

Technological Change and the Destruction of Informational Privacy

A. Michael Froomkin¹
Professor of Law
University of Miami
Coral Gables, USA

Introduction

Both the state and the private sector now enjoy unprecedented abilities to collect personal data regarding individuals. Foreseeable technological developments suggest that costs of data collection and surveillance will decrease, while the quantity and quality of data will increase. This acceleration in data-collection poses new challenges to data privacy law. Existing regulatory regimes, often placing the most emphasis on regulation of data *collation* rather than *collection*, seem poorly equipped to combat this trend.

The easiest way for the individual to control data about himself is to keep information to himself: If information never gets collected in the first place, database issues need never arise. Although privacy-enhancing technologies such as encryption provide a limited ability to protect some data and communications, it seems obvious that total secrecy of this sort is rarely a practical possibility today unless one lives as a hermit. Indeed, cryptography expert Bruce Schneier's new book, *Secrets & Lies*² argues that in the real world, total data security is simply a myth even for highly motivated corporations.

For individuals, lacking the resources of corporations, the data privacy picture is even grimmer. Many basic transactions that form a part of ordinary life in industrialized countries, from getting a driver's license to taking a job, now require identification.³ Homes are permeable to high-tech gadgets used by the police and others; medical and financial data is widely shared; communications are easily monitored. Personal lives thus are becoming increasingly transparent to governments, interested corporations, and even to other citizens. 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 the individual's control.

I. New Technologies—and Old

1. Professor of Law, University of Miami School of Law. B.A. Yale, M.Phil Cambridge, J.D. Yale. Email: froomkin@law.tu. © Copyright 2000 A. Michael Froomkin.

2. BRUCE SCHNEIER, *SECRETS & LIES* (2000).

3. *See, e.g.*, 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).

The cost and variety of tools available to acquire personal data is changing rapidly. Both technologies that facilitate the acquisition of raw data and those that allow processing and collation of data are improving and becoming cheaper. 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.

Old technologies facilitated the collection of vast amounts of personal data. The introduction of new technologies, however, promises to raise the quantity and nature of the information that could be collected to new, somewhat dizzying, heights.

A. *Old Technologies*

Even without high technology, substantial amounts of personal data are routinely collected about almost everyone in the United States. Examples include:

- By the Federal Government
 - annual collection of personal and corporate tax data
 - the decennial census
 - data regarding everyone receiving public assistance
- By the states
 - data collected as a condition of issuing driver's licenses,
 - data collected as a condition of other permits and licenses
- By the private sector
 - vast amounts of data collected by the private sector in the course of selling products and services.

Federal, state, and local governments also collect data from a total of about fifteen million arrestees each year.⁴

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. Sometimes the data is collected purely for commercial purposes, but sometimes the data collection is wholly or partly at the behest of the government even when the transaction is private. For example, financial data is collected from mixed motives. The data have commercial value, but there are also government requirements that require financial intermediaries to 'know their customer' and to make routine reports to assist law enforcement efforts concerning suspicious transactions.

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. Similarly, alternatives to cash, such

4. 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>.

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.

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.

B. *New Technologies for Ubiquitous Surveillance*

If current trends are left unchecked, someday, not too far in the future, there will be no place on earth where an ordinary person will be able to avoid surveillance.

Public places will be watched by terrestrial cameras and 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 scanned and sorted. Copyright protection "snitchware" 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, there may be nowhere to hide and little that can stay hidden.

1. Public spaces

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 technologies include:

- cameras,
- facial recognition software,
- vehicle identification systems.
- sense-enhanced searches
- satellite monitoring

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.

Cameras. Public streets and many formally private but publically accessible spaces such as shopping centers are monitored by Closed Circuit Television ("CCTV") cameras and video recorders. Even the workplace is being filled with cameras, as they are increasingly small and easy to

place, being easy to conceal in “clocks, radios, speakers, phones, and many other items.”⁵ Although public cameras are common in the United States,⁶ they are even more widespread elsewhere. The United Kingdom has pursued a particularly aggressive program of blanketing the nation with cameras. They are used in cities, villages, schools, hospitals and on roads.⁷

Cell Phone Tracking 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). The finer the cell phone zone, the more precisely a person’s location can be identified.

