The Death of Privacy?

A. Michael Froomkin*

The rapid deployment of privacy-destroying technologies by governments and businesses threatens to make informational privacy obsolete. The first part of this article describes a range of current technologies to which the law has yet to respond effectively. These include: routine collection of transactional data, growing automated surveillance in public places, deployment of facial recognition technology and other biometrics, cell-phone tracking, vehicle tracking, satellite monitoring, workplace surveillance, internet tracking from cookies to "clicktrails," hardware-based identifiers, intellectual property protecting "snitchware," and sense-enhanced searches that allow observers to see through everything from walls to clothes. The cumulative and reinforcing effect of these technologies may make modern life completely visible and permeable to observers; there could be nowhere to hide. The second part of the article discusses leading attempts to craft legal responses to the assault on privacy – including self-regulation, privacy-enhancing technologies, data-protection law, and property-rights based solutions – in the context of three structural obstacles to privacy enhancement: consumers' privacy myopia; important First Amendment protections of rights to collect and repeat information; and fear of what other people may do if not monitored. The article concludes that despite the warnings of information privacy pessimists, all is not lost – yet.

---

* Professor of Law, University of Miami School of Law. B.A. Yale, M.Phil Cambridge, J.D. Yale. Email: froomklin@law.tm. I am grateful for advice from Caroline Bradley, Patrick Gudridge, and Eugene Volokh, for research assistance from SueAnn Campbel and Julie Dixson, and extraordinary secretarial assistance from Rosalia Lliraldi. The errors that survive are my own. Unless otherwise noted, this article seeks to reflect legal and technical developments as of Feb. 1, 2000. After completing this article I had a chance to read SIMPSON GARFINKEL, DATABASE NATION (2000), which explores many of the themes discussed in this article. I recommend it anyone interested in these issues. All Internet citations were current as of May 22, 2000.

"You have zero privacy. Get over it."

—Sun Microsystems, Inc., CEO Scott McNealy[1]

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 upon 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."[2] One need look no further than the First Amendment of the United States 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 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 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]

---

1. Deborah Radcliff, *A Cry for Privacy*, COMPUTER WORLD, May 17, 1999 <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.*

3. *See* KARL G. HEIDER, ETHNOGRAPHIC FILM 11-15, 49-62 (1976) (discussing ways in which the act of filming may distort or misrepresent reality); SHOSHANA ZUBOFF, IN THE AGE OF THE SMART MACHINE: THE FUTURE OF WORK AND POWER 344-45 (1988) (describing the phenomenon of "anticipatory conformity" among persons who believe they are being observed). *Cf.* Estes v. Texas, 381 U.S. 532, 545 (1965) (noting that it is "highly probable" that the presence of cameras in the courtroom will influence jurors).

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 will increase. 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 *collection* and not data *collation*. Much of the best work on privacy, and the most comprehensive legislation,[5] while not ignoring 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. Issues of data use and re-use cannot be avoided, however, because one of the ways to reduce data collection is to impose limits on the use of improperly collected data. Conversely, if limits on initial data collection are constitutional, then it is more likely that efforts to prohibit the retransmission or republishing of illicitly collected data would be held to be constitutional as well.

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,"[6] 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 communica-

---

4. The definition differs from that used in United States 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. *See* LAURENCE H. TRIBE, AMERICAN CONSTITUTIONAL LAW § 15-1 (2d ed. 1988); Ken Gormley, *One Hundred Years of Privacy*, 1992 WIS. L. REV. 1335, 1340.

5. The European Union's Privacy Directive, Council Directive 95/46 of the European Parliament and of the Council on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31, is probably the most comprehensive attempt to protect informational privacy, although experts disagree about its domestic and especially extraterritorial effects. *Compare* PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW: A STUDY OF U.S. DATA PROTECTION (1996), *with* PETER P. SWIRE & ROBERT E. LITAN, NONE OF YOUR BUSINESS WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE (1998).

6. BENJAMIN FRANKLIN, POOR RICHARD'S ALMANAC (1735), *reprinted in* THE OXFORD DICTIONARY OF QUOTATIONS 211 (2d ed. 1959).

tions 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.[7] 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 diverse individuals such as Britain's Prince Charles, House Speaker Newt Gingrich, and White House Intern Monica Lewinsky.[8] 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 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."[9] Part I of this article describes a number of illustrative technological developments that facilitate the collection of personal data. Collectively these and other developments 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 profil-

---

7. *See* 8 U.S.C. § 1324a(a)(1)(B) (1996) (prohibiting hiring workers without verifying identity and authorization to work in the United States). Employers must complete an INS Form I-9, Employment Eligibility Verification Form, documenting this verification and stating the type of ID they examined. *See* Verification of Employment Eligibility, 8 C.F.R. § 274a.2 (1999).

8. See Boehner v. McDermott, 191 F.3d 463, 465 (D.C. Cir. 1999) (describing the taping of a cell phone call including Speaker Gingrich); OFFICE OF THE INDEPENDENT COUNSEL, REFERRAL TO THE UNITED STATES HOUSE OF REPRESENTATIVES PURSUANT TO TITLE 28, UNITED STATES CODE, § 595(C) § I.B.3 ("The Starr Report") <http://icreport.loc.gov/icreport/6narrit.htm#L7> (describing recording of Lewinsky calls by Linda Tripp); Paul Vallely, *The Queen Brings Down The Shutters*, THE INDEP., Aug. 19, 1996, *available in* 1996 WL 10952752 (noting the taping of intimate conversation of Prince Charles).

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.

9. *See* Roger Clarke, *Information Technology and Dataveillance*, 31 COMM. ACM 498 (May 1988) (defining dataveillance as "the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons") <http://www.anu.edu.au/people/Roger.Clarke/DV/CACM88.html>.

ing is vastly increased by the power of information processing and the 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 informational equivalent of a goldfish bowl.[10]

If the pace at which privacy-destroying technologies are being devised and deployed is accelerating, the basic phenomenon is nevertheless old enough already 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 will have undesirable or unconstitutional effects, and that even the best will protect only a narrow range of privacy on their own.

The relative weakness of current privacy-enhancing strategies sets the stage for the conclusion of the article, which challenges 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 supporting this view, a case made trenchantly by David Brin's *The Transparent Society*,[11] 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 regain 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,[12] not to mention televised public talk-

---

10. So-called "reality" television programming provides a possible glimpse of this world. The popularity of these shows demonstrates the supply of willing watchers, and there appear to be many willing subjects. *See, e.g.*, Associated Press, *Actress Bares All in Santiago Glass House*, CNN.COM, Jan. 26, 2000 <http://cnn.com/2000/WORLD/americas/01/26/chile.glass.house.ap/> (describing actress "spending two weeks in a house in central Santiago made of nothing but glass").

11. *See generally* DAVID BRIN, THE TRANSPARENT SOCIETY (1998).

12. *See, e.g.*, U.S. GAO, GOVERNMENT AND COMMERCIAL USE OF THE SOCIAL SECURITY NUMBER IS WIDESPREAD 1 (1999) (Letter Report, GAO/HEHS-99-28) <http://frwebgate.access.gpo.gov/cgi-bin/useftp.cgi?IPaddress=162.140.64.88&filename=he99028.pdf&directory=/diskb/wais/data/gao> (noting "the SSN is used for a myriad of non-Social Security purposes, some legal

show confessionals and other forms of media-sanctioned exhibitionism and voyeurism,[13] it may seem reactionary to worry about informational privacy. It also may be that mass privacy is a recent invention, rarely experienced before the nineteenth century save in the hermitage or on the frontier.[14] 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, and the benefits of mass surveillance and profiling outweigh the costs. Nevertheless, in this article I will assume that informational privacy is a good in itself,[15] and a value worth protecting,[16] although not at all costs.[17]

---

and some illegal"); Flavio L. Komuves, *We've Got Your Number: An Overview of Legislation and Decisions to Control the Use of Social Security Numbers as Personal Identifiers*, 16 J. MARSHALL J. COMPUTER & INFO. L. 529, 535 (1998) ("SSN use is so important to business and government in this country that a person who is assertive about their privacy rights may find herself in a position in which another will refuse to do business with her unless she furnishes her SSN.").

13. The phenomenon is everywhere, from the Starr Report to confessional talk shows, from mainstream films to the Internet's 24×7 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, 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, 274 (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 innermost details of others' lives without fear of legal repercussion"); Andrew Leonard, *Microsoft.orgy*, SALON, July 21, 1998 <http://www.salon.com/21st/feature/1998/07/cov_21feature.html> (describing how exhibitionists turned the Microsoft NetMeeting server, which provides means for PC cam video conferencing, into "a 24-hour international sex orgy").

14. 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* JÜRGEN 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 MOORE 255-56 (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.

15. 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). Treating privacy as an intermediate good, then-Professor Posner concluded that personal privacy is generally inefficient, because 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. *See id.* Useful correctives to Posner's views include KIM LANE SCHEPPELE, LEGAL SECRETS: EQUALITY AND EFFICIENCY IN THE COMMON LAW 43-53, 111-26 (1988); James Boyle, *A Theory of Law and Information: Copyright, Spleens, Blackmail, and Insider Trading*, 80 CAL. L. REV. 1413, 1443-57, 1471-77 (1992), and

I. PRIVACY-DESTROYING TECHNOLOGIES

Privacy-destroying technologies can be divided into two categories: those that facilitate the acquisition of raw data and those that 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 clerks, secretaries, and even executives. It also makes it possible to monitor their web browsing habits.[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 characteristics of individuals about whom data is being gathered (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 either governmental or private, although here

---

Edward J. Bloustein, *Privacy Is Dear at Any Price: A Response to Professor Posner's Economic Theory*, 12 GA. L. REV. 429 (1978).

16. Readers needing persuasion on this point should consult Part I of Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1202-20 (1998).

"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%." *See also* 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. In a recent survey, 80% of United States residents, 68% of Britons, and 79% 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, 59%, 63%, and 55% of Americans, Britons, and Germans respectively also agreed that existing laws and organization practices in the their country provide a reasonable level of consumer privacy protection. IBM, IBM MULTI-NATIONAL CONSUMER PRIVACY SURVEY 22 (1999) <http://ibm.com/services/files/privacy_survey_oct991.pdf>. In a different survey, 92% of Canadians expressed some concern, and 52% were "extremely concerned" about privacy. John D.R. Craig, *Invasion of Privacy and Charter Values: The Common-Law Tort Awakens*, 42 MCGILL L.J. 355, 357 (1997).

17. Due to limitations of space, and of my knowledge, this article also adopts an artificially United States-centric focus, although the problems discussed here are of global importance.

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, *Cyberveillance at Work: Surfing the Wrong Internet Sites on the Job Could Get You Fired*, CNN.COM, Jan. 4, 2000 <http://www.cnnfn.com/2000/01/04/technology/webspy/>; *cf.* Eugene Volokh, *Freedom of Speech, Cyberspace, Harassment Law, and the Clinton Administration*, LAW & CONTEMP. PROBS. (forthcoming 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).

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 examples 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, cameras have a far less intrusive effect on privacy if their only use is to be monitored in real time by 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 can be searched or integrated into personal profiles. Equally important, 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.

Reams 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 possible harmful effects are various forms of discrimination, ranging from price discrimination to more invidious sorts of discrimination.[20] Data accumulation enables the construction of personal data profiles.[21] When the data are available to others, they

---

19. *See* ANN CAVOUKIAN, INFO. AND PRIVACY COMM'R/ONTARIO DATA MINING: STAKING A CLAIM ON YOUR PRIVACY (1998) <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 visualization.

Id. (citations omitted) (quoting JOSEPH P. BIGUS, DATA MINING WITH NEURAL NETWORKS 9 (1996)).

20. *See* OSCAR H. GANDY, JR., THE PANOPTIC SORT 91 (1993); Oscar H. Gandy, Jr., *Legitimate Business Interest: No End in Sight? An Inquiry into the Status of Privacy in Cyberspace*, 1996 U. CHI. LEGAL F. 77.

21. *See* Kang, *supra* note 16, at 1239.

can construct personal profiles for targeted marketing,[22] and even, in rare cases, blackmail.[23] For some, just knowing that their activities are being recorded may have a chilling effect on conduct,[24] speech, and reading.[25] 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,[26] but it also gains new techniques for detecting crimes

---

22. *See* 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):

> [Y]ou 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.

23. *See* Phil Agre, *RRE Notes and Recommendations*, RED ROCK EATER NEWS SERVICE, Dec. 26, 1999 <http://commons.somewhere.com/rre/1999/RRE.notes.and.recommenda14.html>:

> 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 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 [has] been predicting their movements using commercially available movement patterns.

24. 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 <http://www.Aristo.org>, a firm that offered to target web users by matching web browsing habits and web site signup data with voter registration records. *See* Lauren Weinstein, *Web Tracking and Data Matching Hit the Campaign Trail*, PRIVACY FORUM DIGEST, Dec. 24, 1999 <http://www.vortex.com/privacy/priv.08.22>.

25. Of course, disclosure also helps prevent evils that 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, 404-07, 410-11 (1996).

26. *See* Financial Crimes Enforcement Network ("FinCEN"), FINCEN FOLLOWS THE MONEY: A LOCAL APPROACH TO IDENTIFYING & TRACKING CRIMINAL PROCEEDS 5 (1999), <http://www.treas.gov/fincen/followme.pdf>. Approximately 200 staffers plus 40 "long-term detailees" from 21 other regulatory and law enforcement agencies use financial, law enforcement, and

and identifying suspects.[27] 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.[28] At 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 in order to predict dangerous or antisocial activities before they happen. People whose profiles meet the criteria will be flagged as dangerous and perhaps subjected to increased surveillance, searches, or discrimination. Profiling is currently used to identify airline passengers who the profilers think present an above-average risk of being terrorists.[29] In the wake of the tragedy at Colombine, schools are turning to profiling to assess children for potential violence.[30] In a world where such

---

commercial databases to operate FinCEN. *See id*. at 3. Working with foreign "financial intelligence units," FinCEN formed the "Egmont Group," an international cooperation designed to exchange information and expertise. *See id*. at 6.

27. *See* FinCEN, HELPING INVESTIGATORS USE THE MONEY TRAIL <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).

28. *See, e.g*., David Cay Johnston, *New Tools for the I.R.S. to Sniff Out Tax Cheats*, NY TIMES, Jan. 3, 2000, <http://www.nytimes.com/00/01/03/news/financial/irs-tax.html> ("The [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."); *see also* Steven A. Bercu, *Toward Universal Surveillance in an Information Age Economy: Can We Handle Treasury's New Police Technology?*, 34 JURIMETRICS J. 383, 400-01 (1994) (discussing FinCEN and possible privacy problems).

29. Air travelers are profiled by a $2.8 billion monitoring system that uses a secret algorithm to compare their personal data to profiles of likely terrorists. *See* Declan McCullagh, *You? A Terrorist? Yes!*, WIRED, Apr. 20, 1999 <http://www.wired.com/news/news/politics/story/19218.html>:

> The CAPS [computer-assisted passenger screening] system operates off the computer reservation systems utilized by the major United States air carriers as well as some smaller carriers. The CAPS system relies solely on information that passengers presently provide to air carriers for reasons unrelated to security. It does not depend on the gathering of any additional information from air travelers, nor is it connected to any law enforcement or intelligence database.

Security of Checked Baggage on Flights Within the United States, 64 Fed. Reg. 19220, 19222 (1999) (to be codified at 14 C.F.R. pt. 108) (proposed Apr. 19, 1999).

30. Examples of this profiling in the wake of the Columbine shootings include a psychological tool being offered by the FBI to identify "potentially violent" schoolchildren, *see* Jon Katz, *Take the FBI's Geek Profile Test*, SLASHDOT, Nov. 29, 1999 <http://slashdot.org/features/99/11/23/1712222.shtml>, and Mosaic-2000, a profiling tool developed by the Bureau of Alcohol, Tobacco, and Firearms, *see* Frances X. Clines, *Computer Project Seeks to Avert Youth Violence*, N.Y. TIMES, Oct. 24, 1999. *See also Software to Predict "Troubled Youths,"* SLASHDOT, Oct. 24, 1999 <http://slashdot.org/yro/99/10/24/1147256.shtml> (open discussion of Mosaic-2000); Gavin de Becker Inc., MOSAIC-2000 (1999) <http://www.gdbinc.com/mosaic2000.htm> (analysis of Mosaic-2000).

profiling is common, who will dare to act in a way that will cause red flags to fly?

In a thorough survey, Roger Clarke suggested that the collection and collation of large amounts of personal data create 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[31]

There is little reason to believe that the nosiness of neighbors, employers, or governments has changed recently. What is changing very rapidly, however, 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 that privacy is becoming impossible.

A. *Routinized Low-Tech Data Collection*

Large quantities of personal data are routinely collected in the United States today without 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.

---

31. Clarke, *supra* note 9.

1. *By the United States government.*

The most comprehensive, legally mandated United States 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.[32] 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.[33]

Anyone who takes a new job must be listed in the "new hires directory" designed to support the Federal Parent Locator Service.[34] This growing national database of workers enables 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 the Department of Health and Human Services.[35] Anyone receiving public assistance is likely to be in a state maintained database of aid recipients. Federal, state, and local governments also collect data from a total of about fifteen million arrestees each year.[36] The government continues to collect (and publish) data about some convicts even after they have served their sentences.[37]

License applications are formally optional data collections that have wide application—licenses are optional, but if one wants a license, one must answer the required questions. Perhaps the most widespread data collection comes from driver's license applications, as most of the United States adult

---

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 identify 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 the 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).

33. *See generally* Lillian R. Bevier, *Information About Individuals in the Hands of Government: Some Reflections on Mechanisms for Privacy Protection*, 4 WM. & MARY BILL RTS. J. 455 (1995) (discussing government's use of data provided by citizens).

34. 42 U.S.C. § 653 (1996).

35. *See* Department of Health and Human Services, *What is NECSRS?* <http://ocse.acf.dhhs.gov/necsrspub/Navigation/Questions/Ques.htm#NECSRS1> (stating that the "National Electronic Child Support Resource System . . . is used to identify and electronically index Federal, State, and local resource materials").

36. See Electronic Privacy Information Center ("EPIC"), *Reno Proposes National DNA Database*, EPIC ALERT, Mar. 4, 1999 <http://www.epic.org/alert/EPIC_Alert_6.04.html>.

