here.
to evaluate the meaning of a trustmark or competing certifications, TRUSTe certainly has no economic incentive to be tough on its funding sources.

Perhaps the worst aspect of the TRUSTe story is that TRUSTe’s defense of its actions has a great deal of merit: The expectations loaded on to it, and perhaps the publicity surrounding it, vastly exceed its modest self-imposed mission of verifying members’ web-site privacy assertions, and bringing members into compliance with their own often quite limited promises. Taken on its own terms, TRUSTe is a very modest first initiative in self-regulation. That said, TRUSTe’s nonprofit status, the sponsorship of public interest groups such as the Electronic Frontier Foundation, and the enlightened self-interest of participant corporations who may wish to stave off government regulation all provide reasons why privacy certification bodies might someday grow teeth.

A more generic problem with self-regulatory schemes, even those limited to e-commerce or web sites in general, is that they regulate only those motivated or principled enough to take part in them. It may be that competitive pressures might ultimately drive firms to seek privacy certification, but given that currently fewer than 1000 firms participate in either TRUSTe or BBBOnline’s programs, the facts suggest that market pressure of this sort is currently weak to nonexistent. Indeed, after several years of calling for self-regulation regarding the collection of data from children, the Federal Trade Commission finally decided to issue extensive regulations controlling online merchants who sought to collect personal information from minors. If, as seems to be the case, industry self-regulation is at best marginally effective without legal intervention, and current third-party trust certification bodies have only a very limited influence, that does not mean that the FTC’s response is necessarily the only way to proceed.

The United States may be unique in putting faith in self-regulation without legal sanctions to incentivize or enforce it; it is hard to believe that the strategy was anything more than a political device to put off regulation. It does not follow, however, that self-regulation is a bad idea

---

278 See McCarthy, supra note ‘272’ (noting that TRUSTe is by far the industry leader in the U.S. Its only competitor, BBBOnline, has fewer than 100 members, compared to TRUSTe’s 750).

279 See, e.g., note 270, supra.

280 See Children’s Online Privacy Protection Rule, 16 C.F.R. § 312.5 (effective April 21, 2000) (requiring parental consent prior to collection of information from children under 13).

so long as legal conditions exist to create incentives to engage in it seriously. For example, an enormous amount of energy has gone into crafting “fair information practices.”

One way of creating incentives for accurate, if not necessarily ideal, privacy policies would be to use properly crafted legislation, harnessing market forces and the litigiousness of Americans, to create a self-policing as opposed to self-regulating system for web-based data collection. If all sites that collected personal data were required to have a privacy policy that stated what they collect and what they do with it, and if it were an actionable offense to violate a posted privacy policy, and if that private right of action were to carry statutory damages, then users—or class-action counsel—would have an effective incentive to police privacy policies for accuracy. Indeed, the surreptitious harvesting of user music preference data by RealJukeBox motivated two sets of enterprising lawyers to file class action lawsuits. One federal class action suit alleges misrepresentation and violation of the Computer Fraud and Abuse Act. Another class action was filed in California state court under the state’s unfair business practices law. Both lawsuits, however, face a problem in valuing the damages. In the federal case, the plaintiffs seek only a refund of the $30 some users paid for the registered version of the software. In the California case, plaintiffs say they will base their damages claim on their estimate of the market value of data about the class that RealJukebox collected—and that they will pick a figure after discovery. Unfortunately for the plaintiffs, there is no reason to believe that even a great deal of music preference information is going to be worth anything near the $500 per head that their lawyers estimated for the press. The willingness of the Federal plaintiffs to sue for only $30 per head suggests that creating a statutory damages remedy, even only $30 per user per offense, might create all the incentive needed to police online privacy policies.

The web, however, is not the world, and other means will also be required to cope with other technologies.


283 See Brian McWilliams, Real Hit With Another Privacy Lawsuit, INTERNETNEWS.COM, Nov. 10, 1999, available in http://www.internetnews.com/streaming-news/article/0,1087,8161_236261,00.html


285 See McWilliams, supra note 283.
PETs and other self-help.

Privacy Enhancing Technologies (PETs) have been defined as “technical devices organizationally embedded in order to protect personal identity by minimizing or eliminating the collection of data that would identify an individual or, if so desired, a legal person.” In addition to PETs embedded in organizations, there are also a number of closely related technologies that people can use for self-help, especially when confronted by organizations that are not privacy-friendly. These other PETs can be hardware, such as masks or thick curtains, or software, such as the Platform for Privacy Preferences (P3P), which seeks to reduce the transaction cost of determining how much personal data should be surrendered in a given transaction.

