Information Privacy in Cyberspace Transactions

Jerry Kang*

Cyberspace is the rapidly growing network of computing and communication technologies that have profoundly altered our lives. We already carry out myriad social, economic, and political transactions through cyberspace, and, as the technology improves, so will their quality and quantity. But the very technology that enables these transactions also makes detailed, cumulative, invisible observation of our selves possible. The potential for wide-ranging surveillance of all our cyber-activities presents a serious threat to information privacy. To help readers grasp the nature of this threat, Professor Jerry Kang starts with a general primer on cyberspace privacy. He provides a clarifying structure of philosophical and technological terms, descriptions, and concepts that will help analyze any problem at the nexus of privacy and computing-communication technologies. In the second half of the article, he focuses sharply on the specific problem of personal data generated in cyberspace transactions. The private sector seeks to exploit this data commercially, primarily for database marketing, but many individuals resist. The dominant approach to solving this problem is to view personal information as a commodity that interested parties should contract for in the course of negotiating a cyberspace transaction. But this approach has so far failed to address a critical question: Which default rules should govern the flow of personal information when parties do not explicitly contract about privacy? On economic efficiency and human dignity

---

* Acting Professor, University of California at Los Angeles ("UCLA") School of Law. kang@law.ucla.edu; <http://www.law.ucla.edu/faculty/kang>. For helpful conversations and comments, I thank Rick Abel, Keith Aoki, Stephen Bainbridge, Paul Bergman, Stuart Biegel, Gary Blasi, Daniel Bussel, Evan Caminker, Ann Carlson, Margaret Chon, Richard Fallon, Catherine Fisk, Jody Freeman, Robert Heverly, Peter Huang, Kenneth Karst, Ken Klee, William Klein, Stan Kurzban, Mark Lemley, Larry Lessig, Gillian Lester, Gerald López, David Post, Gary Rowe, Pamela Samuelson, Rick Sander, Gary Schwartz, Paul Schwartz, Seana Shiffrin, David Sklansky, Clyde Spillenger, Kirk Stark, Richard Steinberg, Eric Talley, Eugene Volokh, John Wiley, Stephen Yeazell, and Fred Yen. Special thanks go to my colleague Mitu Gulati. Preliminary thoughts were presented to the 1996 Conference of Asian Pacific American Law Faculty, at UCLA School of Law, the Junior Faculty Group at UCLA, and the UCLA School of Law Faculty Colloquium. I thank my research assistants, Philip Lee, Paul Ohm, Jean-Paul Saulnier, and especially John Padovan for expert assistance, which was funded by grants from the UCLA Academic Senate, the UCLA Asian American Studies Center, and the UCLA School of Law Dean's Fund. As always, the staff of the Hugh & Hazel Darling Law Library at UCLA was enormously helpful. I worked on some of the government reports I critique; a full disclosure appears in note 19 *infra*. I dedicate this to my confidant, Sung Hui Kim.

grounds, Professor Kang argues in favor of a default rule that allows only "functionally necessary" processing of personal information unless the parties expressly agree otherwise. The article concludes with a proposed statute, entitled the Cyberspace Privacy Act, which translates academic theory into legislative practice.

INTRODUCTION

Cyberspace is shorthand for the web of consumer electronics, computers, and communication networks that interconnects the world.[1] Coursing through this web is information, which makes useful our telephones, radios, televisions, pagers, faxes, satellite dishes, and computer networks. The revolution in our communications infrastructure—in particular, the explosive growth[2] of the Internet[3]—has fundamentally transformed how we create, acquire, disseminate, and use information.

The benefits are striking. Now, digitized libraries make available vast resources, regardless of distance.[4] Telemedicine allows remote experts to advise local caregivers.[5] Shopping and entertainment can be accessed im-

---

1. A more official-sounding name is the Global Information Infrastructure ("GII"). *See generally* The Global Information Infrastructure: Agenda for Cooperation, 60 Fed. Reg. 10,359 (1995) (setting forth the U.S. Government's vision for developing the GII and identifying the policy issues critical to encouraging its use). The United States is committed to developing its portion of the GII, the National Information Infrastructure ("NII"). The NII has an expansive meaning, which includes low- and high-tech hardware, software, network interconnection standards and protocols, information, and the people who make all this possible. *See generally* The National Information Infrastructure: Agenda for Action, 58 Fed. Reg. 49,025 (1993) [hereinafter Agenda for Action].

2. The number of hosts and domains listed in the Internet Domain Name System went from 9,472,000 hosts and 240,000 domains in January 1996, to 16,146,000 hosts and 828,000 domains in January 1997. *See* NETWORK WIZARDS, *Internet Domain Survey, January 1997* (visited June 11, 1997) <http://www.nw.com/zone/WWW/report.html>. Even more impressive, between January 1993 and January 1997, the numbers of hosts and domains increased by 14,833,000 and 807,000, respectively. *See id.*

Actual Internet use is difficult to determine. Yet one recent survey found that nearly one in four people over the age of 16 in the United States and Canada now use the Internet. In absolute numbers, the survey found that about 50.6 million people in the United States and Canada use the Internet in some way, whereas about 37.4 million use the World Wide Web. *See* Rajiv Chandrasekaran, *Internet Use Has More Than Doubled in Last 18 Months, Survey Finds*, WASH. POST, Mar. 13, 1997, at E3. Another study found that "[m]ore than 31 million Americans age 18 or older—almost one in six adults—regularly use the Internet or commercial online services [and] that another 9 million people have used the Internet in the past year, but don't consider themselves regulars." Elizabeth Corcoran, *1 in 6 U.S. Adults Regularly Online, Study Indicates*, WASH. POST, May 7, 1997, at C10; *see also CyberAtlas/Market Size* (visited Feb. 5, 1998) <http://www.cyberatlas.com/market/siza/historical_data.html> (providing historical data on Internet and Web use).

3. *See generally* ED KROL, THE WHOLE INTERNET USER'S GUIDE & CATALOG (2d ed. 1994) (describing the structure and uses of the Internet). More technical descriptions appear in GILBERT HELD, UNDERSTANDING DATA COMMUNICATIONS 379-418 (2d ed. 1996), and RAY HORAK, COMMUNICATIONS SYSTEMS AND NETWORKS: VOICE, DATA & BROADBAND TECHNOLOGIES 367-400 (1997). For an engaging history of the Internet, see generally KATIE HAFNER & MATTHEW LYON, WHERE WIZARDS STAY UP LATE: THE ORIGINS OF THE INTERNET (1996).

4. For example, the House of Representatives has made available the entire United States Code on the Internet. *See* U.S. HOUSE OF REPRESENTATIVES, INTERNET LAW LIBRARY: U.S. CODE (visited Mar. 15, 1998) <http://law.house.gov/usc.htm>.

5. *See, e.g.*, William McCall, *The Doctor Will See You Now—On TV; Medicine: Many Hope Telemedicine Will Bring Better Health Care at Lower Cost to Rural Areas*, L.A. TIMES, May 12, 1997, at D9 (discussing the benefits to patients who no longer need to travel long distances to be

mediately through virtual malls and auditoriums.[6] Individuals now debate the day's burning issues in electronic fora, oblivious to geographical separation.[7]

Unfortunately, cyberspace also raises new concerns. Consider, for example, the much-publicized conflicts concerning cyberspace copyright[8] and pornography.[9] The buzz around these issues is not surprising; intellectual property and freedom of expression are critical to our economics and politics. But cyberspace presses upon us a third issue, the significance of which is less obvious. That issue is privacy, what Justice Louis Brandeis once called "the most comprehensive of rights and the right most valued by civilized men."[10]

The public is already apprehensive about privacy. For example, a 1996 study conducted by Equifax, a leading credit bureau, and Alan Westin, a privacy scholar, found that 89% of those polled in the United States were either

---

treated); Jube Shiver, Jr., *A Tonic for Telemedicine*, L.A. TIMES, June 16, 1997, at D12 (discussing the need for better Internet access to rural areas in order to support telemedicine).

6. By one estimate, in 1996, $900 million in commerce took place on the Internet. *See I.B.M. Sees Business on Internet Improving*, N.Y. TIMES, Jan. 9, 1997, at D4. Some expect $400 billion worth of commerce by 1999. *See* Joshua B. Konvisser, *Coins, Notes, and Bits: The Case for Legal Tender on the Internet*, 10 HARV. J.L. & TECH. 321, 322 (1997).

7. *See, e.g.*, Peter H. Lewis, *Exploring New Soapboxes for Political Animals*, N.Y. TIMES, Jan. 10, 1995, at C6 (discussing the presence of political "chat rooms" on the Usenet); Alice Thomas, *Computer Meeting Packed; Try Again If Popular Town Hall Is "Busy,"* COLUMBUS DISPATCH, May 3, 1995, at 2B (discussing participation in an electronic "town hall"); *cf.* Sheila Tefft, *China Attempts to Have Its Net and Censor It Too*, CHRISTIAN SCI. MONITOR, Aug. 5, 1996, at 1 (describing the Chinese government's requirement that all domestic Internet users register with the police and not "produce, retrieve, duplicate, and spread information that may hinder public order").

8. The digitalization of information makes simple the reproduction and quick transmission of perfect copies through cyberspace. This technological transformation disturbs the truce that has so far existed between information producers and consumers. Not surprisingly, a fierce battle now rages to revise the law of copyright and establish a new truce in this new technological regime. *See, e.g.*, Peter Jaszi, *Caught in the Net of Copyright*, 75 OR. L. REV. 299 (1996) (criticizing the government's new suggestions for intellectual property policy); Jessica Litman, *Revising Copyright Law for the Information Age*, 75 OR. L. REV. 19 (1996) (urging a restructuring of copyright law as applied to computers); Pamela Samuelson, *The Copyright Grab*, WIRED, Jan. 1996, at 134 (describing the Clinton administration's intellectual property proposal as a "wholesale giveaway" to the copyright industry).

9. Notwithstanding our constitutional commitment to uninhibited expression, we disfavor certain types of speech, such as criminal threats, securities fraud, defamation, and obscenity. As individuals leverage cyberspace to increase radically their ability to speak and to listen, they sometimes do so in ways that amplify the harms associated with such disfavored speech. Recently, Congress reacted to one such aspect of the cyberspace speech problem, obscene and indecent speech. *See* Communications Decency Act of 1996, 47 U.S.C. § 223 (Supp. 1997). The Supreme Court declared those provisions of the Act applying to "indecent" and "patently offensive" speech violative of the First Amendment. *See* Reno v. ACLU, 117 S. Ct. 2329, 2334 (1997).

10. Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting) (discussing "the right to be let alone"). I would hope that Brandeis, if writing today, would say "civilized persons."

very or somewhat concerned about privacy.[11] Some of the most extensive surveys of Internet users indicate that cyberspace will exacerbate that anxiety.[12] This growing concern recognizes, if vaguely, that, as our communica-

---

11. *See* Alan F. Westin, *"Whatever Works": The American Public's Attitudes Toward Regulation and Self-Regulation on Consumer Privacy Issues*, *in* NATIONAL TELECOMMS. & INFO. ADMIN., U.S. DEP'T OF COMMERCE, PRIVACY AND SELF-REGULATION IN THE INFORMATION AGE ch. 1, § F (1997), *available in* <http://www.ntia.doc.gov/reports/privacy/selfreg1.htm#1F> [hereinafter NTIA REPORT]. According to the same poll conducted in 1995, "Nearly one out of every two people in the U.S. is 'very' concerned about threats to their personal privacy today (47%) and another 35% are 'somewhat' concerned." LOUIS HARRIS & ASSOCS., INC. & Alan F. Westin, *Equifax-Harris Mid-decade Consumer Privacy Survey* (visited Nov. 9, 1996) <http://www.equifax.com/consumer/survey95/docs/title.htm>. Furthermore, "[o]ne out of every four people in America (25%) say they have been the victim of an improper invasion of privacy." *Id.*

12. The Graphic, Visualization & Usability Center's ("GVU") Seventh World Wide Web User Survey, which involved 19,970 unique respondents, tracked the issues most important to users of the World Wide Web. In both the seventh survey and the sixth survey, conducted six months earlier,

> the largest category of respondents (33.58% Seventh [survey] vs. 35.9% Sixth [survey]) feel that censorship is the most important issue facing the Internet today. *This is followed by privacy (26.17% Seventh vs. 26.2% Sixth)* and navigation (13.14% Seventh vs. 14.1% Sixth). . . . And among women, privacy outranks censorship as the most important issue.

GRAPHIC, VISUALIZATION & USABILITY CENTER, *Seventh World Wide Web Survey Results* (visited July 2, 1997) <http://www.gvu.gatech.edu/gvu/user_surveys/survey-1997-04/> [hereinafter *GVU Seventh Study*] (emphasis added).

What is more telling is the result of the GVU Eighth World Wide Web User Survey, which surveyed over 10,000 users. For the first time, censorship and privacy flipped their order of importance; privacy ranked at the top (30.49%), followed by censorship (24.18%). A total of 72% of respondents agreed strongly (39%) or somewhat (33%) that there should be new Internet privacy laws. The single most contested statement in the survey was that content providers have the right to resell user information (63% disagree strongly, and another 19% disagree somewhat). *See* GRAPHIC, VISUALIZATION & USABILITY CENTER, *Eighth World Wide Web User Survey* (visited Jan. 26, 1997) <http://www.gvu.gatech.edu/user_surveys/survey-1997-10/#exec> [hereinafter *GVU Eighth Study*].

According to another on-line poll of 9300 individuals conducted by Boston Consulting Group, "[O]ver 70 percent . . . [are] more concerned about privacy on the Internet than they are about information transmitted by traditional media such as phone and mail." TRUSTE, *Survey Reveals Consumer Fear of Privacy Infringement Inhibits Growth of Electronic Commerce* (visited Nov. 7, 1997) <http://www.truste.org/users/article003.html>.

In another survey, adults flagged abuse of personal information on the Internet as their top concern (88%), with credit card fraud (60%) a distant second. *See* ZIFF-DAVIS, INC., *Kids' Safety: Survey Results* (visited Jan. 26, 1997) <http://www.zdnet.com/familypc/content/ kidsafety/results.html> (surveying 750 families).