37. *See* Megan's Law, N.J. STAT. ANN. § 2C:7-1 to 7-11 (West 1999) (registration of sex offenders); Violent Crime Control and Law Enforcement Act of 1994, Pub. L. No. 103-322, 108 Stat. 2038 (1994) (codified as amended at 42 U.S.C.A. § 14071 (West Supp. 1999)) (federal equivalent of Megan's Law).

population hold driver's licenses, at least outside the 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.

2. *Transactional data.*

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) involved in the transaction.

Financial data collection is an interesting example of the private sector collecting data for mixed motives. A single firm, Acxiom, now holds personal and financial information about almost every United States, United Kingdom, and Australian consumer.[38] In many cases, banks and other financial service providers collect information about their clients because the data has commercial value. In other cases, they record data because the government requires them to make routine reports to assist law enforcement efforts. In effect, private banks often act as agents of state data collection efforts.

Until machines for tracking bills by their serial numbers become much more common than today, cash payment will remain relatively anonymous. In their quest to gather personal data about customers, merchants have turned to loyalty reward programs, such as frequent shopper cards and grocery club cards. Depending upon 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 means 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 because of their location in neighborhoods thought by law enforcement to be high drug trading zones, must report transactions involving as little as $750 in cash.[39]

---

38. *See* Ian Grayson, *Packer Sets up Big Brother Data Store*, AUSTRALIAN, Nov. 30, 1999 <http://technology.news.com.au/news/4277059.htm>.

39. *See* Financial Action Task Force on Money Laundering, 1997-1998 REPORT ON MONEY LAUNDERING TYPOLOGIES ¶ 28 <http://www.ustreas.gov/fincen/typo97en.html> (noting imposition of Geographic Targeting Orders pursuant to Banking Secrecy Act that required certain money transmitters to report all cash transfers to Columbia of over $750 during 360-day period).

Alternatives to cash, such as checks, debit cards, and credit cards, 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 secure and anonymous or create a digital data trail linking every transaction to the parties involved depends entirely on how such an 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.[40] Because 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 and recorded during any sustained interaction with the United States health care system. In addition to being shared among various health care providers, the information is also shared with the entities that administer the system.[41] Under the "Administrative Simplification" provision of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"),[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 collected about almost everyone in the country. The introduction of new technologies, however, promises to raise the quantity and

---

40. *See* Froomkin, *supra* note 25, at 449-79.

41. As a result, health care related data will be part of a giant distributed database. *See generally* Paul M. Schwartz, *Privacy and the Economics of Personal Health Care Information*, 76 TEX. L. REV. 1 (1997); Paul M. Schwartz, *The Protection of Privacy in Health Care Reform*, 48 VAND. L. REV. 295 (1995); Spiros Simitis, *Reviewing Privacy in an Information Society*, 135 U. PA. L. REV. 707 (1987); *see also* U.S. GAO, MEDICAL RECORDS PRIVACY: ACCESS NEEDED FOR HEALTH RESEARCH, BUT OVERSIGHT OF PRIVACY PROTECTIONS IS LIMITED, GAO/HEHS-99-55 (1999) <http://www.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=gao&docid=f:he99055.txt.pdf>.

HHS is expected to issue medical privacy regulations by February 21, 2000, defining rules for the security and disclosure of health care data. The draft regulations allow disclosure of health information without an individual's authorization for research, public health, oversight, and some other purposes; otherwise written authorization is required. Databases must be kept secure. Collectors of medical data must conform to fair information practices, inform people how their information is used and disclosed, and ensure that people can view information being held about them. The draft rules propose that their protections would attach as soon as information is "electronic" and run with the information as long as the information is in the hands of a covered entity. The proposed rules do not, however, apply to downstream recipients of medical data. *See* NPRM HHS, Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. 59,918 (1999), <http://aspe.hhs.gov/admnsimp/pvcnprm.pdf> (technical corrections available in <http://aspe.hhs.gov/admnsimp/nprm/991215fr.pdf>).

42. Health Insurance Portability and Accountability Act, Pub. L. No. 104-191, § 264, 110 Stat. 1936 (1996) (codified as amended at 42 U.S.C. § 1320d- 2).

nature of the information that could be collected to new, somewhat dizzying, heights.

B. *Ubiquitous Surveillance*

Unless social, legal, or technical forces intervene, it is conceivable that there will be no place on earth where an ordinary person will be able to avoid surveillance. In this possible future, 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 subject to sense-enhanced viewing. All communications, save perhaps some encrypted messages, will be scannable and sortable. Copyright protection "snitchware"[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 observed by camera, but also anything involving computer use will be subject to detailed monitoring, analyzed for both efficiency and inappropriate use. As the cost of storage continues to drop, enormous databases will be created, or disparate distributed databases linked, allowing data to be cross-referenced in increasingly sophisticated ways.

In this very possible future, indeed perhaps in our present,[44] there may be nowhere to hide and little that can stay hidden.

1. *Public spaces.*

Moving about in public is not truly anonymous: Someone you know may recognize you, and 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 with anonymity. 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 technology for routinely monitoring public spaces and identifying individuals. Monitoring

---

43. *See* note 110 *infra* and accompanying text.

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").

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.

a. *Cameras*.

Perhaps the most visible way in which spaces are monitored is the increasingly ubiquitous deployment of Closed Circuit Television ("CCTV") cameras and video recorders. Monitoring occurs in both public and private spaces. 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 United States,[45] they are even more widespread abroad. Perhaps because of fears of IRA terrorism, in addition to 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 Bournemouth, covering a coastal path."[46] Cameras are also commonly used on the roads to enforce speed limits by taking photos of speeding vehicles' license plates. 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 antisocial behaviors.[47]

Cameras can also be placed in the office, school, and home. Visible cameras allow parents to keep an eye on junior at day care. Hidden cameras can be concealed in "clocks, radios, speakers, phones, and many other items"[48] to monitor caregivers and others in the home.

Cameras are also an example of how technologies can interact with each other to multiply privacy-destroying effects. All of 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 way to identify the people in them. Thus, for example, the London Police obtained excellent quality photographs

---

45. *See, e.g.*, Timothy Egan, *Police Surveillance of Streets Turns to Video Cameras and Listening Devices*, N.Y. TIMES, Feb. 7, 1996, at A12 (detailing the methods and equipment of several cities' police departments).

46. Nick Taylor, *Closed Circuit Television: The British Experience*, 1999 STAN. TECH. L. REV. VS 11, ¶ 1 <http://stlr.stanford.edu/STLR/Symposia/Privacy/99_VS_11/article.html>.

47. *See id.* ¶¶ 12-14.

48. Hidden Cameras Solutions, *Catalogue* <http://www.concealedcameras.com/catalogue/main.html>.

of alleged participants in a violent demonstration in the City of London on June 18, 1998, but had to post the photographs on the Internet and ask viewers for help in identification—it worked in some cases.[49]

Human monitors are expensive and far from omniscient.[50] In the near future, however, human observers will become much less important as the task of analyzing 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.[51] In public, however, more sophisticated technologies, such as facial recognition technology, are needed to identify people. Facial recognition technology is becoming better and more reliable every year.[52] Current systems are already capable of picking out 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.[53] The Israeli government plans to use facial recognition technology in the hope of creating "Basel," an automated border-crossing system.[54] The United States Pentagon is also investigating the possibility of using facial recognition systems to identify potential terrorists outside military facilities.[55]

Once mated with, for example, a database full of driver's license photos, images from a series of ubiquitous cameras could be indexed by name and stored for an indefinite period of time. (Indeed, the United States 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

---

49. *See* City of London Police, *Your Help Is Needed . . .*, June 18, 1999 <http://www.cityoflondon.gov.uk/citypolice/j18frame.htm>; City of London Police, *Identity Parade*, June 18, 1999, <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, ¶¶ 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 a teacher objected to a bar code because he believed it to resemble the "mark of the beast"); Americans United For Separation of Church and State, *Teacher Who Fears "Mark of the Beast" Fired in West Virginia*, CHURCH & STATE: AU BULL., Mar. 1999 <http://www.au.org/cs3991.htm>.

52. *See, e.g.*, VISIONICS, CORP., FACEIT: AN AWARD-WINNING FACIAL RECOGNITION SOFTWARE ENGINE <http://www.visionics.com/Newsroom/PDFs/Visionics_Tech1.pdf> (describing one such system); Taylor, *supra* note 47, ¶ 39 (citing TIMES (London), Oct. 15, 1998).

53. Alex Richardson, *TV Zooms in on Crooks' 'Faceprints,'* BIRMINGHAM POST, Oct. 15, 1998, *available in* 1998 WL 21493173. For some reason, the police chose to test the system in the poorest part of London. *See* Taylor, *supra* note 46.

54. *See* Visionics Corp., *Visionics' Face Recognition Technology Chosen For Cutting Edge Israeli Border Crossing*, Sept. 21, 1999 <http://www.visionics.com/Newsroom/PRs/bazel1.htm>.

55. *See* Daniel J. Dupont, *Seen Before*, SCI. AM., Dec. 1999 <http://www.sciam.com/1999/1299issue/1299techbus5.html>.

helping a private corporation amass the data.)[56] Assuming the index and the videos are at least subject to subpoena (or perhaps the Freedom of Information Act) or even routinely placed on the Internet, alibis, mystery novels, and divorce proceedings will never be the same. One's face will nonetheless become an index marker. Devices will be available that warn you every time an individual 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 still, once you enter, the store will be able to determine which merchandise to show you and how much to charge.[57]

b. *Cell phone monitoring*.

Many people can be tracked today without the use of 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 its user every few minutes (within 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.[58]

The finer the cell phone zone, the more precisely a person's location can be identified. In the United States, a Federal Communications Commission ("FCC") regulation due to become effective in 2001 requires all United States 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.[59] The original objective of the rule was

---

56. *See* IMAGE DATA, LLC, APPLICATION OF IDENTITY VERIFICATION AND PRIVACY ENHANCEMENT TO TREASURY TRANSACTIONS: A MULTIPLE USE IDENTITY CRIME PREVENTION PILOT PROJECT 3 (1997) <http://www.epic.org/privacy/imagedata/image_data.html> (document submitted to United States Secret Service proposing to "show the technical and financial feasibility of using remotely stored digital portrait images to securely perform positive identification"); Brian Campbell, *Secret Service Aided License Photo Database*, CNN.COM, Feb. 18, 1999 <http://www.cnn.com/US/9902/18/license.photos/>.

57. *See generally* J. Bradford DeLong & A. Michael Froomkin, *Speculative Microeconomics for Tomorrow's Economy*, *in* INTERNET PUBLISHING AND BEYOND: THE ECONOMICS OF DIGITAL INFORMATION AND INTELLECTUAL PROPERTY (Brian Kahin & Hal Varian eds., forthcoming 2000) <http://www.law.miami.edu/~froomkin/articles/spec.htm>.

58. *See* Alan Sipress, *Tracking Traffic by Cell Phone: Md., Va. to Use Transmissions to Pinpoint Congestion*, WASH. POST, Dec. 22, 1999, at A1 (stating that Maryland and Virginia will track "anonymous" callers on highways to measure speed of traffic).

59. *See* 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

to allow emergency 911 calls 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 that they should be entitled to all location information available to the carrier.[60]

Governments are not the only ones who want to know where people are. Parents could use cell phone tracking to locate their children (or where they left the phone). Merchants are also interested in knowing who is in the neighborhood. A United Kingdom 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.[61]

The privacy-destroying consequences of cell phone tracking increase dramatically when movement is archived. It is one thing to allow police to use the data to track a fugitive in real time. It is another thing to archive the data, perhaps even in perpetuity, in case police or others wish to reconstruct someone's movements. In 1997, a Swiss newspaper revealed that a local phone company kept information recording the movement of one million subscribers, accurate to within a few hundred meters, and that the data was stored for more than six months. Swiss police described the data as a treasure trove.[62] However atypical the collection and retention of cellular phone subscribers' movements may be, the Swiss phone company's actions are clearly not unique.[63] The Swiss government, at least, values this locational data so highly 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

---

user can then relay to the 911 operator, but only if the user is able to speak. *See* Steve Ginsberg, *Cell Phones Get a Homing Device*, S.F. BUSINESS TIMES, Sept. 28, 1998 <http://www.amcity.com/sanfrancisco/stories/1998/09/28/focus7.html>.

60. *See* FCC, Third Report and Order in the Matter of Communications Assistance for Law Enforcement Act, CC Docket No. 97-213, ¶¶ 12, 21, 22, Aug. 26, 1999 <http://www.fcc.gov/Bureaus/Engineering_Technology/Orders/1999/fcc99230.wp>.

61. *See Watching Me, Watching You*, BBC NEWS, Jan. 4, 2000 <http://newsvote.bbc.co.uk/hi/english/uk/newsid_590000/590696.stm>.

62. *See* Daniel Polak, *GSM Mobile Network in Switzerland Reveals Location of its Users*, PRIVACY FORUM DIGEST, Dec. 31, 1997 <http://www.vortex.com/privacy/priv.06.18>.

63. *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 Hazard: Little Privacy in Billing Records*, WALL ST. J., Mar. 16, 1999, at B1 (stating that AT&T wireless unit fields roughly 15,000 subpoenas for phone records per year).

Swiss cell phone users to buy prepaid phone cards that 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.[64]

c. *Vehicle monitoring*.

Automobiles 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.[65] Ultimately, ITS promise continuous, real-time information as to the location of all moving vehicles.[66] Less complex systems already create travel records that can be stored and accessed later.[67] Some countries have also considered putting bar codes on license plates to ease vehicle identification.[68] While it is possible to design ITS in a manner that preserves the traveler's anonymity,[69] this has not been the norm.

2. *Monitoring in the home and office*.

Staying home may be no defense against monitoring and profiling. Existing technology can monitor every electronic communication, be it a telephone call, fax, or email. In the United States, 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 ever-increasing volume of communications will be subjected to increasingly sophisticated automated processing.[70]

---

64. *See* Gabriel Sigrist, *Odilo Guntern: Le Détenteur de Natel Doit Pouvoir Rester Anonyme*, LE TEMPS July 7, 1998 <http://www.inetone.com/cypherpunks/dir.98.07.1398.07.19/msg00084.html>.

65. *See generally Santa Clara Symposium on Privacy and IVHS*, 11 SANTA CLARA COMPUTER & HIGH TECH. L.J. 1 (1995) (dedicated to privacy and "intelligent vehicle highway systems").

66. *See* Margaret M. Russell, *Privacy and IVHS: A Diversity of Viewpoints*, 11 SANTA CLARA COMPUTER & HIGH TECH. L.J. 145, 163 (1995).

67. *See id*. at 164-65.

68. *See* Andrew Sparrow, *Car Tagging May Help Cut Theft, Says Minister*, DAILY TELEGRAPH (London), Oct. 17, 1998, *available in* 1998 WL 3053349.

69. *See, e.g.*, ONTARIO INFO. AND PRIVACY COMM'R, 407 EXPRESS TOLL ROUTE: HOW YOU CAN TRAVEL THIS ROAD ANONYMOUSLY (1998) <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.").

70. *See, e.g.*, University of Southern California, *Novel Neural Net Recognizes Spoken Words Better Than Human Listeners*, SCI. DAILY MAG., Oct. 1, 1999 <http://www.sciencedaily.com/releases/1999/10/991001064257.htm> (announcing advance in machine recognition of human speech).

Meanwhile, a number of legal technologies are already being deployed to track and archive many uses of the web.

a. *Workplace surveillance*.

Outside of restrooms, and the few laws banning wiretapping and reading email during transmission,[71] there are relatively few privacy protections applicable to every workplace in the nation.[72] Thus, employers may use hidden cameras, monitoring software, and other forms of surveillance more or less at will.[73] A 1993 survey, taken long before surveillance technology got cheap, showed that twenty million workers were subject to monitoring of their computer files, voice and electronic mail, and other networking communications.[74] Today, digital cameras are so small they fit on a one-inch by two-inch chip. Miniaturization lowers costs, which are expected to fall to only a few dollars per camera.[75] 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 one hundred dollars and, once installed on the target PC, covertly monitors everything that it does and routinely emails detailed reports to the boss.[76] In addition, every technology described below that can be targeted at the home can also be targeted at the office.

b. *Electronic communications monitoring*.

According to a report prepared for the European Parliament, the United States and its allies maintain a massive worldwide spying apparatus capable

71. *See* Electronic Communications Privacy Act, 18 U.S.C. §§ 2510-2710 (1968).

72. *See* 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.").

73. Covert video surveillance violates some states' laws. *See* Quentin Burrows, *Scowl Because You're on Candid Camera: Privacy and Video Surveillance*, 31 VAL. U. L. REV. 1079, 1114-21 (1997) (collecting cases and statutes).

74. *See* Gary Marx, *Measuring Everything That Moves: The New Surveillance at Work* <http://web.mit.edu/gtmarx/www/ida6.html>.

75. *See* Daniel Grotta & Sally Wiener Grotta, *Camera on a Chip*, ZDNET PC MAG, Oct. 7, 1999 <http://www.zdnet.com/pcmag/stories/trends/0,7607,2349530,00.htm>.

76. *See* Stuart Glascock, *Stealth Software Rankles Privacy Advocates*, TECHWEB, Sept. 9, 1999 <http://www.techweb.com/wire/story/TWB19990917S0014>.

of capturing all forms of electronic communications.[77] Known as "Echelon," the network can "access, intercept and process every important modern form of communications, with few exceptions."[78] 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.[79] Similarly, text messages such as faxes and emails can be run through so-called dictionary programs that flag messages with interesting references or word patterns.[80] As artificial intelligence improves, these programs should become increasingly sophisticated. Meanwhile, advances in voice recognition (translating speech into text) promise to transform the telephone monitoring problem into another type of text problem. Further, once a 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 procedure that produces a topical summary of a conversation using a "tree-word-list" to score the text. The patent describes a "preprocessing" phase that removes "stutter phrases" from a transcript. Then, a computer automatically assigns a label, or topic description, to the text.[81] The method promises to allow computerized sorting and retrieval of transcripts and other documents based upon their meaning, not just keywords.[82]

Not only have the communications intelligence agencies of the United States and its major allies "reaffirmed their requirements for access to all the world's communications,"[83] but 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 monitor and collect traffic at nine major Internet exchange points.[84] On May 7, 1999, the European Parliament passed the Lawful Interception of Communications Resolution on New Technologies,[85] known as Enfopol.