PETs and other privacy protection technologies can be part of a system design, or they can be a reaction to it. Law can encourage the deployment of PETs, but it can also discourage it, sometimes unintentionally. Some have suggested that the law should require, or at least encourage, the development of PETs. “Government must . . . act in a fashion that assures technological development in a direction favoring privacy protections rather than privacy intrusions.” That is a worthy goal and should be part of a comprehensive response to privacy-destroying technologies.

What is sometimes overlooked, however, is the ways in which existing law can impose legal obstacles to PETs. Laws and regulations designed to discourage the spread of cryptography are only the most obvious examples of the law imposing impediments to privacy-enhancing technology. Legal obstacles to privacy self-help also reach to the lowest technologies, as with antimask laws. In some cases, all PETs may need to flourish is the removal of legal barriers.

---


287 Reidenberg, supra note 264, at 789; see also Joel R. Reidenberg, Lex Informatica: The Formulation of Information Policy Rules through Technology, 76 Tex. L. Rev. 553, 584 (1998) (advocating that companies which do not protect personal data through PETs should have legal liability).
Privacy can be engineered into systems design. Systems can be built without much thought about privacy, or they can be constructed in ways intentionally designed to destroy it, perhaps to capture consumer information, perhaps to create audit trails for security purposes. In each case, after the system is in operation, users may be able to deploy self-help PETs to increase their privacy.

System designers frequently have great flexibility to build in privacy if they so choose. For example, when designing a road-pricing system, transponders can be connected to a card which holds the paid-up toll balance and deducts the funds as needed. No data identifying the driver or the car is needed, just whether there are sufficient funds on the card. Or, the transponder can instead emit a unique ID code, which is keyed to a record that identifies the driver and either checks for sufficient funds or bills her. The first system engineers in privacy at the expense of requiring a method of dealing with cars when the onboard card becomes depleted. The second system requires billing and can create a huge database of vehicular movements.

In general, designers can organize the system to withhold (or never know) data about the person, data about the object of the transaction, about the action performed, or even data about the system itself. Most electronic road-pricing schemes currently being deployed identify the vehicle, or a token attached to it.

If privacy has been built into a system, the need for individual self-help may be small, although in this world where software and other high technology is notoriously imperfect, users may have reasons for being cautious. If PETs are not built in to the system, or the user lacks confidence in the implementation, the user may engage in self-help. What sort of technology is likely to be effective depends on the circumstances and the nature of the threats to privacy. If,

---

288 For some suggested basic design principles see INFORMATION AND PRIVACY COMMISSIONER/ONTARIO, CANADA & REGISTRATIEKAMER [Dutch Data Protection Authority], supra note 182; see also Ian Goldberg, David Wagner & Eric Brewer, Privacy-enhancing Technologies for the Internet, available in http://www.cs.berkeley.edu/~daw/papers/privacy-compcon97-www/privacy-html.html (describing existing PETs and calling for additional PETs).

289 For discussion of such systems, see generally Symposium: Privacy and ITS, supra note 66.

for example, the one fears hidden cameras, then a pocket camera detector is just the thing. 291

For matters involving electronic communications or data storage, encryption is the major PET. 292 Here, however, the United States Government has been engaged in a long-running effort to retard the spread of consumer cryptography that might be used to protect e-mails, faxes, stored data, and telephone conversations from eavesdroppers and intruders--ostensibly because these same technologies also enable the targets of investigations to shield their communications from investigators. 293 As a panel of the Ninth Circuit put it in an opinion subsequently withdrawn for en banc consideration:

=xt
The availability and use of secure encryption may offer an opportunity to reclaim some portion of the privacy we have lost. Government efforts to control encryption thus may well implicate not only the First Amendment rights of cryptographers intent on pushing the boundaries of their science, but also the constitutional rights of each of us as potential recipients of encryption's bounty. Viewed from this perspective, the government's efforts to retard progress in cryptography may implicate the Fourth Amendment, as well as the right to speak anonymously, the right against compelled speech, and the right to informational privacy. 294
=ft

Perhaps in fear of another adverse judgment from the Ninth Circuit, the Government recently issued substantially liberalized encryption rules which for the first time allow the unrestricted