The privacy-destroying consequences of both cell phone tracking and public cameras increase dramatically when the information collected 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.⁸ However atypical the collection and retention of cellular phone subscribers’ movements may be, the Swiss phone company’s actions are clearly not unique.⁹ 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 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

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

6. 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).

7. 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>.

8. 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>>.

9. 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).

security.¹⁰

Vehicle Monitoring. 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.¹¹ Ultimately, ITS promise continuous, real-time information as to the location of all moving vehicles.¹² Less complex systems already create travel records that can be stored and accessed later.¹³

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. Sense enhanced searches are not yet routine, perhaps because of the rarity or expense of the necessary equipment. The typical sense-enhanced search is targeted at someone or something specific, or carried out at specific and usually temporary locations. Sense-enhanced searches allow someone on the outside to see what is happening inside a building, a package, or even clothing. 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. 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.

Satellite monitoring. Once the sole property of governments, high-quality satellite photographs in the visible spectrum are now available for purchase. The sharpest pictures on sale today are able to distinguish objects two meters long,¹⁴ with a competing one-meter resolution service planned for later this year.¹⁵ 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. The United Kingdom is considering the adoption of a GPS-based system, already field tested in the Netherlands and Spain,¹⁶ to prevent speeding.

That a government can track a device designed to be visible by satellite does not, of course,

10. 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>>.

11. 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”).

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

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

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

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

16. 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).

necessarily mean that an individual without one could be tracked by satellite. 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.

2. *Monitoring in the home and office*

Even before the recent revelation of technologies such as the FBI's "Carnivore" packet-sniffing system, it was clear that existing technology is capable of monitoring every telephone call, fax, or email. The constraints on monitoring are legal ones, and also the technological impossibility (at least for civilian services) of sorting through so much information. In some areas, such as the workplace and Internet use, the legal constraints are already limited. In the U.S., employers may use hidden cameras, monitoring software, and other forms of surveillance more or less at will.¹⁷ Ubiquitous and hidden monitoring is easily affordable. Software designed to capture keystrokes, either overtly or surreptitiously, is also readily available. In addition, every technology described below that can be targeted at the home can also be targeted at the office.

As voiceprint, voice recognition, and content-analysis technology continue to improve, however, the tasks of sorting communications will be subjected to increasingly sophisticated automated processing.¹⁸ Over time, this will remove the technological constraint, leaving only legal ones. On May 7, 1999, the European Parliament passed the Lawful Interception of Communications Resolution on New Technologies,¹⁹ known as Enfopol. Although the Enfopol

17. 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). It is not legal to spy on employee changing rooms and bathrooms.

18. 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).

19. 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.europa1.eu.int/omk/omnsapir.so/pv2?PRG=DOCPV&APP=PV2&LANGUE=EN&SDOCTA=5&TXTLST=1&POS=1&Type_Doc=RESOL&TPV=PROV&DATE=070599&Pr gPrev=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>>.

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.²⁰

According to a report prepared for the European Parliament, the United States and its allies maintain a massive worldwide spying apparatus capable of capturing all forms of electronic communications.²¹ Known as “Echelon,” the network can “access, intercept and process every important modern form of communications, with few exceptions.”²² The network is supported by a variety of processing technologies, including Voiceprint recognition, which determines whether any of the participants in a call are on a watch list,²³ and dictionary programs that flag text messages (faxes and emails) with interesting references or word patterns.²⁴

Even if all the allegations are true, however, Echelon is limited to an intelligence gathering role. It is not (now) a technology commonly used for law enforcement or marketing. In those realms, however, a number of quite legal technologies are already being deployed to track and archive many uses of the web. The aspects of the web that make it 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 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

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

21. 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>>.

22. *Id.* at Summary ¶ 2.

23. “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.

24. See *id.* § 3 ¶ 72.

that too will be disclosed automatically.²⁵ 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 ZeroKnowledge²⁶ or the anonymizer to mask personal information.²⁷ 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.²⁸

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. 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.