Two recent events reflect the concern over cyber-privacy. In September 1996, Lexis-Nexis' P-TRAK database came under fire in the Internet community for allegedly disclosing personal information that could be used to commit credit card fraud. *See* Amy Harmon, *Public Outrage Hits Firm Selling Personal Data*, L.A. TIMES, Sept. 19, 1996, at A1 (reporting on the numerous telephone complaints to Lexis-Nexis); Kathy M. Kristof, *Deluged Lexis Purging Names from Database*, L.A. TIMES, Nov. 8, 1996, at D5 (reporting on the consumer requests to be deleted from the database). In April 1997, the Social Security Administration's Personal Earnings and Benefits Estimate Statements ("PEBES") online system was criticized for allowing access to these statements over the Internet. *See* John Schwartz & Barbara J. Saffir, *Privacy Concerns Short-Circuit Social Security's Online Service; Agency Unplugs Web Feature As It Reconsiders Security*, WASH. POST, Apr. 10, 1997, at A23 (reporting that 10,000 people called to complain). House hearings

tions infrastructure grows more powerful and user-friendly, we increasingly speak, listen, and act through cyberspace. And such activity generates records, dutifully recorded, sorted, saved, and exchanged by computers.[13]

To focus that vague concern, imagine the following two visits to a mall, one in real space, the other in cyberspace. In real space, you drive to a mall, walk up and down its corridors, peer into numerous shops, and stroll through corridors of inviting stores. Along the way, you buy an ice cream cone with cash. You walk into a bookstore and flip through a few magazines. Finally, you stop at a clothing store and buy a friend a silk scarf with a credit card. In this narrative, numerous persons interact with you and collect information along the way. For instance, while walking through the mall, fellow visitors visually collect information about you, if for no other reason than to avoid bumping into you. But such information is general—e.g., it does not pinpoint the geographical location and time of the sighting—is not in a format that can be processed by a computer, is not indexed to your name or another unique identifier, and is impermanent, residing in short-term human memory. You remain a barely noticed stranger. One important exception exists: The scarf purchase generates data that are detailed, computer-processable, indexed by name, and potentially permanent.

By contrast, in cyberspace, the exception becomes the norm: Every interaction is like the credit card purchase. The best way to grasp this point is to take seriously, if only for a moment, the metaphor that cyberspace is an actual place, a computer-constructed world, a virtual reality. In this alternate universe, you are invisibly stamped with a bar code as soon as you venture outside your home. There are entities called "road providers,"[14] who supply the streets and ground you walk on, who track precisely where, when, and how fast you traverse the lands, in order to charge you for your wear on the infrastructure. As soon as you enter the cyber-mall's domain, the mall begins to track you through invisible scanners focused on your bar code. It automatically records which stores you visit, which windows you browse, in which order, and for how long. The specific stores collect even more detailed data when you enter their domain. For example, the cyber-bookstore notes which magazines you skimmed, recording which pages you have seen

---

have been held on the issue, and legislation has been offered to bar such practices. *See* American Family Privacy Act of 1997, H.R. 1330, 105th Cong. (barring federal agencies from disseminating, inter alia, Social Security account and PEBES information over the Internet); Barbara J. Saffir, *Sharing the Secrets with the Right Party*, WASH. POST, May 8, 1997, at A25 (describing the House hearings).

13. *See* texts accompanying notes 123-153 & 168-171 *infra.*

14. By "road providers," I mean electronic communication providers, such as Internet Service Providers ("ISPs") and telephone companies. *See* text accompanying notes 168-188 *infra*. Similar tracking may become the norm in real space as well. *See generally Symposium: Privacy and ITS*, 11 SANTA CLARA COMPUTER & HIGH TECH. L.J. (1995) (discussing surveillance possibilities through Intelligent Transportation Systems).

and for how long, and notes the pattern, if any, of your browsing. It notes that you picked up briefly a health magazine featuring an article on St. John's Wort, read for seven minutes a newsweekly detailing a politician's sex scandal, and flipped ever-so-quickly through a tabloid claiming that Elvis lives. Of course, whenever any item is actually purchased, the store, as well as the credit, debit, or virtual cash company that provides payment through cyberspace, takes careful notes of what you bought—in this case, a silk scarf, red, expensive.[15]

All these data generated in cyberspace are detailed, computer-processable, indexed to the individual, and permanent. While the mall example does not concern data that appear especially sensitive, the same extensive data collection takes place as we travel through other cyberspace domains—for instance: to research health issues and politics; to communicate to individuals, private institutions, and the state; and to pay our bills and manage our finances. Moreover, the data collected in these various domains can be aggregated to produce telling profiles of who we are, as revealed by what we do and say. The very technology that makes cyberspace possible also makes detailed, cumulative, invisible observation of our selves possible. One need only sift through the click-streams generated by our cyber-activity. The information we generate as a by-product of this activity is quite valuable. The private sector seeks to exploit it commercially, but individuals resist. Both sides lay powerful, clashing claims to this data generated in cyberspace. How we resolve this conflict warrants careful discussion.

A conversation about privacy, of course, has been ongoing for a long time. In American law alone, it is over a century old.[16] And, for the past three decades, many have warned about the privacy dangers posed specifically by the computer.[17] That privacy conversation must now be broadened to consider the impact of the entire communications infrastructure. Not surprisingly, academics have started to address these new issues.[18] More sur-

---

15. Anonymous payment systems, like the cash for the ice-cream cone, are not widely available in cyberspace today. *See* text accompanying notes 221-223 *infra* .

16. A seminal law review article prompted recognition of the common law tort of invasion of privacy. *See generally* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

17. *See, e.g.*, ARTHUR R. MILLER, THE ASSAULT ON PRIVACY: COMPUTERS, DATA BANKS, AND DOSSIERS 39 (1971) (cautioning against a "record prison . . . [created] by the continuous accumulation of dossier-type material on people over a long period of time").

18. *See, e.g.*, FRED H. CATE, PRIVACY IN THE INFORMATION AGE (1997); OSCAR H. GANDY, JR., THE PANOPTIC SORT: A POLITICAL ECONOMY OF PERSONAL INFORMATION (1993); PRISCILLA M. REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY (1995); PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW: A STUDY OF UNITED STATES DATA PROTECTION (1996); H. JEFF SMITH, MANAGING PRIVACY: INFORMATION TECHNOLOGY AND CORPORATE AMERICA (1994); A. Michael Froomkin, *The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709 (1995); George B. Trubow, *Information Law Overview*, 18 J. MARSHALL. L. REV. 815 (1985); Mark A. Lemley, *Right of Attri-*

prisingly, government has also tried to stay ahead of the curve.[19] The goal of this article is to push the conversation forward by uniting the thinking of both worlds. Methodologically eclectic, it draws where useful from philosophy, network engineering, and economics to supplement more traditional doctrinal analysis and legislative drafting.

Structurally, the article divides in half. The first half is a general primer on cyberspace privacy. It begins, in Part I, by clearing the conceptual and linguistic underbrush. Specifically, I identify equivocations latent in the term "privacy," present a definition widely accepted in the policy literature, and explore the conceptual consequences of that definition. Part II then examines what is technologically different in cyberspace and how information privacy will be threatened by new technologies unfettered by old laws. My purpose here is foundational—to build a clear and technically correct structure of terms, descriptions, and concepts. This half should facilitate the analysis of any problem at the nexus of privacy and computing-communication technologies. It is regrettably, but necessarily, long and detailed.

---

bution and Integrity in Online Communications, 1995 J. ONLINE L. art. 2 (visited Mar. 15, 1998) <http://warthog.cc.wm.edu/law/publications/jol/lemley.html>.

19. For example, in the past two years, the Clinton administration's Information Infrastructure Task Force ("IITF") has recommended a general set of privacy principles, with an eye toward cyberspace governance. *See, e.g.*, INFORMATION INFRASTRUCTURE TASK FORCE, PRIVACY AND THE NATIONAL INFORMATION INFRASTRUCTURE: PRINCIPLES FOR PROVIDING AND USING PERSONAL INFORMATION (1995), *available in* <http://www.iitf.nist.gov/ipc/ipc/ipc-pubs/niiprivprin_final.html> [hereinafter IITF PRINCIPLES]. The Task Force has also produced an options paper on a federal privacy agency. *See* PRIVACY WORKING GROUP, INFORMATION INFRASTRUCTURE TASK FORCE, OPTIONS FOR PROMOTING PRIVACY ON THE NATIONAL INFORMATION INFRASTRUCTURE (Apr. 1997), *available in* <http://www.iitf.nist.gov/ipc/privacy.htm> [hereinafter IITF OPTIONS PAPER].

In addition, the National Telecommunications and Information Administration ("NTIA") of the Department of Commerce has released an analysis of telecommunications-related privacy issues. *See generally* NATIONAL TELECOMMS. & INFO. ADMIN., U.S. DEP'T OF COMMERCE, PRIVACY AND THE NII: SAFE-GUARDING TELECOMMUNICATIONS-RELATED PERSONAL INFORMATION (1995), *available in* <http://www.ntia.doc.gov/ntiahome/privwhitepaper.html> [hereinafter NTIA WHITEPAPER]. The Department of Commerce has also published a compilation of essays written by academics, lawyers, and industry representatives. *See generally* NTIA REPORT, *supra* note 11.

Finally, the Federal Trade Commission ("FTC") has held multiple panel discussions and has issued various recommendations to protect consumer privacy in cyberspace. *See, e.g.*, FEDERAL TRADE COMM'N, *FTC Workshop: Consumer Protection and the Global Information Infrastructure* (Apr. 10, 1995); <http://www.ftc.gov/opp.trnscrpt.htm>; FEDERAL TRADE COMM'N, *Workshop on Consumer Information Privacy* (June 10-13, 1997) <http://www.ftc.gov/bcp/privacy/privacy.htm>; FEDERAL TRADE COMM'N, *Workshop on Consumer Privacy on the Global Information Infrastructure* (June 4-5, 1996) <http://www.ftc.gov/bcp/privacy/privacy.htm>.

I worked on some of these projects from 1994-1995 as an employee of the NTIA. I was an active member of the Privacy Working Group, which drafted the IITF PRINCIPLES, *supra*, and I was the principal author of the NTIA WHITEPAPER, *supra*. I participated in early research and deliberations over the IITF OPTIONS PAPER, *supra*. Finally, I was a panelist at the FTC conferences in both 1995 and 1996.

Having built this foundation, the article changes gears in the second half. In aim, it moves from descriptive mapping to normative problem-solving. In scope, it narrows its focus to just one of the many privacy issues that the primer unearths, namely the problem of personal data specifically generated in the course of executing a cyberspace transaction. Specifically, in Part III, I describe the dominant normative approach to the problem, championed by various commentators and suggested in recent federal policy proposals. This approach urges the construction of a market for personal information, which is viewed no differently than other commodities that the market is supposed to price correctly and allocate efficiently. The marketplace approach has many attractions, but it is, as currently conceptualized, seriously incomplete. It fails to address which default rules should govern the flow of personal information when parties do not explicitly contract about privacy. On efficiency and nonefficiency grounds, I argue in favor of a default rule that allows only "functionally necessary" processing of personal information unless the parties expressly agree otherwise. Finally, in Part IV, I translate academic argument into pragmatic policy. The end result is a proposed Cyberspace Privacy Act, which would govern the processing of personal information collected in the course of executing cyberspace transactions in the United States.

An important limit to my project is that it does not examine how privacy may be violated by the state in the course of, for example, doling out public benefits, collecting taxes, or deterring crime in and through cyberspace—although these, too, present critical social issues. Instead, the spotlight is on the private sector and how it processes personal information in the little-regulated marketplace of ideas, information, and goods that is cyberspace. Equally important issues regarding governmental invasion of privacy exist, but I table those for now, partly because they have already received substantial attention.[20] In contrast, private actors' impact on privacy has undergone less exacting scrutiny, which is unwarranted; the private sector has come to rival government in the use of personal information.[21] With this proviso, I

---

20. *See, e.g.*, THE PRIVACY PROTECTION STUDY COMM., PERSONAL PRIVACY IN AN INFORMATION SOCIETY 345-91 (1977) (discussing government access to personal records); U.S. DEP'T OF HEALTH, EDUC. & WELFARE, SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS at xx (1973) [hereinafter HEW REPORT] (recommending a "Code of Fair Information practice for all automated personal data systems"); Froomkin, *supra* note 18, at 735-843 (discussing cryptography rights against the government); Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 IOWA L. REV. 548, 558-60 (1995).

21. *See* IITF PRINCIPLES, *supra* note 19, at 2 ("[T]he private sector now rivals the government in acquiring and using personal information."); *see also* John Markoff, *Remember Big Brother? Now He's a Company Man*, N.Y. TIMES, Mar. 31, 1991, at E7 (discussing the methods companies use to observe their workers). Recent polls indicate that the American public is concerned about threats to privacy from the private sector as much as from government. *See* ANNE WELLS BRANSCOMB, WHO OWNS INFORMATION?: FROM PRIVACY TO PUBLIC ACCESS 17 (1994) (citing a

begin by examining the constituent components of the term "cyberspace privacy." I start with privacy.

I. PRIVACY: A PHILOSOPHICAL CLARIFICATION

It is cliché to note that the threshold obstacle to clear thinking about privacy is the term itself. Privacy is a chameleon that shifts meaning depending on context.[22]

A. *Three Clusters: Space, Decision, and Information*

The term "privacy" conveys numerous ideas that can be clustered into three groupings. The first cluster concerns physical space—in particular, the extent to which an individual's territorial solitude is shielded from invasion by unwanted objects or signals. This spatial privacy is the sort invoked by sociologists who discuss private versus public territories and territorial overcrowding.[23] It is this sense of privacy that informs the Fourth Amendment search-and-seizure concept of curtilage.[24] This is also the sense of privacy employed when one complains about a car alarm or a telemarketing call disturbing one's privacy.

The second cluster views privacy as principally concerned with choice, an individual's ability to make certain significant decisions without interference. This decisional privacy is the sort discussed famously in *Roe v.*

Harris survey). The sharp public/private distinction drawn here for heuristic purposes does not mean that one side has nothing to do with the other. Indeed, what the private sector collects today affects what the public sector accesses tomorrow because the state regularly taps private databanks in the name of the public good. *See, e.g.*, Paul M. Alberta, *IRS Database Plan Under Fire; DMA, Credit Reporting Agencies, Question Legality*, DM NEWS, Jan. 30, 1995, at 1 (discussing Internal Revenue Service plans to tap private commercial databases to improve enforcement). Conversely, the private sector regularly taps public databanks to acquire records to sell in the marketplace.

22. *See* OFFICE OF TECH. ASSESSMENT, U.S. CONGRESS, OTA-TCT-606, INFORMATION SECURITY AND PRIVACY IN NETWORK ENVIRONMENTS 82 (1994); DECKLE MCLEAN, PRIVACY AND ITS INVASION 3-6 (1995) (discussing the subjective nature of the concept of privacy); Judith Jarvis Thomson, *The Right to Privacy*, *in* PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY 272, 273 (Ferdinand David Schoeman ed., 1984) (noting that there is room for disagreement regarding what qualifies as a privacy right).

23. *See, e.g.*, IRWIN ALTMAN, THE ENVIRONMENT AND SOCIAL BEHAVIOR: PRIVACY, PERSONAL SPACE, TERRITORY, CROWDING 146-51 (1975) (distinguishing crowding—a psychological concept resulting from a failure of privacy mechanisms—from density—the physical presence of people per unit of space).

24. *See* California v. Ciraolo, 476 U.S. 207, 212-13 (1986) ("The protection afforded the curtilage is essentially a protection of families and personal privacy in an area intimately linked to the home, both physically and psychologically, where privacy expectations are most heightened."); *cf.* Ken Gormley, *One Hundred Years of Privacy*, 1992 WIS. L. REV. 1335, 1358-59 (1992) (discussing a colonial view that a man's home is his castle and the constitutionalization of that view into the Third and Fourth Amendments); *see also* Stanley v. Georgia, 394 U.S. 557, 565 (1969) (identifying the home as a special place, where a person possesses greater privacy rights).