292 On encryption see generally Froomkin, supra note 261.


294 Bernstein v. United States, 176 F.3d 1132, 1146 (9th Cir. 1999)(citations omitted), opinion withdrawn, rehearing en banc granted, 192 F.3d 1308 (9th Cir. 1999).
The United States’ cryptography policy was an intentional effort to block the spread of a technology for reasons of national security or law enforcement convenience. Cryptography is a particularly significant PET because, if properly implemented, the mathematical advantage lies with the defender. Each increase in key length and security imposes a relatively small burden on the party securing the data, but an exponential computational burden on any would-be eavesdropper. Unlike so many other technologies, cryptography is relatively inexpensive and accessible to anyone with a computer or a dedicated encryption device. Cryptography is no privacy panacea, however. It is difficult to implement properly, vulnerable to every security weakness in the operating systems and programs that use it, and even at its best addresses only communications and records privacy—which as Part I above demonstrates is a significant fraction, but only a fraction, of the ways in which technology allows observers to collect information about us.

In other cases, legal obstacles to PETs are either by-products of other policies, or the result of long-standing prohibitions having new consequences in the networked era. For example, the prohibition against “reverse engineering” software—decompiling it to find out what makes it tick—may or may not be economically efficient, but it makes it nearly impossible for technically sophisticated users to satisfy themselves that programs are cryptographically secure, and thus makes it nearly impossible for them to reassure the rest of us, unless the program’s

---


authors release the source code for review.

Rules banning low-technology privacy tools may also need to be reexamined in light of the reduced privacy in public places. One possible reaction to ubiquitous cameras in public places would be the rise of the mask as a fashion accessory. Many states, however, have antimask laws on the books, usually enacted as a means of controlling the Ku Klux Klan; some of these statutes are over 100 years old.\textsuperscript{298} The statutes make it a crime to appear in public in a mask.\textsuperscript{299} Judicial opinion appears to be divided over whether prohibitions against appearing masked in a public place violate the First Amendment.\textsuperscript{300} Whatever one thinks of the constitutional issues, it is undeniable that existing antimask laws were enacted before anyone

\textsuperscript{298} See, e.g. Walpole v. State, 68 Tenn. 370, 372-73 (1878).


\textsuperscript{300} Decisions saying anti mask laws are unconstitutional include: American Knights of Ku Klux Klan v. City of Goshen, 50 F. Supp. 2d 835, 840 (N.D. Ind. 1999) (holding that city ordinance prohibiting mask-wearing for the purpose of concealing identity in public violated First Amendment rights to freedom of expression and anonymity); Aryan v. Mackey, 462 F. Supp. 90, 91 (N.D. Tex. 1978) (granting temporary restraining order preventing enforcement of antimask law against Iranian students demonstrating against the Shah); Ghafari v. Municipal Court, 150 Cal. Rptr. 813, 819 (Cal. Ct. App. 1978) (holding statute prohibiting wearing masks in public overbroad and finding that state’s fear that violence will result from the mere presence of anonymous persons is “unfounded”).

imagined that all urban public spaces might be subject to round-the-clock surveillance. Masks, which were once identified with KKK intimidation, could take on a new and potentially more benign social purpose and connotation; if so, the merits of anti-mask laws—if indeed they are constitutional after the right to anonymous speech enunciated in *McIntyre v. Ohio Elections Commission*\(^{301}\)—will need to be rethought.

=32. Using law to change the defaults.@

As the dimensions of the technological threat to privacy assumptions gradually have become clearer, academics, privacy commissioners, and technologists have advanced a number of suggestions for legal reforms designed to shift the law’s default rule away from formal neutrality regarding data collection. Rather than having transactional data belong jointly and severally to both parties, some of proposals would create a traditional property or an intellectual property interest in personal data which could not be taken by merchants or observers without bargaining. Others propose new privacy torts and crimes, or updating of old ones, to make various kinds of data collection in public or private spaces tortious or even criminal.

While some of these proposals have evident merit, they also have drawbacks.

=4a. Transactional data-oriented solutions.@

Scholars and others have proposed a number of legal reforms, usually based on either traditional property or intellectual property law, to increase the protection available to personal data by vesting the sole initial right to use that information in the data subject. Although the proposals on offer are the product of great ingenuity and thus vary considerably, the common element in most proposals to create a property interest in personal data is a desire to change the default rules in the absence of agreement. Changing the default rule to make the individual the sole owner of personal data even when it shared with a merchant, or visible in public, has a

---

number of attractive properties.\(^{302}\) It also has significant problems, however, both theoretically and practically.