---

77. *See* DUNCAN CAMPBELL, DEVELOPMENT OF SURVEILLANCE TECHNOLOGY AND RISK OF ABUSE OF ECONOMIC INFORMATION: AN APPRAISAL OF TECHNOLOGIES FOR POLITICAL CONTROL (1999) <http://jya.com/ic2000-dc.htm> [hereinafter STOA REPORT].

78. *Id*. at Summary ¶ 2.

79. "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 deployed to recognise [sic] the speech of targeted individuals making international telephone calls." *Id*. at Summary ¶ 7.

80. *See id*. § 3 ¶ 72.

81. *See* Patent 5937422: Automatically generating a topic description for text and searching and sorting text by topic using the same <http://cryptome.org/nsa-vox-pat.htm>.

82. *See* Suelette Dreyfus, *This Is Just Between Us (and the Spies)*, INDEPENDENT, Nov. 15, 1999 <http://www.independent.co.uk/news/Digital/Features/spies151199.shtml>.

83. STOA REPORT, *supra* note 77, §1, ¶ 6.

84. *See id*. § 2, ¶ 60.

85. European Parliament, Legislative resolution embodying Parliament's opinion on the draft Council Resolution on the lawful interception of telecommunications in relation to new technologies (10951/2/98-C4-0052/99-99/0906 (CNS)) (Consultation procedure) <http://www2.europarl.eu.

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 position information locating their cell phone customers. If the service provider offers encryption as part of the cell phone service, the provider would be required to ensure that it be able to decode the messages.[86]

Similarly, in the United States, 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.[87] The legislation also does not specify how many simultaneous wiretaps the network should be able to support, leaving this to the implementing regulations. In its initial assessment of "capacity requirements," the FBI proposed requiring carriers in major urban areas to install a maximum surveillance capacity of one percent of "engineered capacity"—in other words, to make it possible for a maximum of one out of every one hundred phone lines to be monitored simultaneously.[88] This proposal was so controversial that the FBI withdrew it and substituted a different capacity projection.[89] 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

---

int/omk/omnsapir.so/pv2?PRG=DOCPV&APP=PV2&LANGUE=EN&SDOCTA=5&TXTLST=1&POS=1&Type_Doc=RESOL&TPV=PROV&DATE=070599&PrgPrev=PRG@TITRE|APP@PV2|TYPEF@TITRE|YEAR@99|Find@%69%6e%74%65%72%63%65%70%74%69%6f%6e|FILE@BIBLIO99|PLAGE@1&TYPEF=TITRE&NUMB=2&DATEF=990507>. As of March 2000, European governments had yet to reach a final agreement on Enfopol due to disputes regarding its application to bank secrecy rules. *See* Jelle van Buuren, *No Final Agreement on Convention on Mutual Assistance in Criminal Matters*, Mar. 28, 2000 <http://www.heise.de/tp/english/special/enfo/6691/1.html>.

86. *See* Madeleine Acey, *Europe Votes for ISP Spying Infrastructure*, TECHWEB, May 13, 1999 <http://www.techweb.com/wire/story/TWB19990513S0009>.

87. *See* 1994 Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified as amended at 47 U.S.C §§ 1001-1010 and scattered sections of 18 & 47 U.S.C.); *cf.* James X. Dempsey, *Communications Privacy in the Digital Age: Revitalizing the Federal Wiretap Laws to Enhance Privacy*, 8 ALB. L.J. SCI. & TECH. 65 (1997) (arguing that recent changes in communications technology have required reexamination of privacy policy).

88. *See* 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 assessment 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. *See id.*

89. *See* Implementation of Section 104 of the Communications Assistance for Law Enforcement Act, 62 Fed. Reg. 1902 (proposed Jan. 14, 1997).

proposed by the FBI, the system would have to be able to perform 136,000 simultaneous intercepts in the Los Angeles area alone.[90]

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.[91] State and federal courts authorized 1329 wiretaps in 1998, an increase of eighty percent over the 738 authorized a decade earlier.[92] These statistics are somewhat misleading, however, because a single wiretap order can affect hundreds of phone lines and up to 100,000 conversations.[93] The statistics are also difficult to reconcile with reports, attributed to the FBI, that on peak days up to one thousand different telephone lines are tapped in the Los Angeles area.[94] Although the number of wiretap orders is increasing, and the number of persons subject to legal eavesdropping is also increasing, these statistics are 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 attributable to paying the people who listen to the calls. However, as technology developed by intelligence agencies trickles down to domestic law enforcement, the marginal cost of telephone, fax, and email surveillance should decline considerably. Even if domestic law enforcement agencies remain scrupulously within

---

90. *See* Center for Democracy and Technology, Brief of Amicus Curiae, Cellular Telecomms. Indus. Ass'n v. United States Tel. Ass'n, No. 1:98CV01036 & 1:98CV0210 (D.D.C. 1999) <http://www.cdt.org/digi_tele/capacitybrief.shtml>; Center for Democracy and Technology, *Comments on the FBI's Second CALEA Capacity Notice*, Feb. 18, 1997 <http://www.cdt.org/digi_tele/970218_comments.html>.

91. Warrants are not required abroad, either when the United States is wiretapping foreigners, *see, e.g.*, United States v. Rene Martin Verdugo-Urquidez, 494 U.S. 259 (1990) (holding that the Fourth Amendment does not apply to the search and seizure, by United States agents, of property owned by a nonresident alien and located in a foreign country), or even when democratic foreign governments are wiretapping their own citizens. *See, e.g.*, Nick Fielding & Duncan Campbell, *Spy Agencies Listened in on Diana*, SUNDAY TIMES (London), Feb. 27, 2000 <http://www.the-times.co.uk/news/pages/sti/2000/02/27/stinwenws02035.html?999> (alleging that "a loophole in the 1985 Interception of Communication Act means intelligence officials can put individuals and organisations [sic] under surveillance without a specific ministerial warrant").

92. *See* ADMINISTRATIVE OFFICE OF THE U.S. COURTS, 1998 WIRETAP REPORT 5 (1999) <http://www.uscourts.gov/wiretap98/contents.html;> Associated Press, *State Authorities' Wiretapping Up*, May 5, 1999 <http://jya.com/wiretap98.htm>.

93. *See* Marc Cooper, *Wired*, NEWSTIMESLA.COM., Jan. 23, 1998 <http://www.newtimesla.com/archives/1998/081398/feature1-2.html> ("Under the single wiretap 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.

the law,[96] the number of legal wiretaps is likely to increase rapidly once the cost constraint is reduced.[97]

c. *Online tracking*.

The worldwide web is justly celebrated as a cornucopia of information available to anyone with an Internet connection. The aspects of the web that make it such a powerful information medium (its unregulated nature, the flexibility of browsing software and the underlying protocols, and its role as the world's largest library, shopping mall, and chat room) all combine to make the web a fertile ground for harvesting personal data about Internet surfers. The more that people rely on the web for their reading and shopping, the more likely it becomes that data about their interests, preferences, and economic behavior will be captured and made part of personal profiles.

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 or email address in the browser's communication software that too will be disclosed automatically.[98] These features cannot be turned off—they are part of the hypertext transfer protocol—although one can delete one's name and email address from the software. Web surfers can, however, employ privacy-enhancing tools such as the anonymizer to mask personal information.[99]

The default setting on the two 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 to write data a user's hard drive.[100] Often this works to the user's advantage—stored passwords eliminate the need to memorize or retype passphrases. Preference information allows a web designer to customize web pages to match

96. There is reason to doubt that they do. *See, e.g.*, Cooper, *supra* note 93 (describing LAPD officers' testimony concerning hundreds of illegal "hand offs" of information, acquired in one wiretap, in order to initiate new cases via fictitious informants); Los Angeles Public Defenders Office, *State Wiretap Related Cases* <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 to privately gather caller information. For example, British Telecom searched its records to find people who were regularly calling competing Internet service providers, and had its sales staff call and encourage them to switch to BT. *See* Office of Telecomms., *OFTEL Acts to Ensures Fair Competition in Marketing of BT Click Internet Services*, Sept. 24, 1998 <http://www.worldserver.pipex.com/coi/depts/GOT/coi6043e.ok?> (announcing OFTEL had forced BT to cease practice after complaints).

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

99. *See Anonymizer* <http://www.anonymizer.com/3.0/index.shtml>.

100. *See generally* Netscape, *Cookie Central* <http://www.cookiecentral.com/>.

individual users' tastes. But the process is usually invisible; and even when made visible, it 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. If taken to its limit, this would permit a particularly intrusive site to build a dossier on the user. An online newspaper might, for example, keep track of the articles a reader selects, allowing it over time to construct a picture of the reader's interests. Cookies can be shared between web sites, allowing savvy web designers to figure out what other sites their visitors patronize, and (to the extent the other sites store information in cookies) what they have revealed to those other sites. When pieced together, this "clicktrail" can quietly reveal both personal and commercial information about a user without her ever being aware of it. A frequent visitor to AIDS sites, a regular purchaser of anti-cancer medicine, or even someone who has a passion for Barry Manilow, all may have reasons for not wanting others to know of their interests or actions.

Complicating matters, what appears as one page 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 a 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 can assign a unique identifier to each surfer and not only trace which Doubleclick-affiliated web sites they visit, but also when, how often, and what they choose to view while they are there.[101]

Cookies, however, are only the tip of the iceberg. Far more intrusive features can be integrated into browsers, into software downloaded from the Internet,[102] and into viruses or Trojan horses.[103] In the worst case, the software could be configured to record every keystroke.

The United States government suggested that Congress should authorize law enforcement and counter-intelligence agencies to remotely access and plant a back door in suspects' computers.[104] Using a back door could give

---

101. *See* Chris Oakes, *Doubleclick Plan Falls Short*, WIRED NEWS, Feb. 2000 <http://www.wired.com/news/business/0,1367,34337,00.html>.

102. *E.g.*, Chris Oakes, *Mouse Pointer Records Clicks*, WIRED NEWS, Nov. 30, 1999 <http://www.wired.com/news/technology/0,1282,32788,00.html>.

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* <http://wombat.doc.ic.ac.uk/foldoc/foldoc.cgi?query=trojan+horse>.

104. *See* Draft *Cyberspace Electronic Security Act Bill*, Aug. 4, 1999, § 203 (to amend 18 U.S.C. 2713) <http://www.cdt.org/crypto/CESA/draftCESAbill.shtml>. A "back door" is a deliberate hole in system security. *See* FOLDOC, *Back Door* <http://wombat.doc.ic.ac.uk/foldoc/foldoc.cgi?back+door>.

the government access to every keystroke, allowing it to learn passwords and decrypt files protected with strong, otherwise uncrackable, cryptography.[105] The proposal in the original draft of the Cyberspace Electronic Security Act was sufficiently ambiguous that some imagined the government might even contract with makers of popular software to plant back doors that could be activated remotely as part of an investigation.[106] Instead, the clause in question, § 2713, was quickly dropped in the face of furious opposition from civil liberties groups.[107] Other countries have considered similar plans. For example, according to the uncensored version of the Australian Walsh Report,[108] 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.[109]

---

105. *See* Robert O'Harrow, Jr., *Justice Department Mulls Covert-Action Bill*, WASH. POST, Aug. 20, 1999, at A1 <http://www.washingtonpost.com/wp-srv/business/daily/aug99/encryption20.htm>.

106. The DOJ Section by Section analysis of The Cyberspace Electronic Security Act of 1999 (Aug 4, 1999) <http://www.cdt.org/crypto/CESA/CESAanalysis.shtml#secret>, noted that proposed § 2713 allowed a governmental entity to seek a warrant to search not only for data but also "other information necessary to obtain access to the plaintext of data or communications, or to install and use a recovery device." As the DOJ noted, proposed § 2713 defined a "recovery device" as "any enabling or modification of any part of a computer or other system, including hardware or software, that allows plaintext to be obtained even if attempts are made to protect it through encryption or other security techniques or devices." This definition seemed capacious enough to include back doors built into software that could be activated remotely—something that would expose law enforcement agents to far less risk than making surreptitious entry to gain access to the target computer.

107. *See* The Center for Democracy and Technology, *A Briefing on Public Policy Issues Affecting Civil Liberties Online*, CDT POL'Y POST, Sept. 17, 1999, at 22 <http://www.cdt.org/publications/pp_5.22.shtml/#3> (noting change in administration position).

108. For the strange saga of the attempts to censor the Walsh report, see THE WALSH REPORT: REVIEW OF POLICY RELATING TO ENCRYPTION TECHNOLOGIES <http://www.efa.org.au/Issues/Crypto/Walsh/>.

109. *See id.* § 1.2.33.

> Authority should be created for the AFP, the NCA and ASIO to alter proprietary software so that it performs additional functions to those specified by the manufacturer. Such an authority, which clearly should be subject to warranting provisions, would, for example, enable passive access to a computer work station of a LAN and link investigative capability more effectively to current technology. While there are issues of liability, the Review is convinced the effort should be made to accommodate these so that a target computer may be converted to a listening device. This capacity may represent one of the important avenues of accessing plain text.

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 possi-

Monitoring issues also arise in the context of automated intellectual property rights management. Proposals abound for "copyright management technologies" (sometimes unkindly dubbed "snitchware"),[110] which would record and in some cases disclose every time a user accessed a document, article, or even page of licensed material in order to finely assess charges. Similarly, digital watermarking systems,[111] 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 the information with less fear that it will be copied without payment. If the information is sold in encrypted form, along with a program or device that decrypts it every time a licensee wishes to view part of the content, charging can be done on a pay-per-view basis rather than requiring a large fee in advance. Leaving aside the issue of the effect on fair use,[112] monitoring for pricing purposes only raises privacy issues if information is recorded (and thus discoverable or subject to search and seizure) or reported to the licensor. If only the quantity of use is reported, rather than the particular pages viewed or queries run, user privacy is unaffected. When metering is conducted in real time, however, it is particularly difficult for a user to be confident about what is being reported. If, for example, a copyright management system connects via the Internet to the content owner 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. The temptation to create user profiles for marketing purposes may be quite great.

Already, programs that quietly report, to a central registry in real time, every URL viewed 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 construct a database they can use to guide future surfers. But this data, in conjunction with cookies that recorded personal information,

---

> ble, 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.

Id. § 6.2.10.

110. *See generally* Julie E. Cohen, *A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace*, 28 CONN. L. REV. 981 (1996) <http://www.law.georgetown.edu/faculty/jec/read_anonymously.pdf>; Julie E. Cohen, *Lochner in Cyberspace: The New Economic Orthodoxy of "Rights Management,"* 97 MICH. L. REV. 462 (1998) <http://www.law.georgetown.edu/faculty/jec/Lochner.pdf>; Julie E. Cohen, *Some Reflections on Copyright Management Systems and Laws Designed to Protect Them*, 12 BERK. TECH. L.J. 161 <http://www.law.berkeley.edu/journals/btlj/articles/12_1/Cohen/html/text.html>.

111. *See, e.g.*, *Digimark Corp*. <http://www.digimarc.com/>.

112. *See* note 110 *supra*.

could be used to build extensive dossiers of individual users. There is no evidence that Netscape does this, but there is no technical obstacle preventing it.[113]

d. *Hardware*.

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, akin to airplane flight data recorders known as "black boxes," that are able to record crash data. First introduced in 1990, the automobile black boxes have become progressively more powerful. The 1994 versions:

> record[ed] 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.[114]

Other manufacturers include less elaborate data recorders in their cars.

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

Each Intel Pentium III chip has a unique identification number. Intel originally designed the chip ID to function continuously and be accessible to software such as web browsers.[115] The intention appears to have been to make electronic anonymity impossible. Anonymous users might, Intel reasoned, commit fraud or pirate digital intellectual property.[116] With a unique,

---

113. *See* Matt Curtin, Gary Ellison & Doug Monroe, *"What's Related?" Everything But Your Privacy*, Oct. 10, 1998 <http://www.interhack.net/pubs/whatsrelated/>.

Netscape promises not to misuse the information, and there is no reason to doubt this. *See* Netscape, *Are there Privacy Issues with What's Related?* <http://home.netscape.com/escapes/related/faq.html#12>. Nonetheless, the threat seems particularly acute because Netscape itself sets a fairly detailed cookie before allowing download of browsers containing 128-bit cryptography. Curtin et. al, *supra*. Furthermore, Netscape's reaction to the Curtin, Ellison, and Monroe report was intemperate at best. Netscape set its "what's related" feature to show the Unabomber manifesto as "related" to the report! *See* Matt Curtin, "*What's Related?" Fallout* <http://www.interhack.net/pubs/whatsrelated/fallout/>.

114. Bob Van Voris, *Black Box Car Idea Opens Can of Worms*, NAT'L L.J., June 7, 1999 <http://www.lawnewsnetwork.com/stories/A2024-1999Jun4.html>.

115. *See* Stephanie Miles, *Intel Downplays Chip Hack Report*, Feb. 24, 1999 <http://news.cnet.com/news/0-1003-200-339182.html?tag=> ("Pentium III's serial code can be retrieved without the user's knowledge or approval.").

116. *See* Patrick Gelsinger, *A Billion Trusted Computers* (Jan. 20, 1999) <http://www.intel.com/pressroom/archive/speeches/pg012099.htm>; *see also* Robert Lemos, *Intel: Privacy Is Our Concern as Well*, ZDNET NEWS, Jan. 20, 1999 <http://www.zdnet.com/zdnn/stories/news/0,4586,2190019,00.html> (noting Intel's argument that security justifies a loss of some privacy).

indelible ID number on each chip, software could be configured to work only on one system. Users could only mask their identities when many people used a single machine, or when one person used several machines. The unique ID could also serve as an index number for web sites, cookie counters, and other means of tracking users across the Internet.