Wade.[25] This conception of privacy is less concerned with the maintenance of spatial boundaries and more concerned with a person's freedom to make self-defining choices without state interference.[26] Of the three privacy clusters I will mention, this one has incited the most contentious constitutional and political battles.

Finally, the third cluster of privacy concerns the flow of personal information. More precisely, information privacy concerns an individual's control over the processing—i.e., the acquisition, disclosure, and use—of personal information. In this third cluster, the paradigmatic privacy violation does not occur, for instance, when the state places an undue burden on some significant decision. Rather, this strand of privacy is invaded when, for example, someone obtains sensitive medical data by rifling through confidential files without permission.

I use the term "cluster" to connote that these three types are not sharply separate. They are functionally interconnected and often simultaneously implicated by the same event or practice. For instance, spatial privacy often promotes information privacy: When one is shielded from external stimuli, such that signals—say, the sound wave of a barking dog—cannot flow to the individual, one is often simultaneously shielded from observation, such that signals cannot flow outward from the individual.[27] Being so shielded from observation means that personal information cannot be collected, which bolsters an individual's privacy.[28] As another example, consider how information privacy—e.g., keeping the fact of pregnancy to oneself—can create the breathing space away from familial or societal censure necessary for decisional privacy—e.g., to choose whether to have an abortion.[29] Or, in reverse,

---

25. 410 U.S. 113 (1973); *see also* Eisenstadt v. Baird, 405 U.S. 438, 453 (1972) (holding that the right to privacy includes the right to decide whether or not to bear or beget a child); Griswold v. Connecticut 381 U.S. 479, 485-86 (1965) (holding that a law prohibiting the use of contraceptives unconstitutionally intrudes on the right of marital privacy).

26. In federal constitutional law, decisional privacy rights have been recognized in "matters relating to marriage, procreation, contraception, family relationships, and child rearing and education." Paul v. Davis, 424 U.S. 693, 713 (1976); *accord* Loving v. Virginia, 388 U.S. 1, 12 (1967) (marriage); Pierce v. Society of Sisters, 268 U.S. 510, 518 (1925) (child rearing and education); Meyer v. Nebraska, 262 U.S. 390 (1923) (education).

27. This is not always true, as in successful covert surveillance. Another overlap between the spatial and information privacy clusters is that both may have a common justification—the desire not to be scrutinized.

28. Similarly, physical seclusion can promote autonomy. *See* Jack Hirshleifer, *Privacy: Its Origin, Function, and Future*, 9 J. LEGAL STUD. 649, 650 (1980).

29. Requiring a woman to disclose her decision to abort can be an unconstitutional burden on her right to choose. *See* Planned Parenthood v. Casey, 505 U.S. 833, 887-98 (1992) (finding a legislative requirement that married women disclose to their spouses their decision to abort to be an undue burden); Thornburgh v. American College of Obstetricians and Gynecologists, 476 U.S. 747, 765-68 (1986) (holding unconstitutional abortion reporting requirements because they are likely to result in identification of women choosing abortions). For further discussion of the connection between information privacy and choice, see text accompanying notes 274-294 *infra*.

consider how decisional privacy shields an individual from disclosing to the state her justifications for exercising some choice, thereby fortifying her information privacy. Finally, note how receiving unwanted solicitations through mail, telephone, or e-mail can simultaneously implicate two distinct privacy clusters. The junk mail, phone call, or message invades my space, spamming my physical, voice, and electronic mailboxes.[30] More importantly but less obviously, the initial targeting of that junk mail to me may have involved access to and analysis of personal information, namely my tastes, life events, and consumption history.

Indeed, a serious argument can be made that all three and additional privacy clusters can be integrated into a single, abstract cluster grounded in some moral value such as human dignity[31] or inviolate personality,[32] some sociopsychological process such as interpersonal boundary maintenance[33] or access to the self,[34] or some political theory such as antitotalitarianism.[35] But as intriguing as such grand unification projects may be, my focus lies elsewhere. From a practical point of view, the debate over reproductive freedom is usefully seen as a debate different from the one about personal information.[36] In keeping the clusters separate, I take no position on the ultimate success of a grand unification theory.[37] Instead, my point is simply to pare down concepts into usable components, flag equivocations in the term "privacy," and delimit more precisely the scope of my inquiry. To be explicit,

---

30. *See, e.g.*, CompuServe Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015 (S.D. Ohio 1997) (granting a preliminary injunction against a sender of unsolicited commercial e-mail messages, i.e., "spam," on a common law trespass theory).

31. *See, e.g.*, Edward J. Bloustein, *Privacy As an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. REV. 962, 1000-07 (1964) (refuting Prosser's claim that no single thread connects common law privacy cases and identifying human dignity as the unifying thread).

32. *See, e.g.*, Warren & Brandeis, *supra* note 16, at 195, 205 (distinguishing the principles of private property and inviolate personality).

33. *See, e.g.*, ALTMAN, *supra* note 23, at 10 (defining privacy as "an interpersonal boundary-control process").

34. *See, e.g.*, SISSELA BOK, SECRETS: ON THE ETHICS OF CONCEALMENT AND REVELATION 10 (1983) (defining privacy as "the condition of being protected from unwanted access by others"); Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 423 (1980) (arguing that the interest in privacy is related to our concern over our accessibility to others).

35. *See, e.g.*, Jed Rubenfeld, *The Right of Privacy*, 102 HARV. L. REV. 737, 784 (1989) (arguing that the principle behind the right to privacy is the "freedom not to have one's life too totally determined by a progressively more normalizing state").

36. *See* Sheldon W. Halpern, *Rethinking the Right of Privacy: Dignity, Decency, and the Law's Limitations*, 43 RUTGERS L. REV. 539, 541 n.12 (1991) (maintaining the distinction between these types of privacy for consistency with commentators despite recognition that the distinction may not be desirable); Rubenfeld, *supra* note 35, at 740, 749 (distinguishing "informational" privacy protected by the Fourth Amendment and tort law from "substantive" privacy protected by the Fourteenth Amendment).

37. For a skeptical view, see Gormley, *supra* note 24, at 1339 (arguing that legal privacy is incapable of a single definition because "four or five different species of legal rights" have been promulgated under the label of privacy).

my inquiry focuses on the third privacy cluster, information privacy.[38] Although this cluster may not be privileged in analytic priority or policy significance over the other two, it is precisely this sort of privacy that cyberspace most threatens.

B. *Focus: Information Privacy*

Information privacy is "an individual's claim to control the terms under which personal information—information identifiable to the individual—is acquired, disclosed, and used."[39] This definition comes from *Principles for Providing and Using Personal Information* ("*IITF Principles*"), issued by the Clinton administration's Information Infrastructure Task Force.[40] I adopt the IITF's definition because it is analytically useful, consistent with a broad swatch of academic and policy thinking,[41] and likely to be influential in gov-

---

38. Note also that the concept of privacy differs materially from the related concepts of confidentiality, *see* note 50 *infra*, and security, *see* note 60 *infra*.

39. IITF PRINCIPLES, *supra* note 19, at 5.

40. The Clinton administration created the IITF to address policy issues burgeoning in cyberspace. The IITF comprises high-level representatives from various federal agencies responsible for and expert in information and technological issues. *See generally* INFORMATION INFRASTRUCTURE TASK FORCE, *The President's Information Infrastructure Task Force* (visited Jan. 9, 1998) <http://www.iitf.doc.gov> (describing IITF organizational structure). Of the three committees established by the IITF—Telecommunications Policy, Information Policy, and Applications and Technology—the work of the Information Policy Committee has drawn the most academic and political attention. Within that committee are two working groups: the Intellectual Property Working Group and the Privacy Working Group. The Intellectual Property Working Group has drawn heavy fire for its recommendations on revising copyright in cyberspace. *See* note 8 *supra*. By contrast, the Privacy Working Group's efforts have created fewer sparks, at least for now.

The central privacy document produced by the Privacy Working Group, adopted by the IITF and endorsed by the Office of Management and Budget, is the *IITF Principles*. Although these principles do not have the force of law, they are meant to "guide all NII participants as well as those who are drafting legislation and creating policy regarding the use of personal information." IITF PRINCIPLES, *supra* note 19, at 4. The *IITF Principles* update earlier codes of fair information practice and attempt to provide "meaningful guidance" to policymakers confronted with a new information environment. *See* IITF PRINCIPLES, *supra* note 19, at 2.

41. *See* HEW REPORT, *supra* note 20, at xx ("Concern about computer-based record keeping usually centers on its implications for personal privacy, and understandably so if privacy is considered to entail control by an individual over the uses made of information about him.") (public policy); MILLER, *supra* note 17, at 25 ("[T]he basic attribute of an effective right of privacy is the individual's ability to control the circulation of information relating to him—a power that often is essential to maintaining social relationships and personal freedom.") (law); ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967) ("Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.") (sociology); Charles Fried, *Privacy*, 77 YALE L.J. 475, 482 (1968) ("Privacy is not simply an absence of information about us in the minds of others; rather it is the control we have over information about ourselves.") (law); W.A. Parent, *Recent Work on the Concept of Privacy*, 20 AM. PHIL. Q. 341, 346 (1983) ("[P]rivacy is the condition of a person's not having undocumented personal information about himself known by others.") (philosophy).

ernmental, private sector, and academic discussion.[42] If history repeats itself, it will be the foundation for future federal privacy legislation.[43]

1. *Personal information.*

Not surprisingly, the central component of this and nearly all definitions of information privacy is the term "personal information."[44] It is also the least self-explanatory.[45] For example, the *IITF Principles* define personal information as "information identifiable to the individual."[46] In other words, "personal" does not mean especially sensitive, private, or embarrassing.[47]

---

42. *See, e.g.*, NTIA WHITEPAPER, *supra* note 19 (analyzing telecommunications privacy issues in terms of the *IITF Principles*). For law review engagement with the *IITF Principles* and the *NTIA Whitepaper*, see, for example, Julie E. Cohen, *A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace*, 28 CONN. L. REV. 981, 994-1003 (1996) (suggesting that digital copyright management technologies may infringe seriously on privacy).

43. The Code of Fair Information Practice contained in the *HEW Report*, *supra* note 20, was the basis for the passage of the 1974 Privacy Act. The *IITF Principles* revised the Code of Fair Information Practice. *See* IITF PRINCIPLES, *supra* note 19, at 4; *see also* CATE, *supra* note 18, at 91 (noting the importance of the *IITF Principles*).

44. The other elements of the definition do not require lengthy exposition. "Acquisition" means the collection of personal information directly from the individual herself or the receipt of personal information indirectly from a third party. *See* IITF PRINCIPLES, *supra* note 19, at 7. The term does not distinguish between information obtained legally or illegally, free or for a fee. "Disclosure" can be defined as revealing personal information to those previously unaware. This term's presence in the privacy definition emphasizes that, regardless of how personal information is used, its mere disclosure may be intrinsically disturbing to the individual. Finally, "use" means storing, organizing, analyzing, matching, consulting, and destroying personal information, often to make some decisions. This term emphasizes that privacy is concerned with more than mere disclosure of sensitive information. One often wants control of personal information, not because its disclosure would be particularly embarrassing, but because of what may be done with that information. I use the term "processing" to encompass acquisition, disclosure, and use.

45. For instance, the privacy provision of the Cable Communications Policy Act of 1984 (the "1984 Cable Act") applies solely to "personally identifiable information," but this term is not affirmatively defined in the Act. *See* 47 U.S.C. § 551 (1994). At most, it is defined negatively to exclude "any record of aggregate data which does not identify particular persons." 47 U.S.C. § 551(a)(2). Little else is found in the legislative history, which merely states that a cable operator may not disclose the particular viewing selections of a subscriber or the details of a transaction conducted over the cable system. *See* H.R. REP. NO. 98-934, at 76-79 (1984), *reprinted in* 1984 U.S.C.C.A.N. 4655, 4713-16; *see also* Warner v. American Cablevision, 699 F. Supp. 851, 855 (D. Kan. 1988) (concluding that the term includes at a minimum the subscriber's name, address, and telephone number).

The Video Privacy Protection Act of 1988 ("VPPA") defines the term "personally identifiable information" to include "information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider." 18 U.S.C. § 2710(a)(3) (1994). However, the legislative history creates ambiguity by describing this as a minimum definition that is not necessarily exclusive. *See* S. REP. NO. 100-599, at 11-12 (1988), *reprinted in* 1988 U.S.C.C.A.N. 4342-1, 4342-9.

46. IITF PRINCIPLES, *supra* note 19, at 5.

47. This is an important clarification because other commentators have used "personal" in the sense of "especially sensitive." *See, e.g.*, William A. Parent, *Privacy: A Brief Survey of the Conceptual Landscape*, 11 SANTA CLARA COMPUTER & HIGH TECH. L.J. 21, 23 (1995).

Rather, it describes a relationship between the information and a person, namely that the information—whether sensitive or trivial—is somehow identifiable to an individual.

But what does it mean for information to be "identifiable to an individual"? In my view, information can be identifiable to an individual in three ways: It can bear (1) an authorship relation to the individual, (2) a descriptive relation to the individual, or (3) an instrumental mapping relation to the individual. First, the individual could have purposefully created or prepared the information—typically to communicate that information to another party—such that an authorship relationship connects the individual to the information. This relationship explains why a telephone conversation, personal diary, love letter, or e-mail constitutes personal information.[48]

Second, the information could describe the individual in some manner besides the above authorship relation. On the one hand, it could speak to some permanent or nonfleeting status of the individual, either biological or social. For example, it could describe the individual's biometric state, such as sex, height, weight, blood type, fingerprint, retina pattern, DNA, or state of health. It could relate biographical facts, such as birth date, marital status, sexual orientation, immigration status, criminal history, or educational degrees. It could identify social connections, such as membership in religious and political organizations. On the other hand, descriptive information could record more discrete, transient actions taken by an individual. For example, it could chronicle that a particular individual visited a particular store at a particular time to purchase a particular item. Such information is routinely collected during undercover surveillance. Of course, in cyberspace, surveillance is not performed through traditional methods, such as a private investigator parked outside the target's home with thermos and binoculars. Instead, it is done through cyberspace itself, by collecting and sifting the data trail left by the individual's cyber-activity.[49]

Third, information not in the above two categories may still be personal if it is instrumentally mapped to the individual for institutional identification,

---

48. This view of "authorship" may be broader than that under copyright law. For one interesting intersection between copyright and privacy law, see text accompanying note 361 *infra*.

49. In classifying information as personal or not, should it matter that the descriptive information is accurate? For instance, is there any privacy issue when a newspaper "discloses" that someone is pregnant when she in fact is not? On the one hand, no. Since the information is inaccurate, or even purposefully made up, its dissemination does not seem to undermine the person's control over information about herself. It simply is not information about the individual. It is fiction. To be sure, dissemination of false information about oneself can be grating. But irate individuals can protect their reputations through false light, defamation, and libel.