One problem is that any such rule has to be crafted with care to avoid trampling the entire First Amendment. Any rule which makes it an offense to repeat what one sees, or who shops in one’s store, or who slept with whom, strikes dangerously close to core values of free speech.\(^{303}\) Current doctrine leaves open a space for regulation of transactional data along the lines of the Cable Television Act and the Bork Bill.\(^{304}\) That does not mean such rules are wise or easy to draft. As Professor Kang reminds us: “Consider what would happen if Bill Clinton had sovereign control over every bit of personal information about him. Then the New York Times could not write an editorial using information about Bill Clinton without his approval.”\(^{305}\) No one seriously suggests giving anyone that much control over their personal data, and certainly not to public figures. Rather, property or intellectual property based proposals usually concentrate on transactional data.

From a privacy perspective, the attractive properties of shifting the default rule are evident. Currently, user ignorance of the privacy consequences of disclosure, of the extent of data collection, and of the average value of a datum conspires with the relatively high transaction costs of negotiating privacy provisions in consumer transactions governed by standard form clauses to make privacy issues drop off the radar in much of routine economic life. Firms interested in capturing and reselling user data have almost no incentive to change this state of affairs.\(^{306}\) Shifting the default so that the data collector must make some sort of agreement with the data subject before having a right to reuse the data gives the data subject the benefit of notice and of transaction costs.

\(^{302}\) For a micro-economic argument that this change would be efficient given existing market imperfections, see Kenneth C. Laudon, \textit{Extensions to the Theory of Markets and Privacy: Mechanics of Pricing Information} in \textit{Privacy and Self-Regulation in the Information Age} 41 (U.S. Dep't of Commerce ed. 1997).


\(^{304}\) See \textit{supra} text at notes 258-259.

\(^{305}\) Kang, \textit{supra} note 16, at 1297 n.332.

The transaction cost element is particularly significant, but also potentially misleading. Shifting the default means that so long as the transaction costs of making an agreement are high, the right to personal data will not transfer and privacy will be protected. It is a mistake, however, to think that the transaction costs are symmetric. The very structural features of market exchange that make it costly for individuals to negotiate exceptional privacy clauses in today’s market make it cheap for the author of the standard form clause to change it to include a conveyance of the data and a consent to its use.  

Whether it is worth the trouble, or even economically efficient, to craft a system that results in people selling their data for a frequent flyer mile or two depends primarily on whether people are able to value the consequences of disclosure properly and whether contract rules can be changed to prevent the tyranny of the standard form. If not, then the standard form will continue to dominate much of the solution, to the detriment of data privacy; privacy myopia will do the rest.

Ironically, the advances in technology which are reducing the transactions costs of particularized contracting would also work to facilitate the sale of personal data, potentially lowering the cost enough to make the purchase worthwhile. If transaction costs really are dropping, it may be more important to craft rules that require separate contracts for data exchange and prevent the data sale from being part of a standard form. Such a rule would require not only an option to “opt-in” or “opt-out” as an explicit step in a transaction, if not a wholly separate one, but also require that failure to convey rights to personal data have no strings attached. But even that may not suffice. Here, the European experience is especially instructive. Despite state-of-the-art data privacy law, people, routinely and unknowingly contracted away their right to informational self-determination as part and parcel of a business deal, in which the right itself was not even a ‘bargaining chip’ during negotiations. But, since consent of the data subject had to be sufficient ground to permit information processing if one takes seriously the right to self-determination, such contractual devaluations of data protection were legally valid, and the

---

individual’s right to data protection suddenly turned into a toothless paper tiger.³⁰⁹
In short, even when faced with European data protection law, the standard form triumphed.

Given that property-law based solutions are undermined in the marketplace, some
European nations have gone further and removed the consumer’s freedom to contract away the
right to certain classes of data, such as information about race, religion, and political opinions.³¹⁰
While likely to be an effective privacy-enhancing solution, this cannot be said to be one that
corrects market failure in order to let the market reach an efficient outcome, nor one that relies
on property rights, thus eliminating the most common justifications for property-law-based
proposals to data privacy.³¹¹

=S4b. Tort law and other approaches to public data collection.@

Tort- and criminal-law-based proposals to enhance data privacy tend to differentiate
between information relating to behavior in places where one has a reasonable expectation of
privacy, such as one’s home, and public places where the law usually presumes that there is no
such expectation. Some of the more intriguing proposals further differentiate by the means used
to collect information, with sense-enhanced collections, especially new ones, being subject to
increased regulation.