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. Cookies, however, are only the tip of the iceberg. Far more intrusive features can be integrated into browsers, into software downloaded from the Internet,²⁹ and into viruses or Trojan horses.³⁰ In the worst case, the software could be configured to record every keystroke.

The problems are by no means limited to software. Hardware manufacturers are also deploying privacy-compromising features in a wide variety of devices. For example:

- Biometric devices

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

26. See <<http://www.zeroknowledge.com>>.

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

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

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

30. 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>>.

- Vehicles equipped with devices programmed to act similar to flight data recorders;³¹
- Computer chips and ethernet card adapters with unique serial numbers
- Sense-enhanced searches
- Smart dust

Biometric Devices. 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, DNA is a particularly powerful identifier. It is almost unique³² and (so far) impossible to change. 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.³³ Others may provide the capability to detect states of mind, truthfulness, fear, or other emotions.³⁴

Vehicle Black Boxes. 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 recorded "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."³⁵

31. 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>>.

32. See *DNA Fingerprinting*, ENCYCLOPEDIA BRITANICA 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)").

33. 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 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> 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.").

34. See generally Dutch Data Protection Authority (Registratiekamer), R. Hes, T.F.M. Hooghiemstra & J.J. Borking, *At Face Value: On Biometrical Identification and Privacy* §§ 2.2-2.3 (1999) <http://www.registratiekamer.nl/bis/top_1_5_35_1.html>.

35. 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>>.

Unique ID Numbers. 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.³⁶ The intention appears to have been to make electronic anonymity impossible. Anonymous users might, Intel reasoned, commit fraud or pirate digital intellectual property.³⁷ With a unique, 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 count-ers, and other means of tracking users across the Internet.

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 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 mis-delivered. 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"),³⁸ 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.³⁹ Thus, "[e]very packet you send out onto the public Internet using IPv6 has your fingerprints on it. And unlike your IP address under IPv4, which you can change, this address is embedded in your hardware. Permanently." In response to criticism, the standard-setting bodies are reconsidering revisions which would allow

36. 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.").

37. See Patrick Gelsinger, *A Billion Trusted Computers* (Jan. 20, 1999)
<<http://www.intel.com/pressroom/archive/speeches/pg012099.htm>>.

38. 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>>.

39. See King et al., *supra* note 38, 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).

users-if they are savvy enough to do so-to pick a random number to replace the GUID from time to time.⁴⁰ But this modification is still under consideration and would not, apparently, be the default.

Sense-enhanced Searches. Suitably equipped observers can now draw informed conclusions about what is occurring within a house without having to enter it, or what is in a package without opening 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 preëxisting emanations. Thermal imaging, for example, allows law enforcement to determine whether a building has “hot spots”⁴¹ and computer monitors broadcast signals that can be replicated from a considerable distance.⁴² Computer programs and viruses can use this capability to surreptitiously broadcast information other than what is displayed on the screen.

If stealth access is not required, very intrusive searches are possible without actually touching an object or opening a container. Passive millimeter wave imaging reads the electromagnetic radiation emitted by an object.⁴³ Much like an X-ray, this technology can specifically identify the

40. 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>>.

41. 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, 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 Battlefield 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).

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

43. 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).

radiation spectrum of most objects carried on the person, even those in pockets, under clothes, or in containers.⁴⁴ It thus allows the user to see through clothes, and conduct a “remote frisk” for concealed weapons,⁴⁵ or other contraband.⁴⁶ Imagers are available as handheld scanners, visible gateway scanners, or in hidden surveillance models.⁴⁷

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.

Smart dust. The goal of the “smart dust” project – which contemplates a network of miniature sensors floating around in the air – 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. 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.⁴⁸

44. See Millivision, *Security Applications* <<http://www.millivision.com/security.html>>; Merrick 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).

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

46. See Millivision, *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.”).

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

48. 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/>>.

II. Responding to Privacy-Destroying Technologies in the Face of Privacy Myopia

The prospect of “smart dust,” of cameras too small to see with the naked eye, evokes a world without privacy.⁴⁹ As the previous discussion demonstrates, however, even without ubiquitous micro-cameras, 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.