On the other hand, inaccurate information can implicate a crucial privacy interest. As explained below, one benefit of having control over personal information is to prevent the use of inaccurate information in decisionmaking processes that affect the individual. Accordingly, a conception of information privacy that concerned itself exclusively with truthful information would be incomplete. Even falsehoods raise information privacy concerns.

secured access, or provision of some service or good. Usually, such information bears no prior relation to the individual. The best example is the Social Security number. In no way does the individual create or author the number. Nor does it describe the individual's state-of-being or actions, except that it is mapped to the individual by the federal government for record-keeping purposes. This category of personal information includes confidential[50] pieces of information that act as keys to secured functions or processes, such as passwords to login to a network and to use automatic teller machines.

These three categories are not mutually exclusive. For instance, an e-mail that describes a specific individual is personal in at least two different senses. It is personal vis-à-vis the sender of the e-mail in an authorship relation; it is personal vis-à-vis the individual mentioned in a descriptive relation. Also, certain types of information that are personal in an instrumental mapping sense may be personal in a descriptive sense. Consider the common practice of using the mother's maiden name as a password for remote access to one's bank account. Viewed solely as a key to secured processes, it is an instrumentally mapped piece of personal information; viewed as disclosing familial relationships, it is a descriptive piece of personal information. Despite some overlap, these three categories clarify the different ways in which a datum might be "personal," differ enough so as to be conceptually useful, and span the space of personal information.

2. *Nonpersonal information.*

If information bears no linkage to an individual, then it is not personal information and, according to the definition of privacy, lacks privacy significance. The link may be missing in three ways. First, the information simply may not be about an individual human being. For instance, the datum "π is

50. Confidentiality is often mistaken for privacy. I define the former as a measure of the degree and terms of disclosure. If information has been disclosed to many people or to the world at large, then it is said to be "not confidential." Of course, if this disclosure is accompanied by firm restrictions on subsequent dissemination, then it may be called "confidential," in the hope that the cat will stay in the bag. If the information has been disclosed to a few persons, but with no terms or restrictions on its subsequent dissemination, it is again said to be "not confidential." Finally, when used as a legal term-of-art, "confidential" often describes those communications within a relationship legally protected by a testimonial privilege. *See, e.g.*, BLACK'S LAW DICTIONARY 298 (6th ed. 1990).

Information privacy differs from confidentiality in at least two ways. First, privacy concerns itself only with personal information, whereas confidentiality is relevant to all types of sensitive or valuable information. In addition, as made plain by the IITF definition, information privacy is not only concerned with the disclosure of personal information, but also with its acquisition and use. *See* IITF PRINCIPLES, *supra* note 19, at 5. Even if personal information is maintained confidentially, it still can be used inappropriately. For example, if I voluntarily disclose my Social Security number for one authorized purpose, but the number is used for another unauthorized purpose, then my privacy would have been violated even though the confidentiality of the number would not necessarily have been breached.

3.14 to three significant digits" is not linked to any individual via an authorship, description, or instrumental mapping relation. Therefore, it is not personal information, which means it poses no privacy concerns.

Second, although about an individual, the information may not be identifiable to that specific individual because it has been anonymized. Consider, for example, an anonymous poll conducted by phone, in which responses are not linked to the telephone number, and the individual's identity is never ascertained. Here, by hypothesis, the data cannot be traced back to the specific individual from whom they were collected. Thus, although the data are about the views of human beings, they are not personal information and seemingly pose no privacy threat.

But we must recognize that anonymity comes in shades. Although no specific individual is identified facially, the individual may be identifiable in context or with additional research.[51] A prime example of such superficial anonymity is the interviewee—typically victim, witness, or whistle-blower—who is ensured anonymity by law enforcement or the media, but is nevertheless recognized under the totality of the circumstances.[52]

A more subtle qualification also deserves mention. Imagine that a psychiatrist publishes verbatim counseling notes in a best-selling book, but in a way that the specific identity of the patient cannot be determined. If the patient protests at having her story chronicled in agonizing detail to the public, could the good doctor respond that because the information is not identifiable to the specific patient, even with additional research, it is not "personal information." And, because it is not personal information, the patient lacks any privacy claim? To my mind, this reasoning fails to account for the residual privacy interest that exists, notwithstanding the anonymity. Recall that privacy involves the control of the flow of personal information in all stages of processing—acquisition, disclosure, and use. Simply because the information is anonymized at the disclosure and use stages, and thus not personal in one sense, does not mean that it was not personal information when originally acquired from the individual. This refutes the doctor's claim that no "personal information" is at stake. In other words, a genuine privacy claim is in play.[53]

---

51. *See* David G. Post, *Pooling Intellectual Capital: Thoughts on Anonymity, Pseudonymity, and Limited Liability in Cyberspace*, 1996 U. CHI. LEGAL F. 139, 149-51 (discussing how context can sometimes provide identity information of facially anonymous e-mails).

52. *See, e.g.*, Doe v. American Broad. Cos., 543 N.Y.S.2d 455 (N.Y. App. Div. 1989) (noting that rape victims interviewed on television were recognized despite assurances of anonymity). Further, courts have recognized the possibility that information, not personally identifiable on its face, may be personally identifiable in context. *See, e.g.*, Arieff v. United States Dep't of the Navy, 712 F.2d 1462, 1465 (D.C. Cir. 1983) (discussing whether pharmaceutical prescription reports revealed the user's identity and were therefore exempt from the Freedom of Information Act).

53. In disclosing the information to her psychiatrist, the patient undoubtedly did not intend her story to be featured in rich detail in a bestseller. By printing her story, the psychiatrist disrespected

Third, although about individuals and not anonymized, the information is directly identifiable to a group and only indirectly identifiable to the individuals constituting that group. Under one interpretation of the privacy definition, because the information is directly about the group and not the individuals that constitute the group, the data are not personal and stand outside privacy's realm. But this seems formalistic. A more functional approach would recognize that groups, even those recognized as legal persons, function only through the actions of the human individuals who are its members. Accordingly, information concerning a group concerns also those individuals that constitute the group. What we ultimately label as "personal" should thus depend on context, such as the size of the group and the degree of focus the information places on some subset of that group.

With this nuanced, functional understanding, we can better answer the perplexing question whether, for example, a corporation has privacy interests. A corporation *qua* corporation does not. Only the individuals that make up the corporation do. This does not mean that the corporation must lack standing to argue the privacy interests of its constituent individual members. It does mean, however, that the foundation of any such group privacy claim lies originally in the interests of individual human beings.[54]

In practice, then, the answer to group privacy questions turns on context. On the one extreme, we can have information such as "IBM's stock is at thirty points today." In some ways, this information is identifiable to all those individuals affiliated with IBM, as directors, officers, and shareholders, but the link is so diffuse that I am comfortable classifying this datum as not personal information. At the other extreme, we can have information that a closely held corporation with one stockholder and two officers evaded taxes. This information is tightly enough linked to few enough people that it should be considered personal information.[55]

---

the individual's desires regarding her personal information. This, in my view, diminishes her privacy. The crucial point here, however, is not the substantive judgment about whether the patient's privacy was violated; instead, the essential insight is that this type of fact-pattern presents an authentic, if unusual, privacy problem, which cannot be dissolved by wordplay. *Cf.* Doe v. Roe, 400 N.Y.S.2d 668 (N.Y. Sup. Ct. 1977) (finding a breach of implied contract between psychiatrist and patient).

54. Compare Edward Bloustein's thoughts. Although he has used the concept of "group privacy," it is entirely derivative of the privacy enjoyed by each individual who constitutes the group. *See* Edward J. Bloustein, *Group Privacy: The Right to Huddle*, 8 RUT.-CAM. L.J. 219, 221 (1977) ("'Group privacy' is an attribute of individuals in association with one another within a group, rather than an attribute of the group itself.").

55. As another example, the datum that five people living on a particular street block are Asian American should be considered personal. Notwithstanding its promise of confidentiality, the Census Bureau disclosed to the Army the number of Japanese Americans living on each block to facilitate their internment in World War II. *See* DAVID BURNHAM, THE RISE OF THE COMPUTER STATE 56 (1983).

Rest assured that this nuanced view of group privacy will not leave corporate entities—which, like individuals, surely have their secrets[56]—unable to control the flow of information about themselves. Even if such data cannot be controlled under the rubric of privacy, they can be managed through alternate legal categories, such as contract, tort, and intellectual property.[57] Indeed, a potent array of unfair competition, trade secret, patent, trademark, and copyright law, in addition to confidentiality agreements,[58] support an institution's ability to control various types of information identifiable to itself.[59] In addition, collective entities often have the wherewithal to employ self-help security[60] measures so that information in their control flows only in ways they choose.

---

56. Certain commentators have argued that it makes more economic sense to protect organizational secrets than individual ones. *See, e.g.*, Richard A. Posner, *The Right of Privacy*, 12 GA. L. REV. 393 (1978).

57. My take on group privacy comports with the common law tort of invasion of privacy. *See* RESTATEMENT (SECOND) OF TORTS: PERSONAL CHARACTER OF RIGHT OF PRIVACY § 652I (1977) ("Except for the appropriation of one's name or likeness, an action for invasion of privacy can be maintained only by a living individual whose privacy is invaded."); *id.* cmt. (c) ("A corporation, partnership or unincorporated association has no personal right of privacy. . . . It has, however, a limited right to the exclusive use of its own name or identity in so far as they are of use or benefit, and it receives protection from the law of unfair competition.").

58. *See, e.g.*, Cohen v. Cowles Media Co., 501 U.S. 663 (1991) (finding a newspaper liable for breaching a source confidentiality agreement notwithstanding the First Amendment); Snepp v. United States, 444 U.S. 507 (1980) (holding that a former Central Intelligence Agency ("CIA") employee breached his fiduciary obligation by failing to submit material concerning the CIA for prepublication review).

59. *See* Edmund W. Kitch, *The Law and Economics of Rights in Valuable Information*, 9 J. LEGAL STUD. 683, 688-708 (1980) (describing ways in which institutions control their information).

60. Another term consistently confused with privacy is "security," which measures the degree of confidentiality, integrity, reliability, and availability of information and related systems. "Confidentiality" is the assurance "that information will be held in confidence with access limited to appropriate persons." SECURITY ISSUES FORUM, INFORMATION INFRASTRUCTURE TASK FORCE, NII SECURITY: THE FEDERAL ROLE 2 (June 5, 1995). "Integrity" is the confidence "that information will not be accidentally or maliciously altered or destroyed." *Id.* at 1. "Reliability" is the confidence "that systems will perform consistently and at an acceptable level of quality." *Id.* at 2. "Availability" is the assurance "that information and communications services will be ready for use when expected." *Id.*

Privacy concerns itself only with personal information, whereas security is relevant to all types of information. For example, the recipe for Coca-Cola Classic may be a trade secret that warrants military-grade security. However, that information is not personal information and has no privacy ramifications. Moreover, "privacy" should appear prior to "security" in the policymaker's lexicon because privacy answers "what to do," whereas security answers "how to do it." The right to privacy is a right that society should ensure to some reasonable degree. Once that measure is set, security enters the picture and illuminates how, through managerial and technical procedures, personal information can be kept secure in accordance with established privacy norms.

C. *Privacy's Values*

1. *Values.*

Now that we know what information privacy is, we should probe what purpose it serves.[61]

Avoiding embarrassment. In any given culture, disclosures of certain behaviors, actions, or fates will embarrass the individual—even when the behavior, action, or fate is neither blameworthy nor stigmatized. Take urination for example. There is nothing wrong with urination; all humans do it. The fact that someone urinates is not going to be used against her. However, a visual disclosure of that behavior—for instance, being caught on videotape through a hidden camera—would cause intense embarrassment for most Americans. Another example is minor hemorrhoids. Assume that this fact will not be used against the person in any way. The individual will not pay more for health insurance, will not drop in social standing, and will not lose her job or friends. Nevertheless, the broad disclosure of this fact would embarrass many, perhaps most, people.

That these examples are culturally contingent makes them no less real.[62] In other words, the fact that different cultures may react differently to such disclosures does not deny that, for each culture, there are some zones of behavior, actions, or fates the disclosure of which—in and of itself—will cause discomfort or embarrassment.[63] One value of information privacy, then, is to avoid the simple pain of embarrassment.

Constructing intimacy. An individual's capacity to disclose personal information selectively also supports her ability to modulate intimacy. Charles Fried has argued this case most prominently.[64] By virtue of information privacy, one can selectively regulate the outflow of personal information to others. By reducing this flow to a trickle, one can construct "aloofness, removal, and reserve,"[65] and maintain substantial social distance. Conversely,

---

61. The analysis here of the relevant values supporting privacy is not complete. I discuss the value of dignity separately in Part III.A.2 below. Other values on which I do not dwell are listed in KIM LANE SCHEPPELE, LEGAL SECRETS: EQUALITY AND EFFICIENCY IN THE COMMON LAW 181-83 (1988) (arguing that privacy is also necessary for sanity and role maintenance).

62. *See* Irwin Altman, *Privacy Regulations: Culturally Universal or Culturally Specific?*, 33 J. SOC. ISSUES 66, 67 (1977). For interesting discussions of how different cultures maintain privacy, see, for example, ALTMAN, *supra* note 23, at 14 (discussing the Tuareg veil worn almost continually over the mouth), and Robert F. Murphy, *Social Distance and the Veil*, *in* PHILOSOPHICAL DIMENSIONS OF PRIVACY, *supra* note 22, at 34, 42-44 (same).

63. *See* ALTMAN, *supra* note 23, at 42 ("[I]t might be said that mechanisms for separating the self and non-self—that is, for regulating interpersonal boundaries to achieve a desired level of privacy—are universal and present in all societies.").

64. *See* Fried, *supra* note 41. *See generally* James Rachels, *Why Privacy Is Important*, *in* PHILOSOPHICAL DIMENSIONS OF PRIVACY, *supra* note 22, at 290 (offering similar arguments).

65. Murphy, *supra* note 62, at 34.

one can release a more telling flow of personal information,[66] which invites and affirms intimacy.[67]

According to Fried, information privacy is necessary to create social relationships that go beyond the basic respect due all human beings.[68] Something in addition to basic human respect must exist between two individuals to transform their relationship into one of trust, friendship, or love. That additional something is intimacy, which is partly created by the release of secrets—the selective disclosure of personal information.[69] Without information privacy, we would be less able to disclose on a case-by-case basis the nonpublic facets of our personality. Thus, we would lack the "moral capital"[70] needed to construct intimacy.[71]

I concur with Jeffrey Reiman's critique of Fried that intimacy is more related to the sharing of experiences than the sharing of secrets.[72] This does not mean that information privacy has nothing to do with modulating intimate relationships. I believe that intimacy, at least for adults in current American culture, involves the display of certain behaviors unseen in public areas, such as playfulness, childlikeness, and certain types of physical touching—which take root and flower best in an information preserve, away from the harsh light of publicity.[73] If we were under observation, we would not be able to display caring to other individuals as freely, spontaneously, or completely as we might otherwise.[74] This, in turn, would hinder the construction of deep social relationships.