For example, there are proposals to expand the tort of unreasonable intrusion to include
peering into private spaces from public ones. Where previously the tort often required the	
tortfeasor’s presence in the private space,³¹² the proposal is to allow the presence requirement to

³¹⁰ See *id.* at 233.
http://www.sims.berkeley.edu/~hal/Papers/policy/plicy.html; Richard S. Murphy, *Property Rights
³¹² The tort currently requires an objectively reasonable expectation of privacy in place or
circumstances. **RESTATEMENT (SECOND) OF TORTS** § 652B. Some jurisdictions also require an
actual trespass by the defendant. See, e.g., Pierson v. News Group Publications, Inc., 549 F.
be fulfilled, as it were, virtually. A rejuvenated tort of unreasonable intrusion might adapt well to sense-enhanced scanning of the body or the home. It is unlikely to cope as well with data generated in commercial transactions, for the same reasons noted above: transactional data are (at least formally) disclosed with consent. Similarly, privacy torts are unlikely to have much impact on DNA or medical databases since the data are either extracted with consent, or in circumstances, such as arrests, where consent is not an issue.

There is also reason to doubt whether privacy torts can be stretched far enough to cover CCTV and other forms of public tracking. Traditionally, privacy torts do not cover things in public view on the theory that if they are in public view they are, by definition, not private. Expanding them to cover public places would run directly into the First Amendment.

Some states have chosen to promote specialized types of privacy through targeted statutes. California’s antipaparazzi statute may be a model. It carefully focuses on creating

---

313 “The time has come,” argues Professor McClurg, “for courts to recognize openly and forthrightly the existence of the concept of ‘public privacy’ and to afford protection of that right by allowing recovery for intrusions that occur in or from places accessible to the public.” McClurg, supra note 198, at 1054 (proposing to revive the tort of invasion of privacy in public places through application of a multipart test); see also Diane L. Zimmerman, Requiem for a Heavyweight: A Farewell to Warren and Brandeis’ Privacy Tort, 68 CORNELL L. REV. 291, 347-48, 358-62 (1983).

314 See Dow Chemical Co. v. United States, 476 U.S. 227, 239 (1986) (holding than an airplane overflight is not a fourth amendment search); Shulman v. Group W Prods., Inc, 955 P.2d 469, 490 (Cal. 1998) (distinguishing between accident scene, in public view, and medivac helicopter, where there was a reasonable expectation of privacy). PROSSER AND KEETON ON THE LAW OF TORTS § 117 (5t ed. 1984).

315 CAL. CIV. CODE. § 1708.8(b) (1999): A person is liable for constructive invasion of privacy when the defendant attempts to capture, in a manner that is offensive to a reasonable person, any type of visual image, sound recording, or other physical impression of the plaintiff engaging in a personal or familial activity under circumstances in which the plaintiff had a reasonable expectation of privacy, through the use of a visual or auditory enhancing device, regardless of whether there is a physical trespass, if this image, sound recording, or other physical impression could not have been achieved without a trespass unless the visual or auditory enhancing device was used. Id § 1708.8(k):

For the purposes of this section, “personal and familial activity” includes, but is not limited to, intimate details of the plaintiff’s personal life, interactions with the plaintiff’s family or significant others, or other aspects of plaintiff’s private affairs or concerns. Personal and familial activity does not include illegal or otherwise criminal activity as delineated in subdivision (f). However, “personal and familial activity” shall include the activities of victims of crime in circumstances where either subdivision (a) or (b), or both, would apply.
liability for the gathering of information by private persons using sense-enhancing tools. While expanding the zone of privacy in the home, and making the property line into something resembling a wall impermeable to data, the statute does not cover activities on public streets and is crafted to avoid other First Amendment obstacles.