Currently, the default rule in the US is unfriendly to consumer information privacy.⁵⁰ The original alienation of personal data may have occurred with the consumer’s acquiescence or explicit consent. Every economic transaction has at least two parties; in most cases the facts of the transaction belongs equally to both.⁵¹ With a few generally minor exceptions,⁵² both sides to a transaction generally are free to sell the facts of the transaction to any interested third party. Overall, the number of transactions in which confidentiality is the legal default appears relatively small compared to the total number of transactions in the US economy.

A. *The Problem of Privacy Myopia*

Any effective response to privacy-destroying technologies will likely be constrained by market failure caused by rational but myopic, imperfectly informed consumers. Privacy myopic consumers will sell their data too often and too cheaply.

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

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

50. 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).

51. See Spiros Simitis, *From the Market to the Polis: The EU Directive on the Protection of Personal Data*, 80 IOWA L. REV. 445, 446 (1995) (noting traditional view, now retreating in Europe, that “data . . . were perfectly normal goods and thus had to be treated in exactly the same way as all other products and services”).

52. 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. E.g. MODEL CODE OF PROFESSIONAL RESPONSIBILITY Canon 4 (1999); MODEL RULES OF PROFESSIONAL CONDUCT Rule 1.6. (1999).

standing alone. And, assume that once some threshold has been reached the value of additional data to a potential profiler remains linear and that there are not declining returns from another datum. Finally, assume that data brokers or profile compilers are able to buy consumer data from merchants at low transactions costs because these are repeat transactions between repeat players in which substantial amounts of data change hands., Consumers, however, are not aware of the value of their aggregated data to a profile compiler. With the possible exception of the assumption that profilers cannot overdose on data about a given consumer, these all seem to me to be very tame and reasonable assumptions.

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

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

Unfortunately, if the marginal value⁵³ 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 transaction of which it is a minor part.⁵⁴ 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. Furthermore, changing the law to make consumers the default owners of the fact of their economic activity is unlikely to produce large numbers of confidentiality clauses in the agora. In most cases, all it will do is move some of the consumer surplus from information buyers to information producers or sellers as the standard forms change to include a term in which the consumer conveys rights to the information in exchange for a frequent flyer mile or two.

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

54. See Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497, 519-23 (1995).

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

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

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

Consumers sometimes have an interest in disclosure of information. For example, proof of credit-worthiness tends to improve the terms on which lenders offer credit. The myopia story assumes this feature away. It would be interesting to try to measure the relative importance of privacy and disclosure as intermediate and final goods. If it turned out that the intermediate good aspect of informational privacy and disclosure substantially outweighed their final good aspect, this would suggest that the focus on blocking disclosure advocated in this article was misguided, and that European data-protection rules--which focus on requiring transparency regarding the uses to which data will be put--might be the best strategy.

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

There has already been considerable work on privacy-enhancing technologies for electronic transactions.⁵⁵ There seems to be scope for more research, however, on which types of transactions are best suited to using privacy-enhancing technologies such as information intermediaries. The

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

hardest work, however, will be finding ways to apply privacy-enhancing technologies to those transactions that are not naturally suited to them.

Perhaps the most promising avenue, however, is designing contracts and technologies that falsify the assumptions in the myopia story. For example, one might seek to lower the transaction costs of modifying standard form contracts, or of specifying restrictions on reuse of disclosed data. The lower the cost of contracting for privacy, the greater the chance that it will be less than the marginal value of the data (note that merely lowering it below average cost does not solve the underlying problem, as sales will still happen in that price range). If technologies such as P3P⁵⁶ are able to reduce the marginal transactions costs involved in negotiating the conditions attaching to the release of personal data to near-zero, even the privacy myopic will be able to express their privacy preferences in the P3P-compliant part of the marketplace.