---

66. Take, for example, the choice to reveal selectively that one is gay or lesbian. *See* Susan J. Becker, *The Immorality of Publicly Outing Private People*, 73 OR. L. REV. 160, 206 (1994) ("Many gay people find terrifying the option of taking one giant leap to universally disclose this intimate detail of their lives, while the possibility of taking a series of small steps towards that goal is palatable.").

67. *See* Murphy, *supra* note 62, at 36 ("This imposition of distance on the parameters of the role set does more than make other roles possible, for it promotes the solidarity of the relationship itself. In this sense, many role sets are effective secret societies.").

68. *See* Fried, *supra* note 41, at 477.

69. *See id.* at 484-85.

70. *See id.* at 484.

71. Information privacy may have a more complicated relationship with intimacy depending upon where two people are in their relationship. In the beginning of a relationship, a lack of information privacy might actually promote the creation of intimacy. To take a common example, a person is often more inclined to go on a first date with someone if she knows something about him. I think Fried's response would be that, once that relationship starts, information privacy is instrumental in furthering intimacy.

72. *See* Jeffrey H. Reiman, *Privacy, Intimacy, and Personhood*, *in* PHILOSOPHICAL DIMENSIONS OF PRIVACY, *supra* note 22, at 300, 305.

73. *Cf.* Robert S. Gerstein, *Intimacy and Privacy*, *in* PHILOSOPHICAL DIMENSIONS OF PRIVACY, *supra* note 22, at 265, 268 (noting that observation kills the spontaneity necessary for intimacy); *see also* text accompanying notes 274-294 *infra* (discussing the relationship between surveillance and dignity).

74. *See* Richard A. Wasserstrom, *Privacy: Some Arguments and Assumptions*, *in* PHILOSOPHICAL DIMENSIONS OF PRIVACY, *supra* note 22, at 317, 324 (noting that the lack of pri-

Averting misuse. Yet another value of privacy is that it protects against improper uses of personal information. Personal information can be misused in two ways. First, it can derail an otherwise fair process that distributes benefits and burdens. Many social goods—such as jobs, offices, remuneration, and respect—as well as social bads—such as unfriendliness, disrespect, and imprisonment—are granted or denied on the basis of data about ourselves. If these social goods and bads are allocated based on personal data of poor quality, unfairness may result: Garbage in, garbage out.[75] Further, high quality information in one context may be low quality information in another because, as Kenneth Karst explains, "the evaluator and the recipient of his statement may not share the same standards for reducing a complex set of facts to evaluative inferences or even the same language."[76] Worse, such decisions may be difficult to discover and correct,[77] especially when they are generated through automated processes. Computers, with their air of objectivity and infallibility, resist dispute.[78] One way to check against such information misuse is to give the individual greater control over the flow of personal information. An individual with such control will take preventative

---

vacy is harmful because "the kind of spontaneity and openness that is essential to [people] disappears with the presence of an observer").

75. Poor quality includes: inaccurate information; technically accurate but misleading information, because it is incomplete or stale; and irrelevant information, because it is accurate and not-misleading but inappropriately considered. *See* IITF PRINCIPLES, *supra* note 19, at 6 (stating that quality of personal information depends on accuracy, timeliness, completeness, and relevance). Errors in databases are not exceptional. *See, e.g.*, KENNETH C. LAUDON, DOSSIER SOCIETY: VALUE CHOICES IN THE DESIGN OF NATIONAL INFORMATION SYSTEMS 139 (1986) (stating that, over a one year period, 74.3% of records disseminated by the Federal Bureau of Investigation ("FBI") Identification Division had "some significant quality problems"); *id.* at 140-42 (noting that 11.2% of the warrants for persons listed on the FBI Wanted Persons list were no longer valid, 6.6% were inaccurate, and 7.0% dealt with offenses sufficiently trivial that extradition and prosecution were unlikely).

76. Kenneth L. Karst, *"The Files": Legal Controls over the Accuracy and Accessibility of Stored Personal Data*, 31 LAW & CONTEMP. PROBS. 342, 356 (1966); *see also id.* at 357 (arguing that the risk of inaccuracy is greatest when the file is read by an outsider unfamiliar with the system and unaware that the language or the standards of the evaluator differ from his own); Spiros Simitis, *Reviewing Privacy in an Information Society*, 135 U. PA. L. REV. 707, 718 (1987) (arguing that the loss of data's context distorts their content).

77. *See* Karst, *supra* note 76, at 358.

78. *See* BURNHAM, *supra* note 55, at 151 ("[E]ven highly educated people are prepared to grant the computer far more power than it actually possesses."); HEW REPORT, *supra* note 20, at xx ("[T]he net effect of computerization is that it is becoming much easier for recordkeeping systems to affect people than for people to affect recordkeeping systems."); LAUDON, *supra* note 75, at 4 (contending that decisions about us are made less on "personal face-to-face contact" and more on information about us, our "data image"); Simitis, *supra* note 76, at 718 (noting that once a decision has been made by the computer, the burden of proof is shifted onto the individual to prove that the computer is wrong).

measures, for instance, by keeping irrelevant personal data away from the decisionmaker.[79]

Second, information can be misused by making us vulnerable to unlawful acts and ungenerous practices. After all, personal information is what the spying business calls "intelligence," and such "intelligence" helps shift the balance of power[80] in favor of the party who wields it.[81] To take a simple example, knowledge of our home phone number and address makes us more vulnerable to harassers[82] and stalkers.[83] Personal information can also make us vulnerable, for instance, to identity theft.[84] Besides outright illegal acts, another's control of our personal information can make us susceptible to a whole range of ungenerous practices. It could subject us to influence that crosses the line between persuasion and undue influence. Sophisticated advertisers, for example, do not merely track consumer demand; they manu-

---

79. One such example may be the borrower's race in a loan application. *See* GANDY, *supra* note 18, at 200-01 (discussing racially discriminatory lending); 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, 79 (same); *see also* Peter P. Swire, *The Persistent Problem of Lending Discrimination: A Law and Economics Analysis*, 73 TEX. L. REV. 787, 814-30 (1995) (explaining why markets may not stop racial discrimination in lending).

80. I use "power" here to mean nothing more complicated than "an actual capacity to do or prevent something." STEPHEN R. MUNZER, A THEORY OF PROPERTY 178 (1990).

81. For further discussion of how conflicts over information flow are conflicts over power, see BOK, *supra* note 34, at 19. Bok states:

> Conflicts over secrecy—between state and citizen . . . or parent and child, or in journalism or business or law—are conflicts over power: the power that comes through controlling the flow of information. To be able to hold back some information about oneself or to channel it and thus influence how one is seen by others gives power; so does the capacity to penetrate similar defenses and strategies when used by others.

Id. (citation omitted).

82. For a disturbing story of privacy and harassment, see Nina Bernstein, *Personal Files via Computer Offer Money and Pose Threat*, N.Y. TIMES, June 12, 1997, at A1 (describing a prisoner who processed a woman's consumer survey on behalf of Metromail Corporation and later sent her a sexually threatening letter).

83. Actress Rebecca Schaffer was murdered by a crazed fan who had located her home through Department of Motor Vehicles records. *See* REGAN, *supra* note 18, at 102-03 (discussing the types of problems that led to the introduction of the Driver's Privacy Protection Act of 1994 ("DPPA"), 18 U.S.C. §§ 2721-2725, which was later incorporated into the Violent Crime Control and Law Enforcement Act of 1994, Pub. L. No. 103-322, 108 Stat. 1796 (codified as amended in scattered sections of 18 U.S.C.)).

84. In identity theft, an impostor obtains enough personal information to impersonate his victim in financial transactions. Typically, the impostor applies for a credit card under the victim's name and then charges up the card, leaving the victim to deal with the impostor's debts. Often, the victim's credit is ruined and may take years to repair. *See* BOARD OF GOVERNORS OF THE FED. RESERVE SYS., REPORT TO THE CONGRESS CONCERNING THE AVAILABILITY OF CONSUMER IDENTIFYING INFORMATION AND FINANCIAL FRAUD 18-20 (1997) [hereinafter FEDERAL RESERVE REPORT] (on file with the *Stanford Law Review*) (noting the financial effects of fraud on society as a whole); PRIVACY RIGHTS CLEARINGHOUSE, SECOND ANNUAL REPORT 28-32 (1995) (suggesting that government agencies are providing inadequate protection of individual privacy rights).

facture it outright.[85] Detailed knowledge of who we are and what we consume makes the job of preference fabrication that much easier.[86] More disturbingly, personal information can be misused by making us vulnerable to prejudice or unwarranted disesteem. An example is the information that one is gay, which could be evidenced by accessing certain Internet discussion groups or making certain cyberspace purchases.[87] For those not generally "out," the inability to control this information creates tremendous social and psychological vulnerability.

Individual vulnerability has social consequences. It chills individuals from engaging in unpopular or out-of-the-mainstream behavior. While uniform obedience to criminal and tort laws may deserve praise, not criticism, excessive inhibition—not only of illegal activity but also of legal, but unpopular, activity[88]—can corrode private experimentation, deliberation, and reflection.[89] The end result may be bland, unoriginal thinking[90] or excessive

---

85. The argument that advertising, in its multifarious forms, can alter demand is uncontroversial. *See* Daniel Hays Lowenstein, *Commercial Speech and the First Amendment: "Too Much Puff": Persuasion, Paternalism, and Commercial Speech*, 56 U. CIN. L. REV. 1205, 1215-17 (1988) (making a qualified case that advertising increases smoking); *cf.* Glickman v. Wileman Bros. & Elliott, Inc., 117 S. Ct. 2130, 2141 (1997) ("Generic advertising is intended to stimulate consumer demand for an agricultural product in a regulated market. That purpose is legitimate and consistent with the regulatory goals of the overall statutory scheme.").

86. *See* MILLER, *supra* note 17, at 43 (expressing concern over cybernetic manipulation of consumers and voters).

87. *See, e.g.*, Philip Shenon, *Navy Case Combines Gay Rights and On-Line Privacy*, N.Y. TIMES, Jan. 17, 1998, at A6 (describing how the Navy accessed America Online subscription information to obtain the true identity of an on-line personality named "Tim" who had claimed to be both gay and a Navy employee).

88. Consider the chilling effect caused by military surveillance of domestic political groups, including the American Civil Liberties Union, the Southern Christian Leadership Conference, and the National Association for the Advancement of Colored People. *See* MILLER, *supra* note 17, at 40 (explaining that Army intelligence maintained files on these and other activist political organizations). Although the state enjoys a virtual monopoly on lawful coercive force, I believe that a substantially similar effect can be achieved through private sector surveillance. As John Stuart Mill warned:

> [The] means of tyrannizing are not restricted to the acts which [society] may do by the hands of its political functionaries. Society can and does execute its own mandates; and if it issues wrong mandates instead of right, or any mandates at all in things with which it ought not to meddle, it practices a social tyranny more formidable than many kinds of political oppression, since, though not usually upheld by such extreme penalties, it leaves fewer means of escape, penetrating much more deeply into the details of life, and enslaving the soul itself. Protection, therefore, against the tyranny of the magistrate is not enough; there needs protection also against the tyranny of the prevailing opinion and feeling, against the tendency of society to impose, by other means than civil penalties, its own ideas and practices as rules of conduct on those who dissent from them . . . .

JOHN STUART MILL, ON LIBERTY 4-5 (Hacket Publishing 1978).

89. *See* Stanley I. Benn, *Privacy, Freedom, and Respect for Persons*, in PHILOSOPHICAL DIMENSIONS OF PRIVACY, *supra* note 22, at 223, 241 ("We act differently if we believe we are being observed. If we can never be sure whether or not we are being watched and listened to, all our actions will be altered and our very character will change." (quoting Hubert Humphrey)); Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the*

conformity to unwarranted social norms.[91] Worse, the self-repression of activity and communication could undermine the self-critical capacities of a polity.[92] This is why totalitarian regimes have maligned a desire for privacy as deviant, in part to sap an individual's ability to question the status quo and to experiment with alternate conceptions of the good life.[93]

2. *Countervalues.*

It would be one-sided to discuss only the values supporting information privacy when prominent countervalues—values against individual control over personal information—also exist.

Commerce. By requiring the individual's consent before personal data are processed, privacy applies friction to the flow of information. This friction, the argument goes, hurts commerce; better information leads to better markets. When this argument is made, two stories are often told—one about junk mail, the other about consumer credit. The junk mail story starts by explaining that junk mail is only "junk" because it was sent to the wrong person. If the direct marketing industry had better intelligence about personal interests and preferences—for example, by being able to examine an individ-

---

United States, 80 IOWA L. REV. 553, 560 (1995) (noting how data processing "creates a potential for suppressing a capacity for free choice: the more that is known about an individual, the easier it is to force his obedience").

90. Oliver Wendell Holmes lamented that "the very minute a thought is threatened with publicity it seems to shrink toward mediocrity." Bloustein, *supra* note 54, at 255 (quoting O.W. HOLMES, THE POET AT THE BREAKFAST-TABLE 344 (1872)).

91. Norms are nonlegal obligations obeyed out of a combination of internalized duty and fear of externally imposed sanction. Obviously, not all social norms are warranted. Specifically, Richard McAdams has demonstrated that if social norms arise from individuals' desire for esteem, many social norms will be economically inefficient. *See* Richard H. McAdams, *The Origin, Development, and Regulation of Norms*, 96 MICH. L. REV. 338, 412-16 (1997). Information privacy can resist such norms in two ways. First, it can make norm violations harder to detect, thereby making norms harder to enforce. Second, it may prevent the initial construction of the norm by interfering with the public recognition of group consensus, which is a prerequisite for norm construction. *See id.* at 425-26. McAdams notes two qualifications. First, because privacy resists both efficient and inefficient norms, any judgment on whether privacy produces a net increase in efficiency depends on, among other things, the relative proportion of efficient versus inefficient norms. Second, in certain cases, privacy may perpetuate, not resist, a norm by decreasing communicative exchange about a consensus in the past that has since disappeared. *See id.* at 426-27.

92. *See* Gavison, *supra* note 34, at 455 (arguing that privacy fosters moral autonomy, which is necessary for democracy). The Supreme Court recognized as much in *NAACP v. Alabama*: "This Court has recognized the vital relationship between freedom to associate and privacy in one's associations. . . . Inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs." 357 U.S. 449, 462 (1958).