While the California statute focuses on creating narrow zones of privacy, an alternate approach seeks to regulate access to tools that can undermine privacy. For example, 18 U.S.C. § 2512 prohibits the manufacture, distribution, possession, and advertising of wire, oral, or electronic communication intercepting devices.\textsuperscript{316} Perhaps it is time to call for regulation of “snooper’s tools,” akin to the common law and statutory regulation of “burglar’s tools”?\textsuperscript{317}

Both of these approaches have potential, although both also have practical limitations in addition to the substantial First Amendment constraints. Many privacy-destroying tools have legitimate uses. For example, television cameras, even surveillance cameras, have their place, in banks, for example. Thus blanket rules prohibiting access to the technology are unlikely to be adopted, and would have substantial costs if they were. Rules allowing some uses but not others are likely to be difficult to police. Technology controls will work best if the technology is young and not yet widely deployed; but that is the moment when knowledge about that technology is least, and the chance of public outrage and legislative action are also at a minimum. As for the California antipaparazzi statute, it only applies to private collection of sense-enhanced data. It does not reach data collection by law enforcement, nor does it address database issues.\textsuperscript{318} And, as noted, it does not apply to public spaces.

\textsuperscript{316} 18 U.S.C. § 2512(1): Except as otherwise specifically provided in this chapter, any person who intentionally--(a) sends through the mail, or sends or carries in interstate or foreign commerce, any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications; (b) manufactures, assembles, possesses, or sells any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications, and that such device or any component thereof has been or will be sent through the mail or transported in interstate or foreign commerce.

\textsuperscript{317} Validity, Construction, and Application of Statutes Relating to Burglars’ Tools, 33 A.L.R.3d 798 (1970 & Supp. 1999). (“Statutes making unlawful the possession of burglars’ tools or implements have been enacted in most jurisdictions.”)

\textsuperscript{318} These and other limitations are criticized in Note, Privacy, Technology, and the California “Anti-Paparazzi” Statute, 112 HARV. L. REV. 1367, 1378-84 (1999).
The failure of self-regulation, and the difficulties with market-based approaches, have led regulators in Europe, and to a much lesser extent in the United States, to craft data protection laws. Although European Union laws are perhaps best known for their restrictions on data processing and reuse or resale of data, both the Union’s rules and various European nations’ rules also contain specific limits on collection of sensitive types of data. European Union rules for data use have an extraterritorial dimension, in that they prohibit the export of data to countries that lack data protection rules comparable to the Union’s. These extraterritorial rules do not, however, require that foreign data collection rules meet the Union’s standards, so the United States is on its own when it comes to deciding what data collection protections, if any, to enact for its consumers and citizens.

So far, the rules have been few and generally narrow, with the California antipaparazzi statute being a typical example. There is one sign, however, that things may be starting to change: What may be the most important United States’ experiment with meaningful limits on personal data collection by the private sector is just about to begin. Late last year the FTC promulgated detailed rules restricting the collection of data online from children under thirteen without explicit parental consent. These rules are due to come into effect in April, 2000.

In The Transparent Society, futurist David Brin argues that the time for privacy laws passed long before anyone noticed: “[I]t is already far too late to prevent the intrusion of

319 See Mayer-Schönberger, supra note 309, at 232; Reidenberg & Schwartz, supra note 5.
320 See Swire & Litman, supra note 5; Reidenberg & Schwartz, supra note 5.
321 See FTC Children’s Online Privacy Protection Rule, 16 C.F.R. § 312.5 (effective April 21, 2000), (requiring parental consent prior to collection of information from children under 13).
cameras and databases. . . . No matter how many laws are passed, it will prove quite impossible to legislate away the new surveillance tools and databases. They are here to stay."\textsuperscript{322} Instead, anticipating smart dust, he suggests that the chief effect of privacy laws will be "to make the bugs smaller."\textsuperscript{323} He is equally pessimistic about technical countermeasures to data acquisition, saying that "the resulting surveillance arms race can hardly favor the 'little guy'. The rich, the powerful, police agencies, and a technologically skilled elite will always have an advantage."\textsuperscript{324} Having concluded that privacy as we knew it is impossible, Brin goes on to argue that the critical policy issue becomes on what terms citizens will have access to the data inevitably enjoyed by elites. Only a policy of maximal shared transparency, one in which all state-created and most privately-created personal data is equally accessible to everyone, can create the liberty and accountability needed for a free society.