The revelation that Intel was building unique serial numbers into Pentium III chips caused a small furor. In response, Intel announced it would commission a software program that would turn off the ID function.[117] However, Intel's software can be circumvented by a sufficiently malicious program and the ID number surreptitiously broadcast in a cookie or by other means.[118]

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[119] 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, because it forms part of each device's address, ensuring that no two devices get confused with each other, and that no data packets get misdelivered. The privacy issues become most acute when such a 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 Internet Protocol version 6 ("IPv6"),[120] which will gradually replace the current Internet protocol, contemplates using an ethernet card's unique ID to create a globally unique identifier ("GUID"). The IPv6 standard requires software to include a GUID in the header of every Internet communication (email, web browsing, chat, and others). Computers with an ethernet card would create a GUID by combining the unique ID number assigned to the card's manufacturer with a unique number assigned to the card in the factory.[121] Thus, "[e]very packet you send out onto the public Internet using IPv6 has your fingerprints on it. And unlike

---

117. *See Big Brother Inside Homepage* <http://www.bigbrotherinside.com/#notenough>.

118. *See* Michael Kanellos & Stephanie Miles, *Software Claims to Undo Pentium III Fix*, CNET NEWS, Mar. 10, 1999 <http://news.cnet.com/news/0-1003-200-339803.html?tag=> .

119. DSL stands for "Digital Subscriber Line." *See generally* John Kristoff, *comp.dcom.xdsl Frequently Asked Questions* <http://homepage.interaccess.com/~jkristof/xdsl-faq.txt>.

120. *See generally* STEVE KING, RUTH FAX, DIMITRY HASKING, WEAKEN LING, TOM MEEHAN, ROBERT FINK & CHARLES E. PERKINS, THE CASE FOR IPV6 4 (1999) <http://www.ietf.org/internet-drafts/draft-iab-case-for-ipv6-05.txt> (touting IPv6's "enhanced features, such as a larger address space and improved packet formats"); *Ipv6: The Next Generation Internet!* <http://www.ipv6.org>.

121. *See* KING et al., *supra* note 120, 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* <http://standards.ieee.org/regauth/oui/tutorials/EUI64.html> (explaining ID numbers).

your IP address under IPv4, which you can change, this address is embedded in your hardware. Permanently."[122] In response to criticism, the standard-setting bodies are reconsidering revisions which would allow users—if they are savvy enough to do so—to pick a random number to replace the GUID from time to time.[123] But this modification is still under consideration and would not, apparently, be the default.

Even before IPv6 was introduced, some software products, notably Word 97, Excel 97, and PowerPoint 97, routinely embedded a unique ID number into every document. If a computer had an ethernet card, the programs used its MAC, much like IPv6.[124] 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 to Microsoft; visitors to the Microsoft web site who had previously registered were then given a cookie with the ID number.[125] As a result, the Microsoft ID not only identified a computer, but tied it directly to an individual's personal data. These features were not documented.[126] Although there is no reason to believe that Microsoft used the information for anything other than tracking the 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 four billion dollars.[127] Not sur-

---

122. Bill Frezza, *Where's All the Outrage About the IPv6 Privacy Threat?,* TECHWEB, Oct. 4, 1999 <http://www.internetwk.com/columns/frezz100499.htm>

123. *See* THOMAS NARTEN, & R. DRAVES, PRIVACY EXTENSIONS FOR STATELESS ADDRESS AUTOCONFIGURATION IN IPV6 1 (1999) <ftp://ftp.isi.edu/internet-drafts/draft-ietf-ipngwg-addrconf-privacy-01.txt>.

124. *See* Yusef Mehdi, *Microsoft Addresses Customers' Privacy Concerns*, PRESSPASS, Mar. 8, 1999 <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 <http://news.cnet.com/news/0-1006-200-339622.html?st.ne.160.head>.

125. *See* David Methvin, *WinMag Exclusive: Windows 98 Privacy Issue Is Worse than You Thought*, TECHWEB, Mar. 12, 1999, <http://www.windowsmagazine.com/news/1999/0301/0312a.htm>. Users can test for the problem at Pharlap Software, *Windows 98 RegWiz Privacy Leak Demo Page* <http://security.pharlap.com/regwiz/index.htm>. A patch for Word 97, Excel 97, and PowerPoint 97 is available at <http://officeupdate.microsoft.com/downloadDetails/Off97uip.htm>

126. Associated Press, *Microsoft Promises a Patch for ID Feature*, Mar. 9, 1999 <http://search.nytimes.com/search/daily/homepage/bin/fastweb?getdoc+cyber-lib+cyber-lib+4112+0+wAAA+microsoft%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.").

127. Kathleen Murphy, *$4B Sought from Yahoo for Not Sharing Customer Data*, INTERNET WORLD NEWS, Dec. 27, 1999 <http://www.internetworldnews.com/GetThisStory.cfm?Storyid=746B3487-B95D-11D3-976500A0CC40B49B>.

prisingly, other companies, including RealNetworks and Amazon.com, have been collecting, or considering collecting, similar personal information.[128] 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 have paid an annual fee for a Windows license in future versions of the operating system.[129] Annual billing would most likely have required registering and identifying users.

Hardware with built-in ID numbers is not yet ubiquitous, but proposals for expanding its 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 that people could use color copiers to counterfeit United States currency has spurred makers of color copiers to put invisible, unique ID numbers in each machine in order to trace counterfeits.[130] The ID number appears in all color copies, making every copied document traceable to its originating machine. Because the quality of personal color printers continues to improve, the U.S. Treasury Department 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 printer manufacturers to build tracing information into all color printers.[131]

Ubiquitous hardware ID numbers are probably inevitable because they will enable smart homes and offices. Consider, for example, the smart refrigerator: Its 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. A smart fridge also can be linked to an online cookbook to suggest suitable recipes depending upon its contents.[132] Once every food is tagged,[133] and the fridge knows its expiration date, the smart fridge can even

---

128. *See* John Markoff, *Bitter Debate on Privacy Divides Two Experts*, N.Y. TIMES, Dec. 30, 1999 <http://www.nytimes.com/library/tech/99/12/biztech/articles/30privacy.html>.

129. *See* Jason Catlett, *A Study of the Privacy and Competitiveness Implications of an Annuity Model for Licensing Microsoft Windows 2000*, JUNKBUSTERS, Mar. 4, 1999 <http://www.junkbusters.com/ht/en/bill.html>.

130. *See* Lauren Weinstein, *IDs in Color Copies—A PRIVACY Forum Special Report*, PRIVACY FORUM DIGEST, Dec. 6, 1999 <http://www.vortex.com/privacy/priv.08.18>.

131. *See* U.S. Bureau of Engraving and Printing, *Counterfeit Deterrence Features* <http://www.bep.treas.gov/countdeterrent.htm>.

132. *See* Ny Teknick, *Electrolux Demonstrates the Smart Fridge Concept*, ETHOS NEWS, Mar. 4, 1999 <http://www.tagish.co.uk/ethosub/lit7/1484e.htm>; *see also* Joseph 'Jofish' Kaye, *Counter Intelligence & Kitchen Sync: White Paper* 3 (June 1999) (unpublished manuscript) <http://www.media.mit.edu/ci/research/whitepaper/cil3.htm> (detailing "Kitchen Sync," the "digitally connected, self-aware kitchen").

133. *See* Joseph Kaye, Niko Matsakis, Matthew Gray, Andy Wheeler & Michael Hawley, *PC Dinners, Mr. Java and Counter Intelligence: Prototyping Smart Appliances for the Kitchen* (Nov. 1, 1999) (unpublished manuscript submitted to IEEE) <http://www.media.mit.edu/ci/ieee.cga.jofish/

be programmed to remind 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 devising plans to get and use that information.[134] 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 the insured's home, whether she snacks regularly, and how often she eats fatty foods.

3. *Biometrics*.

Technology for identifying people is advancing at least as quickly as technology for identifying machines. With technologies for distinguishing human irises, fingerprints, faces, or other body parts[135] 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.[136] Biometrics can be used for identification (who is this?) or authentication (what permissions does this person have?).[137]

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 withdraw money from an ATM.[138] The United States government uses biometric identifiers in the border crossing identification cards issued to aliens who frequently travel to and from the United States on business,[139] as

---

ieee.cga.jofish.htm> ("We predict—even assume, in many of our scenarios—that all products sold will have a digital ID.").

134. *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) <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.").

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

136. *See generally* Ontario Info. & Privacy Comm'r, *Consumer Biometric Applications: A Discussion Paper* <http://www.ipc.on.ca/web_site.eng/matters/sum_pap/papers/cons-bio.htm> (discussing biometrics, its benefits and concerns, and its effects on privacy); Clarke, *supra* note 9.

137. *See generally* Dutch Data Protection Authority (Registratiekamer), R. Hes, T.F.M. Hooghiemstra & J.J. Borking, *At Face Value: On Biometrical Identification and Privacy* § 2 (1999) <http://www.registratiekamer.nl/bis/top_1_5_35_1.html> (discussing the various applications of biometrics).

138. *See, e.g.*, Guy Gugliotta, *The Eyes Have it: Body Scans at the ATM*, WASH. POST., June 21, 1999, at A1 <http://www.washingtonpost.com/wp-srv/national/daily/june99/scans21.htm>.

139. *See* 8 U.S.C.A. § 1101(a)(6) (West Supp. 1999); Theta Pavis, *U.S. Takes Immigration in Hand*, WIRED, Sept. 15, 1998 <http://www.wired.com/news/news/technology/story/15014.html> (describing INSPASS system, which relies on handprints).

do several states seeking to prevent fraudulent access to welfare and other benefits.[140]

Despite the potential to enhance privacy, biometrics pose a two-pronged threat. 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 a biometric identifier, the more it is likely to be used, and the greater the amount of data likely to be linked to it.[141] Because a 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 a witness protection program. As far as we know, changing an iris or a fingerprint is much more difficult. Second, some biometrics, particularly those that involve DNA typing, disclose information about the data subject, such as race, sex, ethnicity, propensity for certain diseases, and (as the genome typing improves) even more.[142] Others may provide the capability to detect states of mind, truthfulness, fear, or other emotions.[143]

DNA is a particularly powerful identifier. It is almost unique[144] and (so far) impossible to change. A number of state and federal databases already collect and keep DNA data on felons and others.[145] Attorney General Janet

---

140. *See* JOHN D. WOODWARD, JR., U.S. DEP'T OF COMMERCE, COMMENTS FOCUSING ON PRIVATE SECTOR USE OF BIOMETRICS AND THE NEED FOR LIMITED GOVERNMENT ACTION § II.B (1998) <http://www.ntia.doc.gov/ntiahome/privacy/mail/disk/woodward.htm> ("Arizona, California, Connecticut, Illinois, Massachusetts, New Jersey, New York and Texas are using finger imaging to prevent entitlement fraud. Florida, North Carolina and Pennsylvania have biometric operational systems pending."); Connecticut Department of Social Services, *Digital Imaging: Connecticut's Biometric Imaging Project* <http://www.dss.state.ct.us/digital.htm> (providing links to extended descriptions of biometrical imaging of AFDC and General Assistance recipients for identification purposes).

141. *See* Ann Cavoukian, *Biometrics and Policing: Comments from a Privacy Perspective* § 4, *in* POLIZEI UND DATENSCHUTZ—NEUPOSITIONIERUNG IM ZEICHEN DER INFORMATIONSGESELLSCHAFT (Data Protection Authority ed., 1999) <http://www.ipc.on.ca/web_site.eng/matters/sum_pap/PAPERS/biometric.htm>.

142. *See id*. 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* Ontario Info. & Privacy Comm'r, *supra* note 136, at text following 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.").

143. *See* Dutch Data Protection Authority (Registratiekamer et al.), *supra* note 137, §§ 2.2-2.3.

144. *See DNA Fingerprinting*, ENCYCLOPEDIA BRITANCICA ONLINE <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)").

145. 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. *But see* Ng Kang-Chung, SOUTH CHINA MORNING POST, Feb. 12, 1999, *Legislators Fear*

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, and sizable, national database: More than fifteen million people were arrested in the United States in 1997 alone.[146] 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.[147]

4. *Sense-enhanced searches.*

Sense-enhanced searches rely on one or more technologies to detect that which ordinarily could not be detected with un-aided human senses. These searches differ from surveillance in public places because, 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 locations. Unlike home or office monitoring, which usually requires equipment inside the location of interest, many sense-enhanced searches allow someone on the outside to see what is happening inside a building, 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 that are not coerced by the observer, these technologies may be permissible under both the Fourth Amendment and private law trespass law. Sense-enhanced search technology is changing rapidly, raising doubts as to what constitutes a reasonable expectation of privacy in a world where we are all increasingly naked and living in transparent homes.

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

a. *Looking down: satellite monitoring.*

Once the sole property of governments, high-quality satellite photographs in the visible spectrum are now available for purchase. The sharpest

---

DNA Test Plans Open to Abuse, available in 1999 WL 2520961 (describing the Hong Kong legislature's fears of "allowing police to take DNA samples from suspects too easily").

146. *See* EPIC, *supra* note 36.

147. Mannvernd, Association for Ethical Science, *The Health-Sector Database Plans in Iceland*, July 7, 1998 <http://www.simnet.is/mannvernd/english/articles/27.11.1998_mannvernd_summary.html>.

pictures on sale today are able to distinguish objects two meters long,[148] with a competing one-meter resolution service planned for later this year.[149]

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 that receives coordinates from global positioning satellites ("GPS") and communicates them to a monitoring center.[150] The cost for this service is low, about $12.50 per target per day.[151]

Meanwhile, the United Kingdom is considering the adoption of a GPS-based system, already field tested in the Netherlands and Spain,[152] to prevent speeding. Cars would be fitted with GPS monitors that would pinpoint the car's exact location, link with a computer built into the car containing a database of national roads, identify the applicable speed limit, and instruct a governor built into the vehicle to stop the fuel supply if the car exceeds a certain speed.[153] GPS systems allow a receiver to determine its location by reference to satellites, but do not actually transmit the recipient's location to anyone.[154] The onboard computer could, however, permanently record everywhere the car goes, if sufficient storage were provided. The United Kingdom proposal also calls for making speed restrictions contextual, allowing traffic engineers to slow down traffic in school zones, after accidents, or during bad weather.[155] This contextual control requires a means to load updates into the computer; indeed, unless the United Kingdom wished to freeze its speed limits for all time, some sort of update feature would be essential. Data integrity validation usually relies upon two-way communication. Once the speed control system and a central authority are communicating, the routine downloading of vehicle travel histories would become a real possibility. And even without two-way communication, satellite-control over a vehicle's fuel supply would allow immobilizing vehicles for purposes other than traffic control. For example, cars could be stopped for riot control or if being

---

148. *See SPIN-2 High Resolution Satellite Imagery* <http://www.spin-2.com/>.

149. The improved pictures will come from the Ikonos satellite. *See Ikonos, Carterra Ortho Products Technical Specs* <http://www.spaceimaging.com/carterra/orthotechpan.htm>.

150. *See* Joseph Rose, *Satellite Offenders*, WIRED, Jan. 13, 1999 <http://www.wired.com/news/news/technology/story/17296.html>.

151. *See* Gary Fields, *Satellite "Big Brother" Eyes Parolees*, Apr. 8, 1999, USA TODAY, at 10A.

152. *See Satellites in the Driving Seat*, BBC NEWS, Jan. 4, 2000 <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 the system voluntarily).

153. *See* Jon Hibbs, *Satellite Puts the Brake on Speeding Drivers*, TELEGRAPH, Jan. 4, 2000 <http://www.telegraph.co.uk:80/et?ac=000141005951983&rtmo=kLJAeZbp&atmo=kLJAeZbp&pg=/et/00/1/4/nsped04.html>; "*Spy in the Sky" Targets Speeders*, BBC NEWS, Jan. 4, 2000 <http://newsvote.bbc.co.uk/hi/english/uk/newsid_590000/590336.stm>.

154. *See* WATCHING ME, WATCHING YOU, *supra* note 61.

155. *See* Hibbs, *supra* note 153.

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 an individual without one could be tracked by satellite in the manner depicted by the film *Enemy of the State*. However, a one-meter resolution suggests that it should be possible to track a single vehicle if a satellite were able to provide sufficient images, and satellite technology is improving rapidly.

The public record does not disclose how accurate secret spy satellites might be, nor what parts of the spectrum they monitor 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.

b. *Seeing through walls.*

It may be that "the house of every one is to him as his castle and fortress, as well for his defence against injury and violence, as for his repose,"[156] but the walls of that fortress are far more permeable today than ever before. Suitably equipped observers can now draw informed conclusions about what is occurring within a house without having to enter it. Most of these technologies are passive. 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, most hold that passive thermal imaging that does not reveal details about the inside of the home does not require a warrant.[157]

---

156. Semayne's Case, 77 Eng. Rep. 194, 195 (K.B. 1604), *quoted with approval in* Wilson v. Layne, 526 U.S. 603, 609-10 (1999).

157. *See* United States v. Kyllo, 190 F.3d 1041, 1046-47 (9th Cir. 1999) (holding that the use of a thermal imager did not require a warrant because it "did not expose any intimate details" of the inside of a home, and therefore a privacy interest in dissipated heat was not one that society would accept as "objectively reasonable"); United States v. Robinson, 62 F.3d 1325, 1328-29 (11th Cir. 1995) (holding that a thermal imager search does not violate the Fourth Amendment); *see also* United States v. Ishmael, 48 F.3d 850, 853-55 (5th Cir. 1995); United States v. Myers, 46 F.3d 668, 669-70 (7th Cir. 1995); United States v. Ford, 34 F.3d 992, 995-97 (11th Cir. 1994); United States v. Pinson, 24 F.3d 1056, 1058-59 (8th Cir. 1994); *but see* United States v. Cusumano, 67 F.3d 1497,

The telephone is not the only electronic device that allows new forms of monitoring. Computer monitors broadcast signals that can be replicated from a considerable distance.[158] Computer programs and viruses can use this capability to surreptitiously broadcast information other than what is displayed on the screen. These emissions are so powerful that one of the academics who first documented them suggested that Microsoft 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."[159] 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 this distance monitoring by employing "Tempest fonts." These special fonts will protect the user's privacy by displaying to any eavesdropper a text different from the one actually displayed on the users' screen.[160]

c. *Seeing through clothes.*

Passive millimeter wave imaging reads the electromagnetic radiation emitted by an object.[161] Much like an X-ray, this technology can specifically identify the radiation spectrum of most objects carried on the person, even those in pockets, under clothes, or in containers.[162] It thus allows the user to

---

1500-01 (10th Cir. 1995), *aff'd 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); State v. Young, 867 P.2d 593, 594 (Wash. 1994) (holding that a warrantless thermal image search violates State and Federal Constitutions). For an analysis of the lower courts' thermal imaging cases, see Lisa Tuenge Hale, *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, 833-45 (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, 842-58 (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 Residences and the Fourth Amendment*, 90 NW. U. L. REV. 267, 282-87 (1995).