93. *See* WESTIN, *supra* note 41, at 23 (observing that totalitarian regimes tarnish privacy as immoral and antisocial); Bloustein, *supra* note 54, at 226-27 ("Unlike the totalitarian ideology, democratic political philosophy favors autonomous or private associations because they constitute independent sources of power and initiative which act to forestall undue accumulation of state power.").

ual's history of consumption—people would receive less "junk." Because information privacy makes this more difficult, it increases the search costs of matching interested buyers with interested sellers. In short, more privacy means more junk. The consumer credit story starts by noting that a freer flow of personal information can decrease the costs of consumer credit by helping creditors avoid bad credit risks. Additional personal information allows greater discrimination among individuals according to whatever characteristic is relevant to a particular transaction.[94] This, in turn, decreases the cost of such transactions either generally, or, at the least, for those individuals who possess a favorable set of characteristics.[95]

The commerce argument, as thus stated, presumes that privacy necessarily entails information blockage. But this is not so. If individuals will truly benefit by releasing their personal data, e.g., by getting less junk or cheaper credit, they will rationally choose to do so.[96] Information privacy does not mandate informational quarantine; it merely requires that the individual exercise control within reasonable constraints over whether, and what type of, quarantine should exist. Accordingly, these arguments do not demonstrate that the individual should be deprived of information privacy. At most, they suggest that individuals should be open to information processing in exchange for commercial benefit and that society should make such exchanges feasible.[97]

Truthfulness. Information privacy allows one to have thoughts, beliefs, conditions, and behaviors without the knowledge of others, thereby making it easier to have public personae distinct from private ones. This differentiation between public and private visages need not be used for good, such as self-determination and deliberative politics. Instead, the argument goes, it will be used to deceive and defraud. Individuals will not only keep poor quality information away from decisionmakers, they will also conceal high quality, but legitimately detrimental, information. The cover of privacy might encourage individuals not only to engage in activity unjustifiably

---

94. In credit transactions, these characteristics include the individual's previous repayment history. In other transactions, such as health insurance, such characteristics might include the individual's genetic makeup, medical history, and lifestyle risks. For a thoughtful analysis of medical privacy, see generally Paul M. Schwartz, *Privacy and the Economics of Personal Health Care Information*, 76 TEX. L. REV. 1 (1997).

95. *See* George J. Stigler, *An Introduction to Privacy in Economics and Politics*, 9 J. LEGAL STUD. 623, 628-33 (1980) (arguing that the ability to classify more accurately will lead to greater economic efficiency).

96. *See* Mary J. Culnan, *Self-Regulation on the Electronic Frontier: Implications for Public Policy*, *in* NTIA REPORT, *supra* note 11, at text accompanying note 7 (no pagination in electronic copy).

97. This requires attention not only to what is legally permissible, but also to what is economically feasible. Here I am concerned about transaction costs preventing efficient processing of personal information. For a sustained analysis of privacy in economic terms, see text accompanying notes 229-304 *infra*.

stigmatized but also justifiably stigmatized. Worse, they may be hypocrites, publicly espousing norms they privately abandon.[98] The parade-of-horribles conjures easily: the unrehabilitated child molester volunteering for day care; the domestically violent tyrant passing as winsome celebrity; the sexually promiscuous person, infected with herpes, claiming to be disease free; the reckless driver swearing falsely to be accident free. Perhaps Richard Posner was right to recast invasions of privacy as self-defense against deception.[99]

It would be facile to deny that information privacy can cloak our darker sides and aid misrepresentation. Equally facile, however, is the inference that information privacy is thus inexorably the handmaiden of deception. Privacy is not valuable only to those with something discreditable to hide. Individuals do not always seek to conceal or control personal information to exploit others in some acquisitive, tortious, or immoral way.[100] Put in other terms, secrecy—the intentional concealment of personal information—does not always amount to lying.[101] The hallowed example is the secret ballot.[102]

Moreover, it is not inherently wrong for individuals to have differing private and public masks.[103] Consider how differently we act, and rightly so, between work and home. Only an unsophisticated psychology assumes one true, essential personality, with all other personae spurned as deceitful masks. In fact, all our masks, all our roles, constitute integral facets of our personalities, none of which is necessarily privileged, true, or authentic.[104] This is not to say that no core personality exists. But this core personality is a weighted composite of the multiple personalities we experience and culti-

---

98. Consider the ingenious reporter who investigated Supreme Court nominee Robert Bork's video rental history. The investigation revealed nothing juicy. But members of Congress—painfully aware of their own vulnerability—immediately passed the VPPA, which proscribes the release of such information. *See* Video Privacy Protection Act of 1988, 18 U.S.C. §§ 2710-2711 (1994); *see also* S. REP. NO. 100-599, at 5 (1988) (citing the Bork incident as impetus for the legislation); Joe Domanick, *Maybe There* Is *a God: Six Lessons in the Pitfalls of Public Hypocrisy*, PLAYBOY, Aug. 1990, at 110 (discussing the hypocrisy of, inter alia, Robert Bauman, Jimmy Swaggert, and Jim Bakker).

99. Posner, *supra* note 56, at 395.

100. *See* Edward J. Bloustein, *Privacy Is Dear at Any Price: A Response to Professor Posner's Economic Theory*, 12 GA. L. REV. 429, 445 (1978) (discussing a woman giving birth and a man writing love letters to his wife).

101. *See* BOK, *supra* note 34, at xv (explaining that lying is prima facie bad, but that secrets are not).

102. *See* Sweezy v. New Hampshire, 354 U.S. 234, 250-51 (1957) (discussing the importance of freedom of political expression). Just slightly less hallowed are a jury's secret deliberations. *See* Clark v. United States, 289 U.S. 1, 13 (1933) ("Freedom of debate might be stifled and independence of thought checked if jurors were made to feel that their arguments and ballots were to be freely published to the world.").

103. *See* Ferdinand Schoeman, *Privacy and Intimate Information*, *in* PHILOSOPHICAL DIMENSIONS OF PRIVACY, *supra* note 22, at 403, 408-09 (arguing that it is important that people maintain different dimensions of themselves in different contexts).

104. *See, e.g.*, Margaret Chon, *Multidimensional Lawyering and Professional Responsibility*, 43 SYRACUSE L. REV. 1137, 1138-39 (1992) (agreeing in the context of legal ethics).

vate.[105] The ability to maintain divergent public and private personae creates the elbowroom necessary to resist social and political homogeneity.[106]

In sum, information privacy does not necessarily promote deception and fraud. It can do so only if both the nature of the relationship between the individual and the information user, and the ethical or legal duties of disclosure inherent to that relationship, command an openness that information privacy prevents. What is important is that in most cyberspace transactions, which I describe below, far more information is collected than any self-defense "need to know" principle could justify.

II. CYBERSPACE: A TECHNICAL DESCRIPTION

A. *Cyberspace Introduced: A Brave New World*

The neologism "cyberspace" is shorthand for the emerging Global Information Infrastructure ("GII"). The GII, like all information infrastructures, moves information from sender to receiver through some medium. In cyberspace, information typically moves through a hybrid of wireline[107] and wireless pathways.[108] For example, cable television signals are delivered to

---

105. *See* Rachels, *supra* note 64, at 294 (suggesting that the variances in behavior define the relationships, not the individual). Posner has come around on this point. *See* RICHARD A. POSNER, OVERCOMING LAW 534-35 (1995) (arguing that one's public self is no less real than one's private self).

106. I take no position on privacy's connection to rehabilitation. Some commentators argue, however, that information privacy is necessary for an individual to "remold her identity or reform her character." C. Edwin Baker, *Posner's Privacy Mystery and the Failure of Economic Analysis of Law*, 12 GA. L. REV. 475, 479 (1978). Without such ability, the past would always catch up to the present, never allowing us to "overcome the mistakes of the past." *Id.* at 480. *But see* Richard A. Epstein, *Privacy, Property Rights, and Misrepresentations*, 12 GA. L. REV. 455, 472 (1978) (criticizing rehabilitation as a justification for privacy).

This conflict appears starkly in those laws, such as Megan's Law, which require notification of neighbors when a convicted sex offender moves into a neighborhood. *See, e.g.*, N.J. STAT. ANN. §§ 2c:7-2 to -11 (West 1995). Currently 29 states have such community notification laws. The convicted felon's privacy rights might have to be sacrificed where the safety of the community, especially its children, is in jeopardy. For those who think this notification requirement is excessively harsh or double punishment, I am persuaded by my colleague Eugene Volokh's pithy retort: "These are not punishments, they're consequences." Lori Basheda, *"Megan's Law" Challenged by Molester*, ORANGE COUNTY REG., June 23, 1997, at B1. For the opposite twist on the trade-off between privacy and protection of children, see *Largest Database Marketing Firm Sends Phone Numbers, Addresses of 5,000 Families with Kids to TV Reporter Using Name of Child Killer*, BUS. WIRE, May 13, 1996, *available in* LEXIS, News Library, Bwire File (reporting the sale of phone numbers, addresses, and ages of 5000 children by Metromail to a reporter using the name "Richard Allen Davis," the person convicted of murdering 12-year-old Polly Klaas).

107. In wireline communications, information signals travel along a bounded physical medium, such as twisted-pair copper wire (the local loop portion of our public-switched telephone network), coaxial cable (cable television), and optical fiber (trunk lines between local telephone exchanges). *See* HELD, *supra* note 3, at 45-55 (discussing various transmission media).

108. In wireless communications, information signals travel as electromagnetic radiation, unguided by any tangible medium. Examples include terrestrial broadcast (over-the-air television and

the local cable television company through wireless satellite feeds, but are then carried to the home via a hybrid wireline of optical fiber and coaxial cable. From the user's perspective, the exact path the information takes from place to place is irrelevant. What is important is that the information transfers with speed and security.[109]

Once information is transported, it is processed to provide some communicative functionality. For example, information transferred through our public, switched telephone network is processed to provide oral communications, low-resolution printouts (e.g., facsimiles), and low bandwidth links to computer networks such as bulletin board services (or BBSes), proprietary on-line services,[110] and the Internet.[111] Information transferred through wireless broadcast systems, such as direct-broadcast satellite and wireless cable, may be processed into video signals that provide traditional broadcast television-like content.

Cyberspace transfers, processes, and stores information faster, cheaper, and better than any information infrastructure we have had before. Faster transfer rates mean that video that once took an hour to download through a standard Internet connection now takes minutes.[112] Improved processing

---

radio), cellular telephony, line-of-sight microwave radio (linking telephone or "wireless cable" systems), and satellites (direct broadcast satellite TV). Other wireless examples include pagers, beepers, and satellite up-links and down-links.

109. For an explanation of how security differs from privacy, see note 60 *supra*.

110. Prominent examples include America Online, CompuServe, the Microsoft Network, and Prodigy.

111. The Internet is a worldwide packet-switched data network that exchanges information through a protocol called Transmission Control Protocol/Internet Protocol (individually "TCP" and "IP," collectively referred to as "TCP/IP"). In rough functional terms, the TCP breaks information down into small packets and numbers them sequentially for later reassembly. The IP addresses each packet with its intended destination. The physical technology of the Internet comprises communication lines—imagine them as phone lines—routers, specially designated computers that send packets of information to their IP addresses, and computers, which send, receive, and process the information transmitted. The Internet provides various communicative functions, such as file transfer, remote login, e-mail, video conferencing, news, and, most importantly, hypertext—the World Wide Web. For a brief, helpful description of the Internet in the law reviews, see Dan L. Burk, *Federalism in Cyberspace*, 28 CONN. L. REV. 1095, 1097-100 (1996).

112. Faster transfer rates stem from higher bandwidth communication lines, improved compression algorithms, and faster switching technologies. Consider the improvements to bandwidth made by upgrading from twisted pair copper wire to optical fiber. According to Nicholas Negroponte, the theoretical maximum bits per second that can travel along twisted-pair copper wire is six million bits per second (Mbps), whereas optical fiber has a theoretical maximum of one trillion bits per second (Tbps), which is six orders of magnitude higher. *See* NICHOLAS NEGROPONTE, BEING DIGITAL 22 (1995) (noting rapid improvements in bandwidth, the "capacity to move information down a given channel"). Also, compression algorithms are allowing us to squeeze more information into fewer bits. Currently, four studio-quality digital TV signals can be compressed into the bandwidth taken up by a single analog TV signal. *See id.* at 17 (describing how simple it has become to "compress and decompress, encode and decode"). Finally, superior switching schemes, such as Asynchronous Transfer Mode ("ATM"), can improve the rate of data delivery, holding forth the potential of full-screen, smooth, real-time transmissions of video. *See* HELD, *supra* note 3, at 419-33 (describing ATM technology).

means that users now can search efficiently through the vast cyber-sea of information through easily navigable interfaces. Improved storage means that cost concerns no longer loom large in forcing the reuse of storage media, such as hard drives.[113]

Converging improvements in information transfer, processing, and storage will soon produce a communications system that combines the high-bandwidth of our cable networks, the bidirectionality[114] and addressability[115] of our public, switched telephone networks, and the point-and-click computer interface of the World Wide Web (the "Web").[116] Accordingly, cyberspace of the near-future will likely look like an applet-enabled[117] Web, with data transfer rates fast enough to exchange not only text, but also real-time video and iconic or avatar interfaces far friendlier than today's. Local exchange carriers ("LECs"),[118] cable companies,[119] and their joint ventures are rebuilding their networks to provide such interactive, high-bandwidth, communication channels.[120] The technological advances in computer processing

---

113. *See* Otis Port, *Carnegie Mellon: Aiming for Immortality*, BUS. WK., June 23, 1997, at 99 (discussing the falling prices and rising capacities of hard drives).

114. "Bidirectionality" means that information can be transferred in either direction, at equal speeds. Telephones do this well. Both caller and called can speak to each other on equal terms. By contrast, a typical cable network excels in delivering information only downstream, from the cable company's headend to the consumer's television. The upstream frequencies are limited in bandwidth and subject to noise. *See* Andy Reinhardt, *Building the Data Highway*, BYTE MAG., Mar. 1994, at 46, 60. In 1994, estimates of the percentage of cable systems capable of two-way communications ranged from 5-40%. *See id.*

115. "Addressability" means that a communication can be targeted to a specific address. Our telephone system has excellent addressability, since each call can be targeted to a specific phone number. By contrast, direct broadcast satellite TV has a footprint the size of North America. One gets around this problem by scrambling the signals and charging a fee for descrambling.

116. The World Wide Web is "a hypertext-based system for finding and accessing Internet resources." KROL, *supra* note 3, at 515. "Hypertext is a method of presenting information where selected words in the text can be 'expanded' at any time to provide other information about the word. That is, these words are *links* to other documents, which may be text, files, pictures, anything." *Id.* at 288.

117. Applets are small computer programs delivered to the user and launched in the course of browsing a Web page. These programs make the browsing experience more dynamic by providing, for example, animation, demonstrations, or useful utilities.

118. *See* Mark Berniker, *Bells Close Disney Video Services Deal*, BROADCASTING & CABLE, Apr. 24, 1995, at 33 (discussing regional Bell operating companies' plans to deliver Disney programming over video dialtone networks).

119. *See* Don West, *in The Once and Future Cable*, BROADCASTING & CABLE, May 8, 1995, at 32 (interview with Amos Hostetler, Chairman and CEO of Continental Cablevision, discussing plans to expand the applications his company provides).