B. *Making Privacy Rules That (Might) Work*

The variety and market-friendliness of privacy-destroying technologies makes an effective response difficult; this may explain the relatively limited protection against data acquisition provided by existing privacy rules. Alas, 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 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. Since the economic incentive to provide strong privacy protections is either weak, nonexistent, or at least nonuniformly distributed among all participants in the marketplace, most serious proposals for self-regulation among market participants rely on the threat of government regulation if the data collectors fail to regulate themselves sufficiently.⁵⁷ Without some

56. 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*, available in <http://www.w3.org/P3P/P3FAQ.html> ("P3P [allows] [w]eb sites to express their privacy practices and enable users to exercise preferences over those practices. P3P products will allow users to be informed of site practices (in both machine and human readable formats), to delegate decisions to their computer when appropriate, and allow users to tailor their relationship to specific sites.").

57. 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

sort of government intervention to encourage self-regulation, “[w]olves self-regulate for the good of themselves and the pack, not the deer.”⁵⁸

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.⁵⁹ 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.⁶⁰ 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, contribute up to \$100,000 per year in support.⁶¹ 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, TRUSTe certainly has no economic incentive to be tough on its funding sources. Even 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 motivated or principled enough to take part in them. The United States may be unique in endorsing self-regulation without legal sanctions to incentivize or enforce it;⁶² 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

government regulation can induce them to self-regulate).

58. 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>>.

59. See <http://www.truste.com/users/users_lookup.html> (describing TRUSTe’s services).

60. 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).

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

62. 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>>

legal conditions create incentives for parties to engage in it seriously.

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.”⁶³ Privacy can be engineered into systems design,⁶⁴ 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.

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.

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.”⁶⁵ 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 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.

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

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

64. For some suggested basic design principles, see INFORMATION AND PRIVACY COMMISSIONER/ONTARIO, CANADA & REGISTRATIEKAMER, *supra* note 55; *see also* Ian Goldberg, David Wagner & Eric Brewer, *Privacy-enhancing Technologies for the Internet* <<http://www.cs.berkeley.edu/~daw/papers/privacycomcon97www/privacyhtml.html>> (describing existing PETs and calling for additional ones).

65. Reidenberg, *supra* note 57, 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).

fears hidden cameras, then a pocket camera detector is just the thing.⁶⁶

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.

2. *Changes in the Law*

Legal reforms based upon either traditional property or intellectual property law might increase the protection available to personal data by vesting the sole initial right to use 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.⁶⁷ It also has significant problems, however, both theoretically and practically. The greatest hurdle, again, is privacy myopia.

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.⁶⁸ 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.

Given that property-law-based solutions are undermined in the marketplace, some European nations have gone further and removed a consumer's freedom to contract away her right to certain classes of data, such as information about race, religion, and political opinions.⁶⁹ 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.⁷⁰

66. 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).

67. 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 57, at 41.

68. 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”).

69. See *id.* at 233.

70. 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*

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.

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.⁷¹ 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.⁷² Even after 'safe harbor' agreements, these extraterritorial rules do not require that foreign data collection laws meet the EU's standards, leaving the United States on its own to decide what protections, if any, it should enact to safeguard its consumers and citizens.

16 <<http://www.sims.berkeley.edu/~hal/Papers/policy/policy.html>>.

71. 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); PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW: A STUDY OF U.S. DATA PROTECTION (1996).

72. See PETER P. SWIRE & ROBERT E. LITAN, NONE OF YOUR BUSINESS WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE (1998); SCHWARTZ & REIDENBERG, *supra* note 71.

III. Is Information Privacy Dead?

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.⁷³ Even the vastly more elaborate privacy laws in Europe and Canada permit almost any consensual collection and resale of personal data.⁷⁴ 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."⁷⁵ Unless there is a mechanism that creates an incentive for someone to police for compliance, legal rules will have at best limited effectiveness.⁷⁶

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 to data acquisition, and leaving aside the important issues of data retention and reuse, may make the intellectual 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.

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. A more general strategy will also focus on encouraging the adoption of fair information practices

73. 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."

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

75. David H. Flaherty, *Controlling Surveillance: Can Privacy Protection Be Made Effective*, in TECHNOLOGY & PRIVACY, *supra* note 71, at 167, 170.

76. See Robert Gellman, *Does Privacy Law Work?*, in TECHNOLOGY & PRIVACY, *supra* note 71, at 193, 214-15.

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.

Given the rapid pace at which privacy-destroying technologies are being invented and deployed, a legal response must come soon, or it will be too late.