158. *See* Marcus J. Kuhn & Ross Anderson, *Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations* <http://www.cl.cam.ac.uk/~mgk25/ih98-tempest.pdf>.

159. Email from Ross Anderson to ukcrypto mailing list (Feb. 8, 1998) (available at <http://www.jya.com/soft-tempest.htm>).

160. Tempest-resistant fonts designed by Ross Anderson are available at <http://www.cl.cam.ac.uk/~mgk25/st-fonts.zip>.

161. *See generally* Alyson L. Rosenberg, *Passive Millimeter Wave Imaging: A New Weapon in the Fight Against Crime or a Fourth Amendment Violation?*, 9 ALB. L.J. SCI. & TECH. 135 (1998).

162. *See* Millivision, *Security Applications* <http://www.millivision.com/security.html>; Merrik D. Bernstein, "*Intimate Details*": *A Troubling New Fourth Amendment Standard for Government Surveillance Techniques*, 46 DUKE L.J. 575, 600-04 (1996) (noting that although Millivision can see through clothes it does not reveal anatomical details of persons scanned).

see through clothes, and conduct a "remote frisk" for concealed weapons,[163] or other contraband.[164] Imagers are available as handheld scanners, visible gateway scanners, or in hidden surveillance models.[165]

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 United States customs service is using it as an alternative to 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."[166] The sample photo provided by BodySearch makers American Science and Engineering, Inc. is fairly revealing.[167] Still newer devices such as a radar skin scanner can distinguish

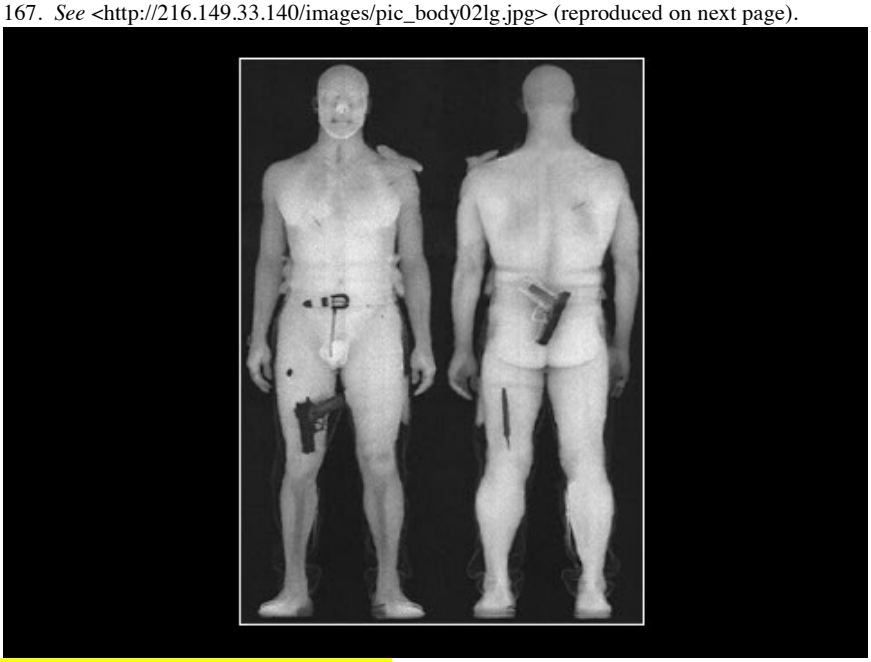
163. *See* Millivision, *Concealed Weapon Detection* <http://www.millivision.com/cwd.html>.

164. *See* Millivison, *Contraband Detection* <http://www.millivision.com/contband.html> ("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.").

165. *See id*. (containing links to various models).

166. Deepti Hajela, *Airport X-Ray Device Spurs Concerns*, AP ONLINE, Dec. 29, 1999 (quoting testimony of ACLU legislative counsel Gregory T. Nojeim).

167. *See* <http://216.149.33.140/images/pic_body02lg.jpg> (reproduced on next page).



[note: copyright permission not yet secured]

all anatomical features over one millimeter, making it possible to "see through a person's clothing with such accuracy that it can scan someone standing on the street and detect the diameter of a woman's nipples, or whether a man has been circumcised."[168]

d. *Seeing everything: smart dust.*

Perhaps the ultimate privacy invasion would be ubiquitous miniature sensors floating 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 properly), the engineers hope to meet their one cubic millimeter 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.[169]

Although funded by the Pentagon, the project managers foresee 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.[170]

II. RESPONDING TO PRIVACY-DESTROYING TECHNOLOGIES

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.[171] As the previous discussion demonstrates, however, even without ubiquitous microcameras, governments and others are deploying a wide variety of privacy-destroying technologies. These developments raise the immediate question of the appropriate legal and social response.

One possibility is to just "get over it" and accept emerging realities. Before adopting this counsel of defeat, however, it seems prudent to explore the

---

168. Judy Jones, *Look Ahead to the Year 2000: Electronic Arm Of The Law Is Getting More High-Tech*, COURIER-J. (Louisville, KY), Oct. 19, 1999, *available in* 1999 WL 5671879.

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

170. *See id.*

171. *See* BRIN, *supra* note 11; 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).

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 that must shape any practicable response to privacy-destroying technologies.

A. *The Constraints*

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

1. *The economics of privacy myopia.*

Under current ideas of property in information, consumers are in a poor legal position to complain about the sale of data concerning themselves.[172] 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 belong equally to both.[173] As evidenced by the existence of the direct mail industry, both sides to a transaction generally are free to sell details about 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.[174] Overall, the number of transactions in which confidentiality is the legal default is relatively small compared to the total number of transactions in the United States.

In theory, the parties to a transaction can always contract for confidentiality. This is unrealistic due because consumers suffer from *privacy myopia*: they will sell their data too often and too cheaply. Modest assumptions about

---

172. For an extreme example, see Moore v. Regents of California, 793 P.2d 479, 488-97 (Cal. 1990) (holding that a patient had no cause of action, under property law, against his physician or others who used the patient's cells for medical research without his permission).

173. *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 the 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.").

174. *See* ABA MODEL CODE OF PROFESSIONAL RESPONSIBILITY Cannon 4 (1999); ABA MODEL RULES OF PROFESSIONAL CONDUCT Rule 1.6. (1999).

consumer privacy myopia suggest that even Americans who place a high value on 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. Most heroically, assume that once some threshold has been reached the value of additional data to a potential profiler remains linear and does not decline. Finally, assume that data brokers or profile compilers are able to buy consumer data from merchants at low transactions costs, because the parties are repeat players who engage in numerous transactions involving substantial amounts of data. Consumers, however, are unaware of the value of their aggregated data to a profile compiler. With one possible exception, the assumption that the value of consumer data never declines, these all seem to be very tame assumptions.

In an ordinary transaction, a consumer will value a datum at its marginal value in terms of lost privacy. In contrast, a merchant, who is selling it to a profiler, will value it at or near its average value as part of a profile. Because, according to our 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 be willing to sell data at a price a merchant is willing to pay.

The ultimate effect of consumer privacy myopia depends upon a number of things. First, it depends on the intrusiveness of the profile. If the profile creates a privacy intrusion that is noticeably greater than disclosing an occasional individual fact—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. 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 people who object to being profiled are unusual, and aggregation does not cause harm to most people's 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 possible. But consumers who place a high value on 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.

Unfortunately, if the marginal value[175] to the consumer of a given datum is small, then the value of not disclosing that datum will in most cases be lower than either the cost of negotiating a confidentiality clause (if that option even exists), or the cost of forgoing the entire transaction.[176] 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 this.[177] Furthermore, changing the law to make consumers the default owners of information about 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 contracts forms add 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 its marginal value rather than its average value, which is difficult to measure—but profilers are not 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 accurate, it has unfortunate implications for many proposals to change the default property rules regarding ownership of personal data in ordinary transactions. The sale will tend to happen even if the consumer has a sole entitlement to the data. It also suggests that European-style data protection rules should have only a limited effectiveness, primarily for highly sensitive personal data. The European Union's data protection directive allows personal data to be collected for reuse and resale if the data subject agrees;[178] the privacy myopia story suggests that customers will ordinarily agree except when disclosing particularly sensitive personal facts with a high marginal value.

---

175. Or even the average value to a well-informed consumer.

176. *See* Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497, 519-23 (1995); Sovern, *supra* note 22, at 1033 (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.").

177. *See* Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 GEO. L.J. 2381, 2413 (1996).

178. *See* Viktor Mayer-Schönberger, *Generational Development of Data Protection in Europe*, *in* TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE 219, 232 (Philip E. Agre & Marc Rotenberg eds., 1997).

On the other hand, the privacy myopia story suggests several 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 than marginal value. Can information provide a corrective lense?[179] Or, perhaps consumers already have the ability to value the privacy interest in small amounts of data if they consider the long term consequences of disclosure.

Consumers sometimes have an interest in disclosure of information. For example, proof of credit-worthiness tends to improve the terms upon 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 the intermediate good aspect of informational privacy and disclosure substantially outweighed their final good aspect, the focus on blocking disclosure advocated in this article might be misguided. European data-protection rules, which focus on requiring transparency regarding the future uses of gathered data, 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 of 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 subject's personal data. Furthermore, it could be useful to know whether 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 would be 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 informational privacy.

There has already been considerable work on privacy-enhancing technologies for electronic transactions.[180] There seems to be a need for more research, however, to determine which types of transactions are best suited to using technologies such as information intermediaries. The hardest work, will involve finding ways to apply privacy-enhancing technologies to those transactions that are not naturally suited to them.

---

179. 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* <http://www.media-awareness.ca/eng/cpigs/cpigs.htm>.

180. *See*, *e.g.*, INFORMATION AND PRIVACY COMM'R/ONTARIO, CANADA & REGISTRATIEKAMER [Dutch Data Protection Authority], THE NETHERLANDS, 1 PRIVACY-ENHANCING TECHNOLOGIES: THE PATH TO ANONYMITY (1995) <http://www.ipc.on.ca/web_site.ups/matters/sum_pap/papers/anon-e.htm>.

Perhaps the most promising avenue is to design contracts and technologies that undercut 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 such a cost will be less than the marginal value of the data (note that merely lowering it below average cost fails to solve the underlying problem, because sales will still happen in that price range). If technologies, such as P3P,[181] reduce the marginal transactions costs involved in negotiating the release of personal data to near zero, even privacy myopics will be able to express their privacy preferences in the P3P-compliant part of the marketplace.

2. *First Amendment*.

The First Amendment affects potential privacy-enhancing rules in at least three ways: (1) most prohibitions on private data-gathering in public (i.e. surveillance) risk violating the First Amendment (conversely, most government surveillance in public appears to be unconstrained by the Fourth Amendment)[182]; (2) the First Amendment may 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 some cases.[183]

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.

---

181. 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., *P3P and Privacy on the Web FAQ* <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.").

182. "[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); *see also* Michigan v. Long, 463 U.S. 1032, 1049-50 (1983).

183. *See generally* A. Michael Froomkin, *Legal Issues in Anonymity and Pseudonymity*, 15 THE INFORMATION SOCIETY 113 (1999).

a. *The First Amendment in public places.*

Perhaps *the* critical question shaping the legal and social response to new surveillance technology is the extent to which the government 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 also include educating people as to the consequences of disclosure or deploying countertechnologies such as scramblers, detectors, or masks.[184] Unlike a legal solution, however, most technological responses involve shifting costs to the data subject. The cost of compliance with laws restricting data collection is likely to fall on the observer, at least initially. The difficulty is writing rules that are consistent with both the First Amendment and basic policies of freedom.

Professor Jerry Kang recently proposed and defended a statute limiting 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 still only a small part of most daily lives. Part I demonstrates that a great deal of the threat to information privacy is rooted firmly in "meatspace" (the part of life that is not cyberspace). The problem is considerably more general. 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.

The core question is whether a legislature could constitutionally change the default rules, which hold that what is visible is public, in order to increase informational privacy. Current doctrine does not make clear the extent to which Congress may seek to preserve, or even expand, zones of privacy in public places (or informational privacy relating to transactions) by making it an offense to use a particular technology to view or record others. This may be because attempts to expand the zone of privacy in the United States by legislation are still relatively rare. Prohibiting the use of technologies that are not already commonplace prevents the public from becoming desensitized, and it ensures a reasonable expectation of being able to walk in

184. On masks, however, see text accompanying notes 301-303 *infra* (discussing antimask laws in several states).

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 restricted technologies will not be used. At some undefined point, perhaps quite close to its inception, any such attempt will begin to intrude on core First Amendment values.

In peacetime, the First Amendment allows only the lightest restrictions upon the ordinary gathering of information in public places (or upon repeating of such information).[185] 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, because most rules designed to protect privacy in public places would probably have a substantial harmful effect upon news gathering and public debate. Nevertheless, there are a few areas where light privacy-enhancing regulation might not impinge upon core First Amendment values. There are also areas where laws that actively hinder privacy might be reformed.

The constitutional status of a regulation of data collection has implications for the regulation of its subsequent uses. If it were unconstitutional to impose a restriction upon the initial collection, then it would 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, for example, the dissemination of mall camera photos or the sale of consumer profiles, will be closely tied, and sometimes identical, to the justification for banning the data collection in the first place. If restrictions upon the initial collection could be imposed constitutionally, then justifications for imposing conditions that run with the data are easy to see. If, on the other hand, the data were lawfully acquired, justifying rules that prevent it from being shared (or, perhaps, even used by the initial collector) is far less onerous if one can categorize the dissemination of the data as the shipment of a data-good in commerce rather than as a publication or other speech act.

The recent and unanimous Supreme Court decision in *Reno v. Condon*[186] could be read to suggest that the act of transmitting personal data for commercial purposes is something less than even commercial speech. In *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 sub-

185. *See* note 191 *infra*.

186. 120 S. Ct. 666, 668 (2000) (upholding Driver's Privacy Protection Act of 1994, 18 U.S.C. §§ 2721-25 (1994 & Supp. III), against claim that it violated federalism principles of Constitution).

ject of congressional regulation" under Congress's Commerce Clause powers.[187] The circumstances and posture of *Condon* suggest, however, that this reading, which would be a radical break with existing First Amendment principles, is not justified.

Gathering information in public. The First Amendment protects the freedom of speech and of the press, but does not explicitly 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.[188] The right is not unlimited. It does not, for example, create an affirmative duty on the government to make information available.[189]

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 recollections, she may also photograph it or videotape events and then publish mechanically recorded images and sounds. Most courts that have examined the issue, however, have held that she may do so, subject only to very slight limitations imposed by privacy torts.[190] "[C]ourts have consistently refused to consider the taking of a photograph as an invasion of privacy where it occurs in a public for a [sic]."[191] "Thus, in order for an invasion of privacy to occur, '[t]he invasion

---

187. *Id*. at 671 (quoting United States v. Lopez, 514 U.S. 549, 558-59 (1995)).

188. In Kleindienst v. Mandel, 408 U.S. 753, 765-70 (1972), the Court acknowledged a First Amendment right to receive information, but said that the right must bow to Congress' plenary power to exclude aliens. *See also* Lamont v. Postmaster General, 381 U.S. 301, 305-07 (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, 146-49 (1943) (invalidating a municipal ordinance forbidding door-to-door distribution of handbills as violative of the recipients' First Amendment rights); *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 [F]irst [A]mendment right to acquire that information.").

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

190. *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, 478 (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 (1977).

191. United States v. Vazquez, 31 F. Supp. 2d 85, 90 (D. Conn. 1998) (finding no invasion of privacy where plaintiffs were photographed on a city sidewalk in plain view of the public eye); *see also* Jackson v. Playboy Enter., 574 F. Supp. 10, 13 (S.D. Ohio 1983); Fogel v. Forbes, Inc., 500 F. Supp. 1081, 1087 (E.D. Pa. 1980) (no invasion of privacy when photographing plaintiff at "a public place or a place otherwise open to the public"); People for the Ethical Treatment of Animals v. Bobby Berosini, Ltd., 895 P.2d 1269, 1281 (Nev. 1995) (no invasion of privacy filming backstage before live performance); Cox v. Hatch, 761 P.2d 556, 564 (Utah 1988) (no invasion of privacy when photographing "in an open place and in a common workplace where there were a number of other people"); Jaubert v. Crowley Post-Signal, Inc., 375 So. 2d 1386 (La. 1979) (holding that the First Amendment protects the right to take and publish photos of a house from a public street); Mark v. KING Broad. Co., 618 P.2d 512, 519 (Wash. Ct. App. 1980), *aff'd sub nom*. Mark v. Seat-

or intrusion must be of something which the general public would not be free to view.'"[192]

Perhaps it might be constitutional to prohibit the use of devices that see through clothes on the theory that there is a limited First Amendment exception allowing bans on outrageous assaults upon personal modesty. On the other hand, the government's use of passive wave imaging, which see through clothes, suggests that the executive branch believes either that there is no constitutional problem, or that the problem can be solved by offering subjects the alternative of an (equally intrusive?) patdown search.[193] Or, perhaps, the government's ability to ban intrusive monitoring sweeps more broadly. The correct doctrinal answer is unclear because 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 becomes. Meanwhile, however, one must look to privacy tort cases in which the First Amendment was raised as a defense in order to get an indication 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 personal data as the property of the data subject, approaches that focus on the targeted individual tend to ask whether there is something private or secluded about the place in which the person was located that 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, such looking under clothes.[194] 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 the expectation not to be subjected to it. Thus, for example, absent statutory change, courts would be unlikely to find a reasonable expectation of not being photographed in public, although it does not necessarily follow that one has no reasonable objection to being on camera all the time.

---

tle Times, 635 P.2d 1081 (Wash. 1981) (no invasion of privacy when filming interior of pharmacy from the exterior of the building).