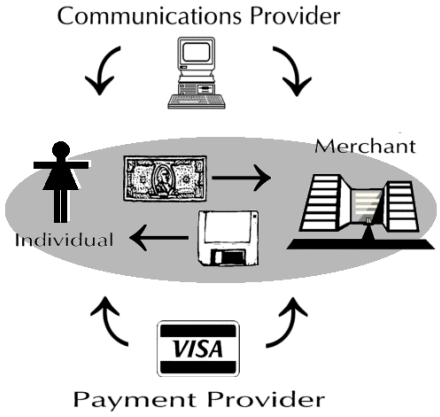
120. For example, telephone and cable companies could team up to provide video programming and local and long-distance telephone services over the same network. *See* John J. Keller & Eben Shapiro, *Time Warner's Cable-TV Unit, AT&T in Talks*, WALL ST. J., May 16, 1995, at A3. Already, long-distance carrier Sprint has formed an alliance with cable television operators Tele-Communications Inc., Comcast Corp., and Cox Communications, Inc. *See* Peter Elstrom, *Sprint's Wireless High-Wire Act*, BUS. WK., Mar. 3, 1997, at 60 (reporting on the delays plaguing this potential alliance). Further, software giant Microsoft is nearing a deal to invest $1 billion in Comcast

and communications that are making this future possible are announced almost daily.

Putting the technological bells and whistles aside, such a network is or will soon be the epitome of convenience. The networked personal computer will become the one-stop information appliance for all types of transactions[121] that now take place in the physical world. These transactions will include the serious, such as news retrieval, research, education, banking, mailing, voting, tax filings, and telemedicine. They will also include the playful, such as shopping, games, movies, music, and socializing. Already, on the current information infrastructure, increasing numbers of people are executing such transactions. As the infrastructure upgrades,[122] and technological literacy explodes, more individuals will employ the new communications technologies to perform more transactions in cyberspace.

B. *Cyberspace's Impact: A Mapping of Information Flows*

From a privacy perspective, the crucial characteristic of cyber-activity is the rich flow of personal information it triggers. The schematic below represents an elementary electronic commerce transaction.



Corp., the nation's sixth largest cable television operator. *See* Mark Landler, *Microsoft Near Deal to Acquire Cable TV Stake*, N.Y. TIMES, June 9, 1997, at A1 (stating that this move would give Microsoft "a crucial foothold in controlling and distributing television programming"). Finally, cable companies and ISPs may join to provide high bandwidth access to the Internet. *See* LELAND L. JOHNSON, TOWARD COMPETITION IN CABLE TELEVISION 46 (1994) (discussing a plan "for several channels of television bandwidth to be dedicated to PSI's Internet customers in several regions").

121. I use the term "transaction" broadly to include all sorts of activities, many of which do not involve monetary payment.

122. "In recent years, U.S. companies have invested more than $50 billion annually in telecommunications infrastructure—and that figure does not account for the vast investments made by firms in related industries, such as computers." Agenda for Action, *supra* note 1, at 49,026-27.

From home, an individual logs into her Internet Service Provider ("ISP")[123] through her computer and modem. She then launches her Web browser. She queries a search engine[124] for the name of a particular software application. After browsing through various merchant home pages, she finds an attractive offer. She selects the specific software package, pays for it by providing a credit card number, and downloads the program and related documentation. This ordinary transaction triggers myriad personal data flows.

1. *Transacting parties.*

First consider the principals to this economic transaction: the individual and the merchant. These transacting parties drive the transaction by exchanging a valuable good, i.e., the software program, for consideration, i.e., money. As a result of this transaction, the merchant has access to all the data that appear on a typical credit card receipt and shipping order.[125] If the merchant requests it, and the individual volunteers it, she may also have the individual's e-mail and physical addresses.[126] Even if such information is not volunteered, the merchant may collect it surreptitiously.

Technical map. When the individual browses a Web page, her computer—the client—provides various fields of information to the merchant's computer—the server. Roughly, these fields reveal some aspect of the client's (1) identity, (2) computer configuration, and (3) browsing activity.

First, the client must provide its own Internet Protocol ("IP") address to any server it contacts.[127] Every computer connected to the Internet is as-

123. Approximately 300 regional and national ISPs allow individuals access to the Internet at various levels. They can provide dedicated access, which may involve leasing a dedicated telephone line and installing an Internet routing computer at the individual's site. They can also provide software that allows individuals to connect their home computers to office, university, or private time-sharing networks that have dedicated access to the Internet. In addition, many on-line services—which principally provide information products and discussion fora to subscribers—offer gateways to communicate via the Internet. The distinction between ISPs and on-line services is dissolving as ISPs gradually provide more information products and as on-line services provide broader access to the Internet. *See* KROL, *supra* note 3, at 456-66 (discussing various methods of obtaining access to the Internet).

124. A search engine is a program that allows keyword searching of a compiled index of material available on the Internet. Popular engines include Yahoo, AltaVista, Excite, and MetaCrawler.

125. This would include: the customer's name and telephone number; the date and time of the purchase; the customer's credit card type, number, and expiration date; the item purchased, including the relevant inventory information listing the name of the software program and the hardware and operating system on which it runs; and the purchase price.

126. In the example, since the product was delivered through cyberspace, a physical mailing address was unnecessary. However, the purchase of a physical object, such as a sweater or a compact disc, would require a delivery address.

127. Each computer on the Internet has a unique IP address, a 32-bit binary number, which consists of a string of 32 ones or zeros. This long binary number, in base 2, can be sectioned off into four bytes, each eight bits long. In turn, each byte can be converted into a number in base 10

signed such an address, either temporarily or permanently. The Internet is a packet-switched[128] network of networks; information is broken down into packets, addressed, and fired off through the network to find its ultimate destination. In order for two computers on the Internet to communicate, each must know the other's IP address.[129] Since an IP address is hard to remember—my host computer's IP address is 149.142.28.67—it is mapped to a more memorable domain name—my host computer's domain name is "kang.law.ucla.edu"[130]—pursuant to the Domain Name System ("DNS").[131] By convention, a server logs the IP address of each client that browses its site. From the IP address, a server can determine the domain name, if any, by performing a reverse look-up through the DNS.[132] Next, from the right portion of the domain name—in my case, the two right-most portions—the server can retrieve the name, physical location (e.g., country, state, and zip code), and contact persons of the organization that originally registered that name with the DNS.[133] In my case, the server can discover that I am affiliated with UCLA, which is located in Los Angeles, California.[134]

---

ranging from 0-255. Thus, all IP addresses can be represented as #.#.#.#, where each "#" is a number from 0-255. This representation is sometimes called a "dotted quad." The left portion of the IP address indicates the network through which the computer accesses the Internet. The right portion of the address indicates the specific computer. *See* KROL, *supra* note 3, at 24-27.

128. A packet-switched network is best understood in contrast to a circuit-switched network. Traditional local phone calls involve circuit-switching. When one phone connects with another, a circuit is created between the two phones via a switch. The circuit is maintained throughout the duration of the conversation, then torn down when the phones disconnect. By contrast, a packet-switched network divides a communication into packets; it bundles together, through multiplexing, packets from various sources and then fires them off to the destination. No circuit is necessarily built up and maintained during the length of the transmission. Packet-switched networks are more efficient in handling bursty traffic. Whereas circuit-switching uses resources even during long bouts of silence in the communication, packet-switching uses resources only in the course of transmitting the packets.

129. This is not strictly true, given the possibility of using anonymous Web proxies. *See* note 217 *infra*.

130. Each domain name has at least two labels, separated by a period. For example, my domain name, "kang.law.ucla.edu," has four labels: kang; law; ucla; and edu. The domain name proceeds from general to specific, from right to left. Thus, "edu" is a top-level domain name that describes educational units; "ucla" points to the UCLA network; "law" points to the UCLA School of Law's network; and, finally, "kang" points to my particular host computer. Typically, though not necessarily, host computers on the same local area network will share the right portion of their domain names. In other words, my colleagues' computers, which reside on the same network, have the domain name "[lastname].law.ucla.edu."

131. The DNS is a distributed database of IP addresses and domain names, as well as a protocol for building and making use of this database.

132. To try a reverse lookup yourself, see RENAISSANCE INTERNET SERVICES, *Renaissance Internet Sources* (visited July 7, 1997) <http://sh1.ro.com/~mprevost/netutils/netutils.html>.

133. To be more specific, the network registered with the DNS can be searched through a WHOIS application. To try a WHOIS search for yourself, see NATIONAL SCIENCE FOUNDATION & NETWORK SOLUTIONS, INC., *InterNIC* (visited July 7, 1997) <http://rs.internic.net/cgi-bin/whois>.

134. E-mail addresses generally are not disclosed, however. Current versions of popular Web browsers are configured so as not to disclose their e-mail address in the request-header field,

The identity information described so far pertains specifically to the client host computer, and not necessarily to the human individual using the computer. While it is true that in my case, my host computer has a domain name with my true last name "kang," this does not have to be the case. If the computer's domain name were "nomad.law.ucla.edu," then the server would have an IP address, the just mentioned domain name, and information about UCLA, but not any part of the individual's specific identity. There are two other ways, however, that the server may be able to access such information. If the individual had to authenticate herself, i.e., by typing in a unique user identification and password, to enter a restricted Web site, the server will be able to identify the specific individual assigned to that user identification.[135] In addition, if the client is configured in a particular manner—which is now uncommon since it is a security threat—then the server may be able to request the individual's local network login name, which is often some portion of the individual's last name.[136]

The client also discloses to the server which human languages it prefers and to what degree it prefers them.[137] Since so much of the Web is in English, this datum is currently not so telling. But soon the Web will become more multilingual, and more users will set their language-preference options accordingly. This bit of information reveals the user's language abilities and, depending on the language, allows the server to make an intelligent guess about the user's ethnicity.[138]

Second, in addition to the identity information discussed above, the Internet client will disclose some basic information about its computer configuration: the browser (e.g., Netscape Navigator or Microsoft Internet Explorer), the operating system (e.g., Mac OS, Windows 3.1, or Windows 95), and the hardware platform (e.g., IBM PC-compatible or Macintosh).[139]

Third, the client will reveal something about its browsing activity. Each client visit to a server is typically logged. In addition to the identity information just described, this log includes: the time and date of visit; the Uni-

---

"from." Moreover, these browsers give individuals the option not to use their e-mail address as the default password when accessing anonymous File Transfer Protocol, which is an Internet convention that has been called into question because of privacy concerns.

135. Authentication involves checking a user identification and password against a list of authorized users. When authenticated, the user identification is typically recorded in the Web server log.

136. More specifically, if both the server and the client are running the "identd" daemon, then the login name may be recorded in the Web server log.

137. This information is available in the "accept-language" variable of the request header.

138. *See* R. Fielding, J. Gettys, J. Mogul, H. Frystyk & T. Berners-Lee, *Hypertext Transfer Protocol—HTTP/1.1, RFC 2068*, at 15.7 (visited Feb. 11, 1998) <http://www.ics.uci.edu/pub/ietf/http/rfc2068.txt> (discussing "Privacy Issues Connected to Accept Headers").

139. This information is available in the "user-agent" variable of the request header.

form Resource Locator ("URL") of the requested resource;[140] the byte length; and the URL of the resource from which the request was made (the "Referer").[141] It bears mention that if I click on a link returned to me by a search engine, the server that I go to—by examining the Referer variable—can determine not only which search engine I used, but also which keywords I used in my query.[142] Finally, a server can track the "clicktrail" of a client—which means it can record which pages a client views—by order, time, and duration. Clicktrails can be maintained in one of two ways. The server can try to match the IP addresses and other identity information in its log to their time-stamps. Or, more easily, the server can set a "cookie."

A cookie is a piece of information sent by the server to the client to store for some time. Its purpose is to store information about the client's state, so as to personalize the browsing experience. For example, various Web servers provide movie listings by zip code. Because it is inefficient to require the user to reenter her zip code at each visit, the server saves the zip code and other "state information" on the client's hard drive in the form of a cookie. Thereafter, by accessing the cookie, the server can automatically present local movie features without querying the user for her location. Many personalized news services operate this way. One's preferences—for example, sports scores in Chicago or the weather in Boston—can be saved in a cookie.[143]

Recently, there has been great public anxiety that cookies can be freely accessed by all Web servers we contact, thereby disclosing details about our browsing history. This fear is somewhat overblown: A client does not serve up cookies simply to anyone who asks. In other words, not all servers have access to all cookies. Each cookie, when initially set, circumscribes the

---

140. For example, the URL for my faculty home page is <http://www.law.ucla.edu/faculty/kang>. "Http" is the transmission protocol; "www.law.ucla.edu" is the server name; "faculty/kang" is the path name; and the unstated but default resource or file-name is "index.htm."

141. In other words, if I am browsing a page with the URL http://www.harvard.edu/test1.htm and click on a hypertext link on that page that takes me to http://www.ucla.edu/test2.htm, the www.ucla.edu server would be provided the Harvard URL in the request-header variable, "referer." However, if I go to a page simply by typing the URL into the browser rather than clicking on a hyperlink, the referer variable is blank. *See generally* Glenn Fleishman, *Web Log Analysis Who's Doing What, When* (visited Feb. 10, 1998) <http://www.junkbusters.com/cgi-bin/privacy>; Lincoln D. Stein, *The World Wide Web Security FAQ: Server Logs and Privacy* (visited Nov. 5, 1997) <http://www.genome.wi.mit.edu/WWW/faqs/wwwsf6.html> ("Q51: What information do readers reveal that they might want to keep private?").

142. When most search engines provide search results, the URL of the search-result page includes the keywords that were entered by the user. This long URL is stored in the referer variable and made available to the server.

143. Another popular use of cookies is to maintain a virtual shopping cart. As one browses a Web site and adds items to a cart, those items are recorded on the client's hard drive as cookies. When the shopper checks out, the server reads the cookies to know which items have been selected for purchase.

range of servers to whom the cookie may be subsequently given. The default range is the domain name of the server that initially set the cookie itself.[144] So, if the server hollywood.movienews.com set a cookie identifying my zip code as 90210 and did not specify a domain name range in the cookie, then, by default, the cookie would be presented only to hollywood.movienews.com in the future. While it is true that hollywood.movienews.com could have set the domain range to a larger set of servers, by setting the domain name range to the tail portion of its name, i.e., movienews.com,[145] it could not have set the range to an entirely different domain name, say, blockbuster.com.[146] Reciprocally, the client will only disclose a cookie to a server if the domain name range for the cookie "tail-matches" the server's domain name. In other words, a cookie with the domain name range movienews.com will not be disclosed to any server that has the tail of blockbuster.com. As a result, cookies can usually be read only by those entities that wrote the cookie in the first place.[147]

That said, there is nothing to keep companies like movienews.com and blockbuster.com from sharing with each other the browsing history of a given individual recorded through their respective cookies. In effect, this is what is done by various Internet advertising companies that target advertisement banners to individuals based on their browsing profile.[148] These advertising companies establish relationships with numerous Web servers. Whenever a client browses one of these Web pages, the client is fed an in-line image that invisibly connects it to the advertising company's server without the individual user's explicit knowledge or command. Once connected, the ad-

---

144. *See* NETSCAPE, *Persistent Client State: HTTP Cookies* (visited Nov. 5, 1997) <http://www.netscape.com/newsref/std/cookie_spec.html> ("The default value of *domain* is the host name of the server which generated the cookie response.").