Brin's pessimism about the efficacy of privacy laws reflects the law's weak response to the reality of rapidly increasing surveillance by both public and private bodies described above in Part I. Current privacy laws in the United States make up at best a thin patchwork, one that is plainly inadequate to the challenge of new data acquisition technologies, as are the rather general international agreements that address the privacy issue.\textsuperscript{325} Even the vastly more elaborate privacy laws in Europe and Canada permit almost any consensual collection and resale of personal data.\textsuperscript{326} The world leader in the deployment of surveillance cameras, the United Kingdom, is a nation subject to what are among the strictest data protection rules in the world, but this has done little or nothing to slow the cameras’ spread. What is more, the law often tends to impose barriers to privacy-enhancing technology, or to endorse and require

\begin{footnotes}
\item[322]Brin, supra note 11, at 8-9.
\item[323]\textit{Id.} at 13.
\item[324]\textit{Id.} at 13.
\item[325]International agreements to which the United States is a party speak in at least general terms of rights to privacy. Article 12 of Universal Declaration of Human Rights, adopted by the United Nations in 1948, states that “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence.” GA Res. 217A (III), UN GAOR, 3rd Sess., Supp. No.13, UN Doc. A/810 (1948) at 71 available in http://www.hrweb.org/legal/udhr.html. Similarly, Article 17 of International Covenant on Civil and Political Rights states that “No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.” 999 UNTS 171 available in http://www.unhchr.ch/html/menu3/b/a_ccpr.htm.

Both agreements state that “Everyone has the right to the protection of the law against such interference or attacks.”
\item[326]Potentially invidious categories such as ethnicity are sometimes subject to special regulation.
\end{footnotes}
various forms of surveillance: in the words of one Canadian Information and Privacy Commissioner, “the pressures for surveillance are almost irresistible.”

Despite the very weak legal protections of informational privacy in the United States today, there is at least a case that Brin’s pessimism about the potential for law to corral technology and Scott McNealy’s defeatism about privacy are unfounded, or at least premature. No legal rule is likely to be perfect. Laws are violated all the time. But, making things illegal, or regulating them, does influence outcomes, and sometimes the effort required to achieve those outcomes is worth the cost.

Wiretap statutes are a case in point. It is illegal for the police to wiretap telephone lines without a warrant, and it is illegal for third parties to intercept both landline and cellular calls without the consent of one or both parties to the call. It would be naive in the extreme to suggest that either of these practices would no longer occur as a result of being illegal; it would be equally wrong, though, to suggest that this demonstrates that the laws are ineffective. If wiretapping and telephone eavesdropping were legal, and the tools easily available in every hobby shop, there would be much more wiretapping and eavesdropping.

Even the drug war, which surely stands for the proposition that law has limits as a tool of social control in a democracy, also supports the proposition that law can sometimes change behavior. It also reminds us, though, that law alone might not be enough, and that there are many different kinds of laws, with command and control regulation often being one of the least effective sorts.

The contrast between the wiretap laws and the drug war underline another important element in any attempt to use law to reign in personal data collection: Unless there is a

---


328 Some states require consent of both parties, some just one.


mechanism that creates an incentive for someone to police for compliance, legal rules will have at best limited effectiveness.331 Policing of so-called victimless crimes such as drug usage is hampered by the lack of such incentives. In contrast, the most important policing of wiretap law is conducted by judges, who throw out illegally gathered evidence in the course of reviewing petitions by highly motivated defendants. In other cases, such as my proposed statutory damages for falsifying privacy policies,332 the law can create or reinforce economic incentives for policing compliance.

At least one other contrast shapes and constrains any attempt to craft new legal responses to privacy-destroying technology. As the contrast between Parts I and II of this paper demonstrate, our legal categories for thinking about data collection are the product of a radically different evolution from the technological arms race that produces new ways of capturing information about people. The two do not line up particularly well. This different evolution explains why the U.S. Constitution is unlikely to be the source of a great expansion in informational privacy rights. The Constitution does not speak of privacy as such, much less informational privacy. Even though the Supreme Court has acknowledged that “there is a zone of privacy surrounding every individual,”333 the data contours of that “zone” are murky indeed. The Supreme Court’s relatively few discussions of informational privacy tend to be either dicta, to come in the context of finding that other interests are more important,334 or both.335

The variety of potential uses and users of data frustrate any holistic attempt to protect data privacy. Again, the Constitution is illustrative. Whatever right to informational privacy may