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

193. The United States Customs offers travelers the option of choosing a pat down search instead of the X-ray, arguing that some might find the imaging to be less intrusive. *See* Hajela, *supra* note 166.

194. *See* note 191 *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 were to apply to all uses. The legislature can ban a technology that happens to be useful for news gathering if it does so through a law of general application, and the ban is reasonably tailored to achieve some legitimate objective. Privacy is surely such an objective. 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.[195] Indeed, federal regulations already criminalize the sale of various types of spy gear.[196]

Whether the ban could be crafted to apply only to use or possession in public places is more dubious, because this cuts more closely against the First Amendment. Pragmatically, the results in court may depend upon 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, as well as 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 interest in privacy.[197] Possibly, however, a more limited ban might be crafted to allow news gathering, but not twenty-four-hour surveillance. Such a rule might, for example, limit the number of images of a particular place per hour, day, or week, although lines would in-

---

195. *Cf.* Andrew Jay McClurg, *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 a similar distinction in connection with a 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").

196. *See* 18 U.S.C. § 2512(1)(a)-(b) (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. *See id.* § 2512(c).

197. *Cf.* Forster v. Manchester, 189 A.2d 147, 150 (Pa. 1963) (rejecting an invasion of privacy claim 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 the 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").

evitably be difficult to draw.[198] A more practical rule, perhaps easier to enforce, would distinguish among various technologies.

Disseminating accurate information. Data collection becomes much less attractive if there are fewer buyers. One way to reduce the number of buyers is to make it illegal to buy, use, or reveal the respective data. Although the issue is not settled, there are good reasons to believe that the First Amendment would forbid most legislation criminalizing the dissemination or use of accurate information.[199] While good for free speech, it makes any ban on data collection much more difficult to enforce. Conversely, if it is constitutional to penalize downstream uses of certain data, or even retention or publication, then enforcement of a collection ban becomes easier, and the incentives to violate the rule decrease.

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, and subsequent criminal prosecution, might be a constitutionally acceptable reaction to the publication of troop movements, or

---

198. The constitutionality of limits on data gathering in public places may be tested by anti-paparazzi statutes. The statute recently adopted in California suggests how such a law might look, 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.
>
> . . . .
>
> (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.

CAL. CIV. CODE § 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 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).

199. "Regulations that suppress the truth are no less troubling because they target objectively verifiable information." 44 Liquormart, Inc. v. Rhode Island, 517 U.S. 484, 502 (1996); *see also* Rubin v. Coors Brewing Co., 514 U.S. 476, 491 (1995) (holding that law abridging brewer's right to provide accurate information to public about the alcoholic content of malt beverages is unconstitutional). *See also* text accompanying notes 205-220 *infra*.

other similar information that might aid an enemy, during armed conflict.[200] In peacetime, copyright protections are justified by a specific constitutional derogation from the general principle of freedom of speech.[201] Some highly regulated industries, such as the securities industry, heavily restrict the speech of individuals, such as financial advisors or those with market-sensitive information, although the constitutionality of those rules is itself subject to some doubt and debate.[202] Generally, however, most truthful disclosures in the absence of a specific contractual duty to keep silent have usually been considered to be constitutionally protected.

The Supreme Court's decisions do not give blanket First Amendment protection to the publication of information acquired legally. Instead they have noted "[t]he tension 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 . . . ."[203] But, other than in cases involving intellectual property rights or persons with special duties of confidentiality,[204] the modern Court has struck down all peacetime restrictions on publishing true information that have come before it. The Court has kept open the theoretical possibility that a sufficiently compelling government interest might justify penalizing the publication of true statements. But, 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.[205] 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 stated in *Smith v. Daily Mail Pub-*

---

200. *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.").

201. *See* U.S. CONST. art. I, § 8, cl. 8.

202. *See* Taucher v. Born, 53 F. Supp.2d 464, 482 (D.D.C. 1999) (upholding a First Amendment challenge to § 6M(1) of the Commodity Exchange Act, 7 U.S.C. § 6m(1) (amended 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 "based solely on a fear that someone may publish advice that is fraudulent or misleading").

203. *Id.* at 530.

204. *E.g.*, Snepp v. United States, 444 U.S. 507, 510-15 (1980) (holding that government could enforce secrecy contract with former CIA agent); Cohen v. Cowles Media Co., 501 U.S. 663 (1991) (holding that a confidential source could recover damages for publisher's breach of promise of confidentiality).

205. In Detroit Edison Co. v. NLRB, 440 U.S. 301 (1979), the Court protected informational privacy interests in holding that the National Labor Relations Board could not compel a company to disclose results of psychological tests on individual employees to a union without the employees' consent. The Court held that, under federal labor law, the employees' right to privacy outweighed the burden on the union despite the union's assertion that it needed the data.

lishing Company, "state action to punish the publication of truthful information seldom can satisfy constitutional standards."[206] 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."[207]

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."[208] 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 upon § 867 of the Restatement of Torts by analogy, the Court noted that "the interests in privacy fade when the information involved already appears on the public record."[209]

Then, in *Landmark Communications, Inc. v. Virginia*, the Court struck down a state statute that criminalized the publication of the names of judges who were subject to confidential judicial disciplinary proceedings.[210] Although the newspaper received the information from someone who had no right to disclose 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 nor did it involve stolen information: "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."[211] And, in *Smith v. Daily Mail Publishing Co.*, the Court said that 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 do so.[212] Although the Court struck down the statute, it left open the possibility that publication of true and lawfully obtained information might be prohibited "to further an interest more substantial than is present here."[213] 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.[214]

---

206. 443 U.S. 97, 102 (1979).
207. *Id.* at 103; *quoted with approval in* Florida Star v. B.J.F., 491 U.S. 524, 524 (1989).
208. 420 U.S. 469, 472 (1975).
209. *Id.* at 494-95.
210. 435 U.S. 829 (1978).
211. *Id.* at 837.
212. 443 U.S. 97 (1979).
213. *Id.* at 103.
214. 491 U.S. 524 (1989).

More recently, in *Rubin v. Coors Brewing Co.*, the Court struck down a statute preventing 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 upon other types of speech.[215]

Thus, although the Supreme Court has "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,'"[216] its decisions suggest that if there is a category of truthful speech that can constitutionally be banned, it is small indeed. The rule remains that "state action to punish the publication of truthful information seldom can satisfy constitutional standards."[217]

The Supreme Court's decisions leave open the possibility that the First Amendment might apply more strongly when facts are 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."[218] Of the cases discussed above, only *Landmark Communications* involved a leak of information by someone with a legal duty to maintain its confidentiality. That case could be read to depend upon the heightened First Amendment protection for reporting upon important public issues, such as the honesty of judges.

Thus, the Supreme Court's cases are unclear as to whether a ban on the publication of illegally acquired information could fall within the presumably small class of regulations of truthful speech that satisfy constitutional standards. Whether it is ever possible to ban the publication of truthful information is unclear because the Court has never defined a "state interest of the highest order"[219] and because it has never decided whether illegally acquired information is (1) contraband per se, (2) contraband so long as a reasonable recipient should have known that it was illegally acquired, or (3) not contraband when laundered sufficiently, thus allowing publication under the protections of the First Amendment.[220] Which of the these is the law will have a

---

215. 514 U.S. 476 (1995). In *44 Liquormart, Inc. v. Rhode Island*, 517 U.S. 484 (1996), a fractured Court overturned Rhode Island's ban on truthful advertising of the retail price of alcoholic beverages.

216. *Florida Star*, 491 U.S. at 532-33 (quoting Cox Broad. Corp. v. Cohn, 420 U.S. 469, 491 (1975)).

217. *Daily Mail*, 443 U.S. at 102.

218. *Id.* at 103; *see also Florida Star*, 491 U.S. at 532-33 (quoting *Daily Mail*, 443 U.S. at 103, with approval).

219. *Daily Mail*, 443 U.S. at 103.

220. *See Florida Star*, 491 U.S. at 534 n.8 (citations omitted):

great impact upon any attempt to regulate technologies of surveillance, and profiling technologies generally, because it affects how easily data can be laundered.[221]

A recent divergence between two circuits suggests that the Supreme Court may be asked to decide whether truthful information, obtained legally by the ultimate recipient, can nonetheless be contraband because it was originally acquired illegally. The D.C. Circuit and the Third Circuit recently reached opposite conclusions regarding the potential liability of a third party receiver of information that was 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 news media. In *Boehner v. McDermott*,[222] 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 U.S.C. § 2511.[223] 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."[224] The Wiretapping Act, the D.C. Circuit suggested, increases the freedom of speech because "[e]avesdroppers destroy the privacy of conversations. The

---

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 *New York Times Co. v. United States*, and reserved in *Landmark Communications*. We have no occasion to address it here.

221. Washington is notoriously leaky. Except for the rare prior restraint cases involving national security such as *New York Times v United States*, 403 U.S. 713 (1971) (the "Pentagon papers" case), and *United States* v. *Progressive, Inc.*, 467 F. Supp. 990 (W.D. Wis. 1979) (the 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., *Mass Communications and the First Amendment: An Overview*, 55 LAW & CONTEMP. PROBS. 53, 57-58 (1992) ("It has been almost twenty years and five administrations since *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 subpoena to trace an inside-the-Beltway leak of information . . . .") (citation omitted).

222. 191 F.3d 463 (D.C. Cir. 1999). Judge Randolph authored the court's opinion, with Judge Ginsburg concurring in the judgment and with parts of the opinion. Judge Sentelle dissented.

223. *See* 18 U.S.C. § 2511(1)(c)-(d), 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. *Boehner*, 191 F.3d at 468.

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."[225] In reaching this conclusion, the court characterized Congressman McDermott's action in being a conduit from the eavesdropper to the media as being a combination of speech and conduct.[226] Judge Randolph characterized his act of handing over the tape as being akin to receiving, and passing on, stolen property.[227] Judge Ginsburg concluded that Congressman McDermott's conduct was outside the *Florida Star* rule—that publishing truthful speech can only be punished if there is a state interest of the "highest order"[228]—because he knowingly and "unlawfully obtained" the tape. Intermediate scrutiny was therefore appropriate, and the statute could survive that test.[229] Judge Sentelle dissented on the grounds that the *Florida Star* rule applied and compelled strict scrutiny. The third-party provisions of the Wiretapping Act failed this more exacting test because they were not a content-neutral regulations.[230] Judge Sentelle also specifically disagreed with the majority's assertion that, as he put it, the government may punish a "publisher of information [who] has obtained the information in question in a manner lawful in itself but from a source who has obtained it unlawfully."[231] Although he conceded that the state interest in protecting the privacy of communications was compelling, he disagreed that a blanket ban on third-party uses was narrowly tailored to serve that end.[232]

The Third Circuit also divided 2-1, but this time a majority saw the issue much like Judge Sentelle. *Bartnicki v. Vopper* involved a tape of a cellular telephone conversation between two members of a teachers' union who were engaged in contentious pay negotiations with their school district. Someone recorded a conversation in which the two union members discussed going to the homes of school members and "blow[ing] off their front porches."[233] An unknown party left the tape in the mailbox of Jack Yocum, an opponent of the teachers' union, who then took it to the press.[234]

---

225. *Id.*

226. *See id.* at 466-67 (citing United States v. O'Brien, 291 U.S. 367, 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").

227. *See id.* at 469.

228. Florida Star v. B.J.F., 491 U.S. 524, 524 (1989) (quoting Smith v. Daily Mail Publishing Co., 443 U.S. 97, 103 (1979)).

229. *See Boehner*, 191 F.3d at 480 (Ginsburg, J., concurring).

230. *See id.* at 480-84 (Sentelle, J., dissenting).

231. *Id.* at 484-85.

232. *See id.* at 485.

233. Bartnicki v. Vopper, 200 F.3d 109, 113 (3d Cir. 1999).

234. *Id.*

On an interlocutory appeal, the Third Circuit held 2-1 that 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 minimize the extent of its disagreement with the D.C. Circuit by focusing on the media defendants, who had no analogue in the *Boehner* case,[235] the *Bartnicki* majority still held that the conduit of the information was protected every bit as much as the ultimate publishers. In so doing, the *Bartnicki* majority characterized Yocum's conduct as pure speech, rejecting *Boehner*'s conclusion that it was more properly seen, at least partially, as conduct.

The first difficulty the Third Circuit had to overcome in reaching its conclusion was *Cohen v. Cowles Media*. In that case, 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."[236] 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."[237]

Despite holding that both Yocum and the media defendants engaged in pure speech, rather than 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 government's interest, and the means selected to effectuate that interest, against countervailing First Amendment freedoms. In doing this balancing, the court determined it must ask whether the regulation is "narrowly tailored" to achieve a "significant governmental interest."[238] The dissent agreed that this was the right test, but rejected the majority's application of it to the facts.[239]

The government argued that the Act was narrowly tailored. The regulation of third-party use, it said, eliminates the demand for the fruits of the wrongdoer's labor.[240] The *Bartnicki* majority was not persuaded, calling the connection between the third-party provisions of the Wiretapping Act and the prevention of the initial interception of communications "indirect at best";[241] in contrast, the dissent accepted the connection.[242]

---

235. *See* 191 F.3d at 467 (noting that the ultimate publishers of the conversation were not defendants in the *Boehner* case).

236. Cohen v. Cowles Media Co., 501 U.S. 663, 669 (1991).

237. *Id.* at 670.

238. *See Barnicki*, 200 F.2d at 124.

239. *See id.* at 130.

240. *Id.* at 125. The government also argued that the Act would "deny[] the wrongdoer the fruits of his [own] labor," but the majority noted on the facts neither defendant was the "wrongdoer"—the eavesdropper—so that justification did not apply. *Id.*

241. *Id.* at 126.

242. *Id.* at 133-34 (Pollak, J., dissenting).

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 sufficiently discourage the illicit acquisition of communications, thus justifying the speech restriction at issue. Although there is something distasteful about considering accurate information contraband, even if hedged with a scienter requirement, it seems hard to believe that criminalizing the receipt and publishing of personal data 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 gather data in the first place, since buyers would be harder to find. The argument is weakest in a context such as *Bartnicki*, where the motives for disclosure are political rather than financial, and the matter is of public interest. The argument is surely stronger when applied to the disclosure of personal profile data. However, even if one accepts a connection between prohibiting the dissemination of information and discouraging its collection, it does not necessarily follow that privacy interests trump free speech rights. How the balance comes out will depend in part upon what sort of scrutiny is applied; that in turn will depend upon how the act of sharing the information is categorized.

A related issue raised by the *Bartnicki/Boehner* split is whether sharing information is always speech protected by the First Amendment, or whether there are occasions in which information is just a regulated commodity. Questions concerning what is properly characterized as "speech" surround the regulation of everything digital, from the sale of bulk consumer data to the regulation of software.[243]

In both *Reno v. Condon* and *Los Angeles Police Department v. United Reporting Publishing Corp*,[244] the Supreme Court treated government-owned personal data as a commodity that could be subjected to reasonable regulations on subsequent use.

Condon, however, is a decision about federalism. Neither side briefed nor argued the First Amendment issues concerning reuse or republication rights of data recipients,[245] so the issue remains open.[246] It remains so even

243. *Cf.* Bernstein v. United States, 176 F.3d 1132, 1146 (9th Cir. 1999), *opinion withdrawn, rehearing en banc granted*, 192 F.3d 1308 (9th Cir. 1999) (deciding that source code is speech).

244. 120 S. Ct. 483, 489 (1999).

245. Neither party briefed or argued the First Amendment issue, except that the United States' reply brief responded to a claim, by an amicus, that *Condon* was analogous to the government targeting a particular member of the press for adverse treatment. *See* Reply Brief for the Petitioners at 17, Reno v. Condon, 120 S. Ct. 666 (2000) (No.98-1464), *available in* 1999 WL 792145.

246. 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.").

though the *Condon* decision specifically relied upon and upheld the part of the DPPA that regulates the resale and redisclosure of drivers' personal information by private individuals (who have obtained that information from a state department of motor vehicles).[247] The DPPA, the Court stated, "regulates the States as the owners of databases."[248] It follows that similar rules could be applied to any database owner; indeed the *Condon* Court defended the DPPA against South Carolina's claim that it regulated states exclusively by noting that § 2721(c) regulates everyone who comes into contact with the data.[249]

In this light, the key factor in *Condon* may be the Court's decision that no one has a right to drivers' license data in the first place because the data belongs 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 regulated. The same logic appears in *Los Angeles Police Department v. United Reporting Publishing Corp*.[250] 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 upon how the information would be used could survive at least a facial First Amendment challenge.[251]

If the Court adopts what amounts to a right/privilege distinction relating to government data, it is hard to see why the government's ability to impose conditions upon the use of its proprietary data should be any less than that of a private party, especially if those conditions arguably restrict speech. If data are just commodities, then data usage can be regulated by contract or license—a view that may import elements of a property theory into what had previously been the preserve of the First Amendment.

---

247. *See* 18 U.S.C. § 2721(c) (1999):

> 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 department upon request.

248. Reno v. Condon, 120 S. Ct. 666, 668 (2000).

249. *See id*. (noting that 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 alleged First Amendment right to view driver's license records, and did not address the republishing issue.

250. 120 S. Ct. 483, 489 (1999).

251. *See id*.

One view of the First Amendment, implied by *Bartnicki*, suggests that the government cannot impose sweeping restrictions on data dissemination in the name of privacy. The alternate view of the First Amendment, offered by *Boehner*, is more likely to allow the government to impose public limits on data dissemination and collection, and thus enhance privacy.[252] The *Boehner* vision, however, has potentially sweeping consequences unless some distinction can be delivered to prevent its application to publishers—which seems particularly dubious now that everyone is a publisher.[253] If it does apply publishers, then every newspaper that publishes a leak based upon classified information is at risk, and political reporting would be thoroughly chilled.[254] Just as a newspaper does not lose its status as protected speech because it is sold for a profit, other information, in other media, may be entitled to full First Amendment protection however it is transferred or sold.

b. *The First Amendment and transactional data.*

Transactional data—who bought what, when, where, and for how much—might be considered ordinary speech, commercial speech, or just an informational commodity. If transactional data is commercial speech, its regulation would be reviewed under the test 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.[255]

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 relating to commerce is surprisingly underlitigated. This may be because there is not (yet) much relevant regulation in United States law. Under the common law, absent a special duty of confidentiality such as an attorney-client relation-

---

252. Ironically, a vision that makes it possible to restrict the speech of persons who receive contraband information in the name of privacy is also the most compatible with diverse enactment such as the Uniform Computer Information Transactions Act and the Copyleft license, each of which impose private conditions on data dissemination.

253. *See generally* Eugene Volokh, *Cheap Speech and What it Will Do*, 104 YALE L.J. 1805 (1995).

254. "[N]early every action, recommendation, or policy decision in the foreign policy or national security field is classified as a secret by someone at some time, often without valid reason, except for bureaucratic convenience," Floyd Abrams, Henry Mark Holzer, Don Oberdorfer & Richard K. Willard, *The First Amendment and National Security*, 43 U. MIAMI L. REV. 61, 75 (1988) (remarks of Washington Post reporter Don Oberdorfer).

255. 447 U.S. 557, 566 (1980).

ship, 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.[256]) Current doctrine suggests that speech relating to 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.'"[257] On the other hand, the two most recent Supreme Court decisions relating to the regulation of personal data seem to imply that some transactional data is just a 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 upon the sharing of private transactional data collected by persons not classed as professionals. The most important may be the Fair Credit Reporting Act.[258] In addition to impressing rules designed to make credit reports more accurate, the statute also contains rules prohibiting credit bureaus from making certain accurate statements about aged peccadilloes, although this restriction does not apply to reports requested for larger transactions.[259] 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

256. *See* RESTATEMENT (SECOND) OF TORTS § 652C (1977) (stating that it is an invasion of privacy for someone to appropriate the name or likeness of another); *see also* CAL. CIV. CODE § 3344.1 (1999) (extending the right protect one's name or likeness from publicity for 70 years after death). For a survey of the evolving right of publicity in the United States, compare Theodore F. Haas, *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 a 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, *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 the First Amendment should prevail).

257. Rubin v. Coors Brewing Co., 514 U.S. 476, 482 (1995) (citing Central Hudson Gas & Electric Corp. v. Public Serv. Comm'n of N.Y., 447 U.S. 557, 562 (1980) (quoting Ohralik v. Ohio State Bar Ass'n, 436 U.S. 447, 455-56 (1978))).

258. 15 U.S.C. §§ 1681-1681s (1999).

259. *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 noncriminal 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 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).

personal data is collected and, in general, must not disclose it to anyone without the subscriber's consent.[260] The "Bork Bill," formally known as the Video Privacy Protection Act, also prohibits most releases of customers' video rental data.[261]

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.[262] More likely, this proves only that merchants in these two industries sell a great deal of sexually themed products and have no incentive to do anything to reduce their customers' confidence that their viewing habits will not become public knowledge. As a doctrinal matter, the statutes seem debatable. At least one other restriction upon the use of legally acquired transactional data failed on First Amendment grounds: When the state of Maine sought to require consumer consent before a firm could request a credit history, credit reporting agency Equifax won a judgment from the state supreme court holding that this was an unconstitutional restriction on its First Amendment right.[263]

3. *Fear.*

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. Law enforcement officials constantly seek new tools to compete in what they see as an arms race with terrorists, drug dealers, and other criminals.[264]

It would be well beyond the scope of this article to attempt to determine which of these fears are well founded, but any political attempt to restrict

---

260. *See* 47 U.S.C. § 551 (1999).

261. 102 Stat. 3195 (1988) (codified as 18 U.S.C. § 2710 (1999)). The act allows videotape rental providers to release customer names and addresses to third parties so long as there is no disclosure of titles purchased or rented. Customers can, however, be grouped into categories according to the type of film they rent. *See id.* § 2710(b)(2)(D)(ii).

262. *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 successfully challenged on First Amendment grounds).

263. *See generally* 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).

264. *See* A. Michael Froomkin, T*he Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709, 850-60 (1995) (discussing fear in the context of constitutional archetypes) <http://www.law.miami.edu/~froomkin/articles/clipper.htm>.

personal data collection will have to confront these fears, whether they are well founded or not.

In arguing 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.[265] Law enforcement officials are generally not required to obtain warrants in order to examine things that people have no reasonable expectation of keeping private; expanding the reasonableness of privacy expectations would mean that law enforcement officials would have to secure warrants before aiming new technologies at homes or bodies. The answer to the subtle fear may be a counter-fear: The more commonplace that ubiquitous surveillance becomes, the less the Fourth Amendment will be able to protect the average citizen.

B. *Making Privacy Rules Within the Constraints*

The result 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.

1. *Nonlegal proposals.*

Proposals for nonlegal solutions to the problem of privacy-destroying technologies 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 I 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 to ensure new ones do not arise.

---

265. *See* Morton, *supra* note 198, at 1470 (noting that current Fourth Amendment law is settled in regard to an individual's reasonable expectation of privacy).

a. *"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 self-regulate.[266] Since the economic incentive to provide strong privacy protections is either weak, nonexistent, or at least non-uniformly 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.[267]

Without some sort of government intervention to encourage self-regulation, "[w]olves self-regulate for the good of themselves and the pack, not the deer."[268] 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 $6900 per year to license it.[269] 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 alleging that firms have violated their privacy policies. It currently receives about 375 complaints per year, and finds about twenty percent to be valid, triggering additional investigation. These decisions do not appear to be published save in exceptional circumstances.[270]

The meaningfulness of the "trustmark" recently was called into question by the actions of a trustmark holder. TRUSTe confirmed that thirteen million copies of trustmark holder RealNetworks' RealJukebox Software had 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 create a

---

266. *See* William J. Clinton & Albert Gore, Jr., *A Framework for Global Electronic Commerce* § 2 (1997) (the "E-Commerce White Paper") <http://www.iitf.nist.gov/eleccomm/ecomm.htm>.

267. *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 3, 11 (U.S. Dep't of Commerce ed., 1997) (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).

268. Roger Clarke, *The Legal Context of Privacy-Enhancing and Privacy-Sympathetic Technologies*, Apr. 12, 1999 <http://www.anu.edu.au/people/Roger.Clarke/DV/Florham.html>.

269. *See* <http://www.truste.com/users/users_lookup.html> (describing TRUSTe's services).

270. *See id.* at *Investigation Results* <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 six investigations (as of April 2000).

profile of their listening habits.[271] 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 its web pages rather than Internet-related privacy intrusions.[272] A similar distinction between data collected via a web page and data collected by user-run software allowed Microsoft to 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.[273] 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.[274]

The RealNetworks incident followed an earlier, similar fiasco in which the FTC settled a complaint against GeoCities.[275] The FTC charged that GeoCities "misrepresented the purposes for which it was collecting personal identifying information from children and adults."[276] 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

---

271. *See RealNetworks' Privacy Intrusion*, JUNKBUSTERS <http://www.junkbusters.com/ht/en/real.html> (detailing the controversies surrounding the GUID discovery); *TRUSTe*, *Truste & RealNetworks Collaborate to Close Privacy Gap* <http://www.truste.org/about/about_software.html> (describing TRUSTe's efforts to resolve the GUID situation); *RealJukebox Update*, REALNETWORKS <http://www.realnetworks.com/company/privacy/jukebox/privacyupdate.html> (announcing RealNetwork's release of a software update designed to address customer concerns about privacy); Robert Lemos, *Can You Trust TRUSTe?*, ZDNET NEWS, Nov. 2, 1999 <http://www.zdnet.com/zdnn/stories/news/0,4586,2387000,00.html> (claiming that TRUSTe does not take active measures to assure that its license holders do not violate consumer privacy).

272. *See TRUSTe & RealNetworks Collaborate*, *supra* note 271 (explaining that the GUID incident was outside the scope of TRUSTe's privacy seal program because it did not involve collection of data on RealNetworks' website); *see also TRUSTe FAQ* <http://www.truste.org/users/users_investigationfaqs.html> (stating that TRUSTe does not deal with software or offline privacy practices but only with information collected and used by web sites).

273. *See Watchdog #1723—Microsoft Statement of Finding*, TRUSTe <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).

274. *See TRUSTe &RealNetworks Collaborate*, *supra* note 271 (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).

275. *See* Jamie McCarthy, *TRUSTe Decides Its Own Fate Today*, SLASH DOT, Nov. 8, 1999 <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).

276. Janet Kornblum, *FTC, GeoCities Settle on Privacy*, CNET NEWS, Aug. 13, 1998 (quoting on FTC statement) <http://news.cnet.com/news/0-1005-200-332199.html>.

level, income, marital status, occupation, and interests] would not be released to anyone without the member's permission."[277] 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.[278] In settling the case, GeoCities issued a press release denying the allegations. GeoCities then changed its privacy policy to state 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 occurred without consent). TRUSTe, which had issued a trustmark to GeoCities during the FTC investigation, did not remove it.[279]

Critics 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.[280] If TRUSTe were to start suspending trustmarks, it would lose revenue; if it were to get a reputation for being too aggressive toward clients, they might decide they are better off without a trustmark and the attendant hassle. In the absence of a meaningful way for consumers to evaluate the meaning of a trustmark or competing certifications,[281] TRUSTe certainly has no economic incentive to be tough on its funding sources.

Perhaps the most troubling aspect of the TRUSTe story is that TRUSTe's defense of its actions has a great deal of merit: The expectations loaded upon 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.[282] 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 avoid 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

---

277. *Id.* (quoting GeoCities' membership sign-up form).

278. *Id.* (quoting FTC statement).

279. *See* Jamie McCarthy, *Is TRUSTe Trustworthy?*, THE ETHICAL SPECTACLE, Sept. 1998 <http://www.spectacle.org/998/mccarthy.html> (detailing the denial).

280. *See* TRUSTe, TRUSTe Sponsors <http://www.truste.org/about/about_sponsors.htm> (listing TRUSTe's corporate sponsors).

281. *See* McCarthy, *supra* note 275 (noting that TRUSTe is by far the industry leader in the United States. Its only competitor, BBBOnline, has fewer than 100 members, compared to TRUSTe's 750.).

282. *See, e.g.*, note 273 *supra*.

motivated or principled enough to take part in them. It may be that competitive pressures might ultimately drive firms to seek privacy certification, but currently fewer than 1000 firms participate in either TRUSTe's or BBBOnline's programs, which suggests that market pressure to participate is 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 seeking to collect personal information from minors.[283] Even 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, it still does not mean that the FTC's response is the only way to proceed.

The United States may be unique in endorsing self-regulation without legal sanctions to incentivize or enforce it;[284] it is hard to believe that the strategy is anything more than a political device to avoid regulation. It does not follow, however, that self-regulation is a bad idea, so long as legal conditions create incentives for parties to engage in it seriously. For example, an enormous amount of energy has gone into crafting "fair information practices."[285]

One way of creating incentives for accurate, if not necessarily ideal, privacy policies would be to use legislation, 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 collect personal data were required to disclose what they collect and what they do with it, 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. Indeed, the surreptitious harvesting of music preference data by RealJukeBox motivated two sets of enterprising lawyers to file class action lawsuits.[286] One federal class action suit alleged misrepresentation and violation of the Computer Fraud and Abuse Act.[287] 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

---

283. *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).

284. *See* ROGER CLARKE, SENATE LEGAL AND CONSTITUTIONAL REFERENCES COMMITTEE INQUIRY INTO PRIVACY AND THE PRIVATE SECTOR (July 7, 1998) <http://www.anu.edu.au/people/Roger.Clarke/DV/SLCCPte.html>

285. *See*, *e.g.*, OECD, GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA <http://www.oecd.org/dsti/sti/it/secur/prid/PRIV-EN.HTM>; Roger Clarke, *Internet Privacy Concerns Confirm the Case for Intervention* <http://www.anu.edu.au/people/Roger.Clarke/DV/CACM99.html>.

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

287. 18 U.S.C. § 1030 (1999).

plaintiffs seek a refund of the thirty dollars that some users paid for the registered version of the software. In the California case, plaintiffs plan to base damages upon their estimate of the market value of data that RealJukebox collected; they will pick a figure after discovery.[288] Unfortunately for the plaintiffs, there is no reason to believe that even a great deal of music preference data is worth anything near the five hundred dollars per head that their lawyers estimated for the press. The willingness of the federal plaintiffs to sue for only thirty dollars per head suggests that creating a statutory damages remedy, even with only small damages, might create a sufficient incentive to police online privacy policies.

The web, however, is not the only source of concern; other means will be required to address different technologies.

b. *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."[289] 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. Such devices 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 integrated in a system design, or they can be a reaction to it. Law can encourage the deployment of PETs, but it can also discourage them, 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."[290] It is a worthy goal and should be part of a comprehensive response to privacy-destroying technologies.

Sometimes overlooked, however, are the ways in which existing law can impose obstacles to PETs. Laws and regulations designed to discourage the spread of cryptography are only the most obvious examples of impediments

---

288. *See* McWilliams, *supra* note 286.

289. Herbert Burkert, *Privacy Enhancing Technologies and Trust in the Information Society* (1997) <http://www.gmd.de/People/Herbert.Burkert/Stresa.html>.

290. Reidenberg, *supra* note 267, 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 that do not protect personal data through PETs should be subject to legal liability).

to privacy-enhancing technology. Legal obstacles to privacy self-help also extend to the lowest technologies, such as antimask laws. In some cases, all PETs may need to flourish is the removal of legal barriers.

Privacy can be engineered into systems design,[291] systems can be built without much thought about privacy, or they can be constructed in ways intentionally designed to destroy it, in order to capture consumer information or 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 include privacy protections if they so choose. For example, when designing a road-pricing system, transponders can be connected to a card that records a toll balance and deducts funds as needed. No data identifying the driver or the car is needed, just whether there are sufficient funds. Or, the transponder can instead emit a unique ID code, keyed to a record, that identifies the driver and either checks for sufficient funds or bills her. The first system protects privacy but requires an alternate way to charge drivers whose cards are depleted. The second system requires billing and can create a huge database of vehicular movements.[292]

In general, designers can organize the system to withhold (or never gather) data about the person, the object of the transaction, the action performed, or even the system itself.[293] Most electronic road-pricing schemes currently deployed identify the vehicle or an attached token.

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 caution. If PETs are not built into the system, or the user lacks confidence in its implementation, she may engage in self-help. The sort of technology that is likely to be effective depends upon the circumstances and the nature of the threats to privacy. If, for example, a person fears hidden cameras, then a pocket camera detector is just the thing.[294]

---

291. For some suggested basic design principles, see INFORMATION AND PRIVACY COMMISSIONER/ONTARIO, CANADA & REGISTRATIEKAMER, *supra* note 180; *see also* Ian Goldberg, David Wagner & Eric Brewer, *Privacy-enhancing Technologies for the Internet* <http://www.cs.berkeley.edu/~daw/papers/privacy-compcon97-www/privacy-html.html> (describing existing PETs and calling for additional ones).

292. For a discussion of such systems, see generally *Santa Clara Symposium on Privacy and IVHS*, *supra* note 65.

293. *See* Herbert Burkert, *Privacy-Enhancing Technologies: Typology, Critique, Vision*, *in* TECHNOLOGY AND PRIVACY, *supra* note 178, at 125, 125-28.

294. *See* Carl Kozlowski, *Chicago Security-Device Shop Gets Caught in Privacy Debate*, CHI. TRIB., Dec. 16, 1999, *available in* 1999 WL 28717597 (describing $400 to $1600 pocket-sized detectors that vibrate when recording devices are near).

For matters involving electronic communications or data storage, encryption is the major PET.[295] Here, however, the United States government has engaged in a long-running effort to retard the spread of consumer cryptography that might be used to protect emails, 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.[296] As a panel of the Ninth Circuit concluded in an opinion subsequently withdrawn for en banc consideration:

> 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.[297]

Perhaps in fear of another adverse judgment from the Ninth Circuit, the government recently issued substantially liberalized encryption rules that for the first time allow the unrestricted export of cryptographic source code.[298] In a striking demonstration of the effects of a removal of government restrictions on PETs, the new rules emboldened Microsoft, the leading manufacturer of consumer PC operating systems, to pledge to include strong 128-bit encryption in the next release of its software.[299]

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 upon the party securing the data, but an exponential computational burden upon any would-be eavesdropper. Unlike so many other technologies, cryptography is relatively inexpensive and accessible to anyone with a com-

---

295. For a discussion of encryption, see generally Froomkin, *supra* note 264.

296. *See generally id.*; A. Michael Froomkin, *It Came From Planet Clipper: The Battle Over Cryptographic Key "Escrow*," 1996 U. CHI. LEGAL F. 15 (1996); Norman Andrew Crain, Commentary, Bernstein, Karn, *and* Junger*: Constitutional Challenges to Cryptographic Regulations*, 50 ALA. L. REV. 869 (1999).

297. Bernstein v. United States, 176 F.3d 1132, 1146 (9th Cir. 1999) (citations omitted), *opinion withdrawn, reh'g en banc granted*, 192 F.3d 1308 (9th Cir. 1999).

298. *See* Revisions to Encryption Items, 65 Fed. Reg. 2491 (2000) (to be codified at 15 C.F.R. pts. 734, 740, 742, 770, 772 & 774); *see also* Letter from the Dep't of Commerce, Bureau of Export Admin., to Cindy A. Cohn, attorney, McGlashnand Sarrail (Feb. 17, 2000) <http://www.cryptome.org/bxa-bernstein.htm> (explaining that source code is not considered "publicly available" and thus remains subject to post-export reporting requirements).

299. *See* Reuters, *Strong Encryption for Win 2000* <http://www.wired.com/news/technology/0,1282,33745,00.html>.

puter or a dedicated encryption device. Cryptography is no privacy panacea, however. It is difficult to implement properly, vulnerable to every security weakness in underlying operating systems and software programs, and even at its best, it 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 which had consequences in the networked era. For example, the prohibition against "reverse engineering" software—decompiling something to find out what makes it tick—may or may not be economically efficient.[300] But, it makes it nearly impossible for technically sophisticated users to satisfy themselves that programs are cryptographically secure, thus making 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 reexamination in light of the reduced privacy in public places. One possible reaction to ubiquitous cameras in public places would be widespread wearing of masks as fashion accessories. 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 more than one hundred years old.[301] The statutes make it a crime to appear in public in a mask.[302] Judicial opinion appears divided over whether prohibitions against appearing masked in public violate the First Amendment.[303] Regardless of the constitutional issues, it is undeniable that

---

300. *See* David McGowan, *Free Contracting, Fair Competition, and Article 2B: Some Reflections on Federal Competition Policy, Information Transactions, and "Aggressive Neutrality,"* 13 BERKELEY TECH. L.J. 1173, 1214–24 (1998); *cf.* Celine M. Guillou, *The Reverse Engineering of Computer Software in Europe and the United States: A Comparative Approach*, 22 COLUM.-VLA J.L. & ARTS 533 (1998) (contrasting rules generally allowing reverse engineering of software in the European Union with more restrictive rules in the United States).