332 See supra text following note 285.
334 E.g. Nixon v. Administrator of Gen. Servs., 422 U.S. 425 (1977) (suggesting that former President has privacy interest in his papers); In Whalen the Court accepted that the right to privacy includes a generalized "right to be let alone," which includes "the individual interest in avoiding disclosure of personal matters." Whalen v. Roe, 429 U.S. 589 (1977) (finding that whatever privacy interest exists for patients in information bout their prescriptions was insufficient to overcome compelling state interest).
335 The leading counter-example to the assertion in the text is United States Dept. of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749 (1989), in which Supreme Court held that there was a heightened privacy interest in an FBI compilation of otherwise public information sufficient to overcome a FOIA application. Even if the data contained in a “rap sheet” were all available in public records located in scattered courthouses, the compilation itself, the “computerized summary located in a single clearinghouse” was not. 489 U.S. at 764.
exist today in the U.S. Constitution is a right against governmentally sponsored invasions of privacy only—it does not reach private conduct.336 Thus, even if the courts were to find in the Constitution a more robust informational privacy right than seems likely, it would address only a portion of the problem.337

Rules about data acquisition, retention, and use that might work for nosy neighbors, merchants, or credit bureaus might not be appropriate when applied to intelligence agencies. Conversely, governments may have access to information or technology that the private sector lacks today but might obtain tomorrow; rules that focus too narrowly on specific uses or users are doomed to lag behind technology. Restricting one’s scope (as I have in this article) to data acquisition, and leaving aside the important issues of data retention and reuse, may make the problem more manageable, but even so it remains dauntingly complex because the regulation of a single technology tends to be framed in different ways depending on the context. Sense-

336 Other than its direct prohibition of slavery, the U.S. Constitution does not directly regulate private conduct.

Some state constitutions’ privacy provisions also apply only to the government. For example, the Florida constitution provides that “Every natural person has the right to be let alone and free from governmental intrusion into the person’s private life except as otherwise provided herein. This section shall not be construed to limit the public’s right of access to public records and meetings as provided by law.” Fla. Const. Art I. § 23, but this does not apply to private actors. Hon. Ben F. Overton & Katherine E. Giddings, The Right of Privacy in Florida in the Age of Technology and the Twenty-first Century: A Need for Protection from Private and Commercial Intrusion, 25 FlA. STATE U.L. REV. 25, 53 (1997).


In 1972 the people of the State of California adopted a ballot initiative recognizing an “inalienable right” to “privacy”: “All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy.” Cal Const. Art. I § 1.

In 1994 the California Supreme Court held that the 1972 privacy initiative created a right of action against private actors as well as the government. Hill v. National Collegiate Athletic Ass’n, 865 P.2d 633, 644 (Cal. 1994). Although it described informational privacy as the “core value furthered by the Privacy Initiative,” the court also listed several conditions that would have to be met before a claim asserting that right could succeed. A plaintiff must show: (1) that the public or private defendant is infringing on a “legally protected privacy interest” – which in the case of informational privacy means the individual’s right to prevent the “dissemination and misuse of sensitive and confidential information” id. at 654; (2) a “reasonable expectation of privacy” based on “an objective entitlement founded on broadly based and widely accepted community norms” id.; and (3) a “serious invasion” of privacy by the defendant. Id. Even then, the court stated that privacy claims must be balanced against countervailing interests asserted by the defendant. Id. at 653.
enhanced searches, for example, tend to be treated as Fourth Amendment issues when conducted by the government. If the viewer is private, the Fourth Amendment is irrelevant. Instead, one might have to consider whether the viewing is an invasive tort of some type or perhaps even a misappropriation of information, who owns the information, and when a proposed rule limiting the acquisition or publication of the information might run afoul of the First Amendment.\footnote{Some issues are common to both public and private contexts: for example, whether the subject enjoys a reasonable expectation of privacy. (Even if the question is the same, however, the answers may be different. But generally the same technology initially raises distinct issues in the two contexts, at least until the information is sold, although this too may create its own special issues. \textit{Cf.} Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 752-53, 762-63, 780 (1989) (holding that the FBI could not release criminal rap sheet consisting predominately of information elsewhere on public record when disclosure would invade subject's privacy).}

That said, technological change has not yet moved so far or so quickly as to make legal approaches to privacy protection irrelevant. There is much the law can do, only a little of which has yet been tried. Many of the suggestions outlined above are piecemeal, preliminary, or incremental. At best they form only part of a more general strategy, which will also focus on regulation of data use once it has been collected. Whenever the law can address the issue of data collection itself, however, it reduces the pressure on data protection law and contributes greatly to data privacy protection.

Alas, there is no magic bullet, no panacea. If the privacy pessimists are to be proved wrong, the great diversity of new privacy-destroying technologies will have to be met with a legal and social response that is at least as subtle and multifaceted as the technological challenge. Given the rapid pace at which privacy-destroying technologies are being invented and deployed, a legal response must come soon, it will indeed be too late.