301. *See, e.g.*, Walpole v. State, 68 Tenn. 370, 372-73 (1878).

302. *See* Wayne R. Allen, *Klan, Cloth and Constitution: Anti-Mask Laws and the First Amendment*, 25 GA. L. REV. 819, 821 n.17 (1991) (citing statutes from 10 states); Oskar E. Rey, *Antimask Laws: Exploring the Outer Bounds of Protected Speech Under the First Amendment—*State v. Miller*, 260 Ga. 669, 398 S.E.2d 547 (1990)*, 66 WASH. L. REV. 1139, 1145 (1991). Additionally, 18 U.S.C. § 241 makes it a felony for two or more persons to travel in disguise on public highways or enter the premises of another with the intent to prevent the free exercise and enjoyment of any legal right or privilege by another citizen. *See* 18 U.S.C. § 241 (1999).

303. Decisions holding antimask laws unconstitutional include: American Knights of Ku Klux Klan v. City of Goshen, 50 F. Supp. 2d 835, 840 (N.D. Ind. 1999) (holding that a 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 that a statute prohibiting wearing masks in public was overbroad and finding the state's fear that violence would result from the mere presence of anonymous persons is "unfounded").

existing antimask laws were enacted before anyone 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 antimask laws—if they are even constitutional under the right to anonymous speech enunciated in *McIntyre v. Ohio Elections Commission*[304]—will need rethinking.

2. *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 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.

a. *Transactional data-oriented solutions.*

Scholars and others have proposed a number of legal reforms, usually based upon either traditional property or intellectual property law, to increase the protection available to personal data by vesting the sole initial right to use

---

Cases upholding antimask laws include: Church of the American Knights of the Ku Klux Klan v. Safir, No. 1999 U.S. App. LEXIS 28106 (2d Cir. Oct. 22, 1999) (staying order of injunction against an 1845 New York state law forbidding masks at public demonstrations); Ryan v. County of DuPage, 45 F.3d 1090, 1092 (7th Cir. 1995) (upholding a rule prohibiting masks in the courthouse against a First Amendment challenge on grounds that the rule was reasonable because "[t]he wearing of a mask inside a courthouse implies intimidation"); Hernandez v. Superintendent, Fredericksburg-Rappahannock Joint Security Center, 800 F. Supp. 1344, 1351 n.14 (E.D. Va. 1992) (noting that a statute might have been held unconstitutional if petitioner had demonstrated that unmasking himself would have restricted his ability to enjoy free speech and freedom of association); Schumann v. State, 270 F. Supp. 730, 731-34 (S.D.N.Y. 1967) (denying temporary injunction of enforcement of a statute requiring licensing of assemblage of masked persons); State v. Miller, 398 S.E.2d 547 (Ga. 1990) (rejecting challenge to antimask statute); State v. Gates, 576 P.2d 1357, 1359 (Ariz. 1978) (rejecting a challenge to an antimask provision in an indecent exposure statute); *Walpole*, 68 Tenn. at 372-73 (enforcing statute); Hernandez v. Commonwealth, 406 S.E.2d 398, 401 (Va. Ct. App. 1991). *Compare* Allen, *supra* note 302, at 829-30 (arguing for the validity and retention of antimask laws), *with* Rey, *supra* note 302, at 1145-46 (arguing that antimask laws are unconstitutional).

304. 514 U.S. 334 (1995).

it in the data subject. Although current proposals are the product of great ingenuity and thus vary considerably, the common element is a desire to change the default rules in the absence of agreement. Changing the default rule to create a property interest in personal data, even when shared with a merchant, or visible in public, has a number of attractive properties.[305] 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 that makes it an offense to express what one sees or knows (such as who shops in one's store or who slept with whom) strikes dangerously close to core values of free speech.[306] Current doctrine leaves open a space for limited regulation of transactional data along the lines of the Cable Television Act and the Bork Bill.[307] 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."[308] 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 attraction of shifting the default rule is evident. Currently, user ignorance of the privacy consequences of disclosure, the extent of data collection, and the average value of a datum, combined with the relatively high transaction costs of negotiating privacy provisions in consumer transactions governed by standard form clauses, causes privacy issues to 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.[309] Shifting the default rule to require a data collector to make some sort of agreement with her subject before having a right to reuse her data gives the subject the benefit of notice and of transaction costs.

---

305. For a micro-economic argument that this change would be efficient given existing market imperfections, see Kenneth C. Laudon, *Extensions to the Theory of Markets and Privacy: Mechanics of Pricing Information*, *in* PRIVACY AND SELF-REGULATION IN THE INFORMATION AGE, *supra* note 275, at 41.

306. *See, e.g.*, Rochelle Cooper Dreyfuss, *Finding (More) Privacy Protection in Intellectual Property Lore*, 1999 STAN. TECH. L. REV. VS 8 <http://stlr.stanford.edu/STLR/Symposia/Privacy/index.htm>; Diane Leenheer Zimmerman, *Information as Speech, Information as Goods: Some Thoughts on Marketplaces and the Bill of Rights*, 33 WM. & MARY L. REV. 665 (1992) (worrying that this is a bad thing).

307. *See* text accompanying notes 260-262 *supra*.

308. Kang, *supra* note 16, at 1293 n.332.

309. *See, e.g.*, Paul Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1686 (1999) (noting "the lack of incentives to make the majority of firms oppose their self-interest, which lies in maintaining the status quo").

The transaction cost element is particularly significant, but also potentially misleading. Shifting the default rule 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 transaction costs are symmetrical. The very structural features of market exchange that make it costly for individuals to negotiate exceptional privacy clauses in today's market make it inexpensive for the author of the standard form clause to award it in order to include a conveyance of the data and a consent to its use.[310]

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 upon 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 that are reducing the transactions costs of particularized contracting 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 becoming 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 would require that failure to convey rights to personal data have no repercussions. 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.[311]

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 a consumer's

---

310. *Cf.* Philip E. Agre, *Introduction*, *in* TECHNOLOGY & PRIVACY, *supra* note 178, at 1, 11 (noting an information asymmetry between firms and consumers: firms control the releases of information about themselves and about what information they have on consumers).

311. Viktor Mayer-Schönberger, *Generational Development of Data Protection in Europe*, *in* TECHNOLOGY & PRIVACY, *supra* note 178, at 219, 232.

freedom to contract away her right to certain classes of data, such as information about race, religion, and political opinions.[312] While likely to be an effective privacy-enhancing solution, this is neither one that corrects market failure in order to let the market reach an efficient outcome, nor one that relies on property rights; it thus eliminates the most common justifications for property-law-based proposals to data privacy.[313]

b. *Tort law and other approaches to public data collection.*

Tort- and criminal-law-based proposals to enhance data privacy tend to differentiate between data collected in places where one has a reasonable expectation of privacy, such as one's home, and public places where the law usually presumes 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. Where previously the tort often required the tortfeasor's presence in the private space,[314] the proposal allows the presence requirement to be fulfilled virtually.[315] 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 extended to cover CCTV and other forms of public tracking. Traditionally, privacy torts do not protect things in public view on the theory that such things are, by

---

312. *See id.* at 233.

313. *Cf.* Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 GEO. L.J. 2381, 2410-16 (1996); Carl Shapiro & Hal R. Varian, U.S. *Government Information Policy* 16 <http://www.sims.berkeley.edu/~hal/Papers/policy/policy.html>.

314. The tort currently requires an objectively reasonable expectation of privacy in place or circumstances. *See* RESTATEMENT (SECOND) OF TORTS § 652B (1965). Some jurisdictions also require an actual trespass by the defendant. *See, e.g.*, Pierson v. News Group Publications, Inc., 549 F. Supp. 635, 640 (S.D. Ga. 1982).

315. "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 195, at 1054-59 (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).

definition, not private.[316] Expanding them to cover public places would conflict directly with the First Amendment.

Some states have chosen to promote specialized types of privacy through targeted statutes. California's antipaparazzi statute may be a model.[317] It carefully focuses on creating liability for the gathering of information by private persons using sense-enhancing tools. While expanding the zone of privacy in the home, treating one's property line like a wall impermeable to data, the statute does not cover activities on public streets and purposely avoids 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.[318] Perhaps it is time to call for regulation of "snooper's

---

316. *See* Dow Chemical Co. v. United States, 476 U.S. 227, 239 (1986) (holding that taking aerial photographs is not a Fourth Amendment search); Shulman v. Group W Prod., Inc, 955 P.2d 469, 490 (Cal. 1998) (distinguishing between an accident scene, in public view, and medivac helicopter, where there was a reasonable expectation of privacy); *see also* PROSSER AND KEETON ON THE LAW OF TORTS § 117 (5th ed. 1984).

317. CAL. CIV. CODE. § 1708.8(b) (West 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.

318. 18 U.S.C. § 2512(1)(a), (b) (2000):

> 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.

tools," akin to the common law and statutory regulation of "burglar's tools?"[319]

Both of these approaches have potential, although both also have practical limitations in addition to 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 both knowledge about the technology, and the chance of public outrage and legislative action are minimal. As for the California antipaparazzi statute, it only applies to private collection of sense-enhanced data. It addresses either data collection by law enforcement nor database issues.[320] And, as noted, it does not apply to public spaces.

c. *Classic data protection law*.

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, reuse, or resale of data, the Union's rules, as well as those of various European nations, also contain specific limits on the collection of sensitive types of data.[321] European Union restrictions on 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.[322] These extraterritorial rules do not, however, require that foreign data collection laws meet the Union's standards, leaving the United States on its own to decide what protections, if any, it should enact to safeguard its consumers and citizens.

So far, laws have been few and generally narrow, with the California antipaparrazi statute 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 about to begin. Late last year the FTC promulgated detailed rules restricting the collection of data online from children under thirteen

---

319. *See* Annotation, *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.").

320. For a criticism of these and other limitations, see *Privacy, Technology, and the California "Anti-Paparazzi" Statute*, *supra* note 198, at 1378-84.

321. *See* Mayer-Schönberger, *supra* note 311, at 232; SCHWARTZ & REIDENBERG, *supra* note 5.

322. *See* SWIRE & LITAN, *supra* note 5; SCHWARTZ & REIDENBERG, *supra* note 5.

without explicit parental consent. These rules are due to come into effect in April, 2000.[323]

III. IS INFORMATION PRIVACY DEAD?

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 invasion of 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."[324] Instead, perhaps anticipating smart dust, he suggests that the chief effect of privacy laws will be "to 'make the bugs smaller.'"[325] 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."[326] Having concluded that privacy as we knew it is impossible, Brin goes on to argue that the critical policy issue becomes whether 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 are 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 in Part I. Current privacy laws in the United States make up at best a thin patchwork, one that is plainly inadequate to meet the challenge of new data acquisition technologies. General international agreements that address the privacy issue are no better.[327] Even the vastly more elaborate privacy laws in Europe and Canada permit almost any

---

323. *See* FTC Children's Online Privacy Protection Rule, 16 C.F.R. § 312.5 (effective Apr. 21, 2000), (requiring parental consent prior to collection of information from children under thirteen).

324. BRIN, *supra* note 11, at 8-9.

325. *Id*. at 13.

326. *Id*.

327. International agreements to which the United States is a party speak in at least general terms of rights to privacy. Article 12 of the Universal Declaration of Human Rights, adopted by the United Nations in 1948, states that "[n]o one shall be subjected to arbitrary interference with his privacy, family, home or correspondence." G.A. Res. 217A (III), U.N. GAOR, 3d Sess., Supp. No. 13, at 71, UN Doc. A/810 (1948) <http://www.hrweb.org/legal/udhr.html>. Similarly, Article 17 of the International Covenant on Civil and Political Rights states that "[n]o 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." International Covenant on Civil and Political Rights, March 23, 1976, art. 17, 999 U.N.T.S. 171 <http://www.unhchr.ch/html/menu3/b/a_ccpr.htm>.

Both agreements state that "[e]veryone has the right to the protection of the law against such interference or attacks."

consensual collection and resale of personal data.[328] The world leader in the deployment of surveillance cameras, the United Kingdom, has some of 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 various forms of surveillance: In the words of one Canadian Information and Privacy Commissioner, "the pressures for surveillance are almost irresistible."[329]

Despite the very weak legal protections of informational privacy in the United States today, there is an agreement that Brin's pessimism about the potential for law to control technology and Scott McNealy's defeatism 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.[330] It would be naive in the extreme to suggest that either of these practices completely disappeared as a result of their illegality; 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,[331] there would be much more wiretapping and eavesdropping.

Even the drug war, which surely stands for the proposition that the law has its 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. There are many different kinds of laws, and command and control regulation is often the least effective option.[332]

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 mechanism that creates an incentive for some-

---

328. Potentially invidious categories such as ethnicity are sometimes subject to special regulation.

329. David H. Flaherty, *Controlling Surveillance: Can Privacy Protection Be Made Effective*, *in* TECHNOLOGY & PRIVACY, *supra* note 178, at 167, 170.

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

331. In the case of analog cellular phones, the tools are available in most Radio Shacks, although they require slight modification. *See* RICH WELLS, RADIO SHACK PRO-26 REVIEW <http://www.durhamradio.ca/pro26r.htm>; *cf.* Boehner v. McDermott, 191 F.3d 463, 465 (D.C. Cir. 1999) (describing the use of a scanner to eavesdrop).

332. *See generally* Richard B. Stewart, *The Reformation of American Administrative Law*, 88 HARV. L. REV. 1667 (1975).

one to police for compliance, legal rules will have at best limited effectiveness.[333] 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 statutory damages for falsifying privacy policies,[334] 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 demonstrates, 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. Privacy-destroying technologies do not line up particularly well with the legal rules that govern them. This explains why the United States Constitution is unlikely to be the source of a great expansion in informational privacy rights. The Constitution does not speak of privacy, much less informational privacy. Even though the Supreme Court has acknowledged that "there is a zone of privacy surrounding every individual,"[335] the data contours of that "zone" are murky indeed. The Supreme Court's relatively few discussions of informational privacy tend to be either in dicta or in the context of finding other interests more important,[336] or both.[337] Similarly, familiar constitutional categories such as public forums, limited public forums, and nonpublic forums map poorly on future debates about how to create or protect zones of privacy against privacy-destroying technologies.

The variety of potential uses and users of data frustrate any holistic attempt to protect data privacy. Again, constitutional doctrine is illustrative. Whatever right to informational privacy may exist today, it is a right against governmentally sponsored invasions of privacy only—it does not reach pri-

---

333. *See* Robert Gellman, *Does Privacy Law Work?, in* TECHNOLOGY & PRIVACY, *supra* note 293, at 193, 214-15.

334. *See* text following note 288 *supra*.

335. Cox Broadcasting Corp. v. Cohn, 420 U.S. 469, 487 (1975); *see also* Griswold v. Connecticut, 381 U.S. 479, 484-85 (1965) (describing how the Third and Ninth Amendments create "zones of privacy").

336. *E.g.*, Nixon v. Administrator of Gen. Serv., 433 U.S. 425, 465 (1977) (suggesting that the former President has a 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, 599 (1977) (finding that whatever privacy interest exists for patients in information about their prescriptions was insufficient to overcome the compelling state interest).

337. The leading counterexample to this assertion is *United States Dept. of Justice v. Reporters Comm. for Freedom of Press*, 489 U.S. 749 (1989), in which the Supreme Court held that there was a heightened privacy interest in an FBI compilation of otherwise public information sufficient to overcome an FOIA application. Even if the data contained in a "rap sheet" were available in public records located in scattered courthouses, the compilation itself, the "computerized summary located in a single clearinghouse" was not. *Id.* at 764.

vate conduct.[338] Thus, even if the courts were to find in the federal Constitution a more robust informational privacy right, it would address only a portion of the problem.[339]

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 upon the context. Sense-enhanced searches, for example, tend to be treated as Fourth Amendment issues when conducted by the government. If the intruder is private, the Fourth Amendment is irrelevant. Instead, one might have to consider whether her actions constitute an invasive tort of some type (or perhaps even a misappropriation of information), who owns the information, and whether a proposed rule

---

338. Other than its direct prohibition of slavery, the United States 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 "[e]very 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. *See* 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. ST. U. L. REV. 25, 53 (1997).

339. Some state constitutions go further. *Compare* State v. Hunt, 450 A.2d 952 (N.J. 1982) (holding that the New Jersey state constitution creates a protectable privacy interest in telephone billing records), *with* United States v. Miller, 425 U.S. 435 (1976), *and* California Bankers Assn. v. Shultz, 416 U.S. 21 (1974) (finding no such right in the Federal Constitution).

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, § I.

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. *See* 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 an individual's right to prevent the "dissemination or misuse of sensitive and confidential information"; (2) a "reasonable expectation of privacy" based on "an objective entitlement founded on broadly based and widely accepted community norms"; and (3) a "serious invasion" of privacy by the defendant. *Id*. at 654-55. Even then, the court stated that privacy claims must be balanced against countervailing interests asserted by the defendant. *Id*. at 653.

limiting the acquisition or publication of the information might run afoul of the First Amendment.[340]

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 encouraging the adoption of fair information practices and the 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; the converse is also true: Rules about data retention and use will shape what is collected and how it is done.[341]

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, or it will indeed be too late.

---

340. 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 answer may be different. 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. *Cf.* United States Department 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).

341. The line of cases beginning with *New York Times Co. v. Sullivan*, 376 U.S. 254 (1964), is a good example of this phenomenon. Case law defining the circumstances in which a publisher could defend itself against a charge of libel—a problem of data use—generates a set of rules and procedures defining data collection actions that reporters must obey in order to be able to prove they complied with basic norms of due care.