145. This would allow other servers, such as boston.movienews.com, access to the cookie because the tail of the server's name, movienews.com, matches the set domain range. According to Netscape, the following two tails match: acme.com and shipping.crate.acme.com. *See id.* But under a new proposed standard for cookies, acme.com would only tailmatch crate.acme.com or any other name in which "crate" is replaced by a single label (i.e., a phrase without any periods). *See* D. Kristol & L. Montulli, *HTTP State Management Mechanism, RFC 2109* (last modified Feb. 1997) <http://ds.internic.net/rfc/rfc2109.txt>; E-mail from David Kristol to Jerry Kang, July 8, 1997 (on file with the *Stanford Law Review*).

146. Here, the details are important. To be more specific, the client will accept a domain range if and only if (1) the domain range has "at least two or three periods in them to prevent domains of the form: '.com', '.edu', and 'va.us'," and (2) the server's domain name hollywood.movienews.com, is within the specified domain range, movienews.com. *See Persistent Client State*, *supra* note 144.

147. This is not strictly true because, as explained in note 145 *supra*, the server boston.movienews.com could read a cookie set by hollywood.movienews.com with the domain name range movienews.com. There is no necessary reason why the servers boston.movienews.com and hollywood.movienews.com must be owned by the same corporate entity.

148. These companies include DoubleClick, Clickstream, and I/Pro. *See, e.g.*, DOUBLECLICK, INC., *Benefits* (visited Nov. 5, 1997) <http://www.doubleclick.net/nf/benefset.htm>; CLICKSTREAM, INC., *Web Site FAQ* (visited Apr. 21, 1998) <http://www.click-stream.com/webfaq.html>.

vertiser retrieves the identity information described above. On the one hand, if the client's IP address or domain name has not been seen before, the advertiser creates a unique identification number and saves it in a cookie on the client's hard drive. On the other hand, if the IP address/domain name has been seen already, then the advertiser accesses the previously set cookie, which contains a unique identification number, and updates the extant database record indexed by that number with the browsing activity of the client. Based on this database of browsing activity collected from all affiliated Web sites, the advertiser delivers a targeted ad banner. These transactions occur within a fraction of a second.[149]

To summarize, a client's browsing behavior at a particular site can be tracked with detail. Through, for instance, the use of cookies, this tracking can continue over multiple visits, over an indefinite period of time, with all browsing information compiled into a database. This does not mean, however, that any other site has automatic access to this information—with the following critical exception: Sites may be linked together through a data sharing relationship, the most prominent of which is affiliation with a common advertiser.

These three types of disclosures—identity, computer configuration, and browsing activity—are not software bugs or security loopholes that will be corrected momentarily.[150] Rather, they are the standard, albeit unpopular,[151] elements of the Web browsing process.[152] Further, these personal informa-

---

149. DoubleClick claims that this entire process takes 20 milliseconds. *See generally Benefits*, *supra* note 148.

150. *See generally* Lincoln D. Stein, *The World Wide Web Security FAQ: Client Side Security* (visited June 9, 1997) <http://www.genome.wi.mit.edu/WWW/faqs/wwwsf7.html> (listing bugs in various Internet applications).

151. As stated in the *GVU Seventh Study*:

> As with the Sixth Survey, three out of four users agree that sites ought to be able to record the page that is requested (74.27% Seventh vs. 76.60% Sixth) and the time of the page request (70.95% Seventh vs. 74.42% Sixth). Under half (43.98% Seventh vs. 43.71% Sixth) feel that the browser that users are using ought to be collected. The machine name/address (28.04% Seventh vs. 27.00% Sixth), the operating system the user operates (28.33 Seventh vs. 26.83% Sixth), the user's email address (19.56% Seventh vs. 21.03% Sixth), and the location of the user (18.36% Seventh vs. 19.70% Sixth) are not high on people's list either. It is interesting to note that most users of the WWW can reliably gather all of the above information except email and location for every page request.
>
> When asked about an identifier that would uniquely label users across sessions at a site, only one out of every five (20.75% Seventh vs. 19.08% Sixth) thought this should be possible.

GVU Seventh Study, *supra* note 12.

152. At least for now. The use of cookies may be changed radically if a new proposed standard is adopted. Under this new standard, when a client browses a server, that server could not create a connection invisibly between the client and a third party, such as an advertiser, without the client's consent. *See* Kristol & Montulli, *supra* note 145. Indeed, many browsers already allow greater individual control over the setting of cookies. For instance, Netscape's Navigator 4.0 allows

tion flows can be leveraged to produce additional information, often cheaply and rapidly, through cyberspace. For example, an e-mail address or domain name may be reverse-indexed, using national computerized White Pages, to find, in many cases, the individual's name, telephone number, and physical address. Even unlisted information can sometimes be located through the use of national lookup databases.[153]

Legal map. The collection of personal information in America by transacting parties is largely unregulated by law. Unlike certain European nations,[154] the United States has no omnibus privacy law covering the private sector's processing of personal information. Instead, American law features a patchwork of rules that regulate different types of personal information in different ways, depending on how it is acquired, by whom, and how it will be used. Since others have canvassed the positive law extensively,[155] my comments are summary.

To set the stage, federal constitutional law provides no protection of an individual's information privacy from invasion by the private sector—first, because of the state action doctrine,[156] and second, because it is unclear to what extent the Constitution actually protects information privacy.[157] The

---

one to set preferences to accept all cookies, reject all cookies, or accept only cookies that return to the originating server and warn the individual whenever cookies are set.

153. *See, e.g.*, DATABASE AMERICA COMPANIES, INC., *People Finder* (visited July 7, 1997) <http://www.databaseamerica.com/html/gpfind.htm> (including also a reverse index from telephone number to street address). I have personally used this Web site to locate a Louisiana attorney's unlisted home phone number.

154. *See* SCHWARTZ & REIDENBERG, *supra* note 18, at 5-17 (discussing the general differences between the American and European approaches); *see also* Paul M. Schwartz, *European Data Protection Law and Restrictions on International Data Flows*, 80 IOWA L. REV. 471, 473-88 (1995) (discussing the Council of Europe Convention and the European Union Directive on data protection). For an extensive discussion of the data protection directive, see Peter P. Swire & Robert E. Litan, *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive* (visited Jan. 24, 1997) <http://www.acs.ohio-state.edu/units/law/swire1/noyb.htm>; *see also* text accompanying note 331 *infra* (claiming that my proposed Cyberspace Privacy Act might ease transborder data flows from the European Union to the United States).

155. *See* ROBERT ALDRICH, PRIVACY PROTECTION LAW IN THE UNITED STATES, NTIA REPORT 82-98 (1982) (discussing the major characteristics of privacy law). *See generally* WAYNE MADSEN, HANDBOOK OF PERSONAL DATA PROTECTION (1992) (comparing international regimes); SCHWARTZ & REIDENBERG, *supra* note 18; ROBERT ELLIS SMITH, COMPILATION OF STATE & FEDERAL PRIVACY LAWS (1992).

156. With rare exceptions, the Constitution applies only to actions attributable to the state. *See* SCHWARTZ & REIDENBERG, *supra* note 18, at 32-36 (summarizing cases and discussing the state action doctrine and the concept of negative rights as they relate to private sector data collection).

157. A right to information privacy has not been clearly established as a matter of federal constitutional law. The closest the Court has come to finding such a right was in *Whalen v. Roe*, 429 U.S. 589 (1977). In *Whalen*, the State of New York enacted a recordkeeping statute to fight prescription drug abuse. Plaintiffs, concerned about information privacy, sued under a constitutional theory of invasion of privacy. The Court avoided deciding whether a definitive right to information privacy exists under the U.S. Constitution. In its most explicit passage, the majority

state action doctrine similarly defangs state constitutional protections of information privacy where they exist.[158] Further, the common law tort of invasion of privacy has thus far provided no effective constraints on the sort of information flows depicted above.[159] Finally, general omnibus privacy stat-

---

suggested that a governmental duty "to avoid unwarranted disclosures" of personal information may "in some circumstances . . . [have] its roots in the Constitution." *Id.* at 60. *Compare id.* at 607 (Brennan, J., concurring) (stating that the Fourth Amendment places limits on both the "type of information the State may gather . . . [and] the means it may use to gather it"), *with id.* at 609 (Stewart, J., concurring) (stating that there is no constitutionally protected "interest in freedom from disclosure of private information"). Perhaps what the Court did is more instructive than what the Court said. In *Whalen*, the Court affirmed the constitutionality of the New York statute after conducting a balancing test—weighing the possible harm to individuals, given the sensitivity of the information and its security, against the societal benefit of the recordkeeping statute. Notably, the Court did not simply rubber-stamp the statute under a rational-basis, due process scrutiny.

The Court continued this trend *in Nixon v. Administrator of Gen. Servs.*, 433 U.S. 425 (1977), in which the Court approved of *Whalen*'s balancing test. So it seems that information privacy is, in practice, granted limited constitutional protection in the form of a weak balancing test that is slightly more rigorous than mere rationality review. *See also* Barry v. City of New York, 712 F.2d 1554 (2d Cir. 1983) (holding that a city-enacted financial disclosure law did not infringe on a public employee's constitutional rights); United States v. Westinghouse Elec. Corp., 638 F.2d 570 (3d Cir. 1980) (concluding that minimal intrusion into the privacy of an employee's medical records is justified by the public interest in research); Plante v. Gonzalez, 575 F.2d 1119 (5th Cir. 1978) (finding that the public's "right to know" justifies mandated public disclosure of a state senators' financial statements). *But see* J.P. v. DeSanti, 653 F.2d 1080 (6th Cir. 1981) (finding no separate information privacy right and arguing that such a right exists solely to the extent that it is alloyed with decisional privacy). For further discussion, see Francis S. Chlapowski, Note, *The Constitutional Protection of Informational Privacy*, 71 B.U. L. REV. 133, 145-50 (1991), and Glenn Chatmas Smith, *We've Got Your Number! (Is It Constitutional to Give It Out?): Caller Identification Technology and the Right to Informational Privacy*, 37 UCLA L. REV. 145, 175 (1989).

158. Some state constitutions protect information privacy against intrusion by private actors. An oft-cited example is California. *See* Hill v. NCAA, 865 P.2d 633 (Cal. 1994). California's constitutional provision, however, requires an invasion "sufficiently serious . . . to constitute an egregious breach of the social norms underlying the privacy right." *Id.* at 655. It therefore protects privacy little more than the common law tort of invasion of privacy, which has been largely ineffective. *See* note 159 *infra.*

159. As argued by Prosser and codified in the Restatement, the privacy tort gathers four separate torts under one title: intrusion upon one's seclusion; misappropriation of one's name or likeness; public disclosure of private facts; and publicity that places one in a false light. *See* RESTATEMENT (SECOND) OF TORTS § 652A (1977). For various reasons, which I will not repeat, these four torts provide little privacy protection against private sector use of personal information. *See* MILLER, *supra* note 17, at 173-85 (outlining why these tort categories are not particularly effective in protecting the privacy of computer data); Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 GEO. L.J. 2381, 2388 (1996) ("[T]he tort of invasion of privacy is probably best described as alive, but on life support."); Joel R. Reidenberg, *Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?*, 44 FED. COMM. L.J. 195, 221-26 (1991) (discussing the four categories of privacy rights in the context of data processing); George B. Trubow, *Protecting Informational Privacy in the Information Society*, 10 N. ILL. U. L. REV. 521, 531-41 (1990) (examining issues of privacy in the private sector); Diane L. Zimmerman, *Requiem for a Heavyweight: A Farewell to Warren and Brandeis's Privacy Tort*, 68 CORNELL L. REV. 291, 292-93 (1983) ("[D]espite the ever-increasing number of claims under the Warren-Brandeis theory, plaintiffs rarely win.").

utes, such as the federal Privacy Act and its state analogues,[160] fail because they apply only to government action.[161]

There are, however, numerous statutes that govern specific sectors of personal information, such as consumer credit,[162] education,[163] cable programming,[164] electronic communications,[165] videotape rentals,[166] and motor vehicle records.[167] But it turns out that none of these statutes substantially constrains a transacting party from collecting the information identified above. More detailed analyses of specific statutes are provided where relevant.

2. *Transaction facilitators.*

Now let us focus on the category of players I call transaction facilitators, those who help execute the transaction but are not the principal drivers of the exchange. In this example, the telephone company, ISP, and credit card company are all transaction facilitators, which help to consummate the deal between the principal parties: the individual and the merchant. The two most common types of transaction facilitators are communications providers, which provide the channel through which the individual and merchant communicate, and payment providers, which arrange payment between the transacting parties. In this example, the telephone company and the ISP carry the communications, and the credit card company arranges for payment.

---

160. According to Schwartz and Reidenberg, only 13 states have passed analogues to the federal Privacy Act, Pub. L. No. 93-579, 88 Stat. 1896, 5 U.S.C. § 552(a) (1994). *See* SCHWARTZ & REIDENBERG, *supra* note 18, at 131.

161. The Privacy Act governs federal agencies' acquisition, disclosure, and use of personal information. *See* OFFICE OF INFORMATION AND PRIVACY, U.S. DEP'T OF JUSTICE, FREEDOM OF INFORMATION ACT GUIDE & PRIVACY ACT OVERVIEW 459 (1994).

162. *See* Fair Credit Reporting Act of 1970, 15 U.S.C. § 1681 (1988); Equal Credit Opportunity Act of 1975, 15 U.S.C. § 1691 (1988 & Supp. V 1993).

163. *See* Family Educational Rights and Privacy Act of 1974, 20 U.S.C. §§ 1221 note, 1232g (1988 & Supp. V 1993).

164. *See* Cable Communications Policy Act of 1984, 47 U.S.C. § 551 (1988 & Supp. V 1993).

165. *See* Electronic Communications Privacy Act of 1986 ("ECPA"), 18 U.S.C §§ 2510-2522, 2701-2709 (1988 & Supp. V 1994).

166. *See* Video Privacy Protection Act of 1988, 18 U.S.C. §§ 2710-2711 (1994). The VPPA prohibits video tape service providers from knowingly disclosing personal information, such as titles of video cassettes rented or purchased, without the individual's written consent. *See id.* § 2710(b)(1). The VPPA likely does not apply to firms that provide video-like content through telecommunications networks because they are not "video tape service providers" within the meaning of the statute. *See* NTIA WHITEPAPER, *supra* note 11.

167. *See* Driver's Privacy Protection Act of 1994, 18 U.S.C. §§ 2721-2725 (Supp. V 1994). The DPPA prohibits the knowing disclosure of personal information from a motor vehicle record, unless such disclosure fits within one of numerous exception. *See id.* § 2721(a). The DPPA also restricts resale and redisclosure of motor vehicle data to the terms under which the data was initially made available by the state motor vehicle department. *See id.* § 2721(c).

Communications providers—Technical map. Communications providers, e.g., the telephone company and ISP, collect subscription data when an individual signs up for their services.[168] More specific to the software purchase, the communications providers have access to certain kinds of transactional data, such as routing information used to connect the individual and the merchant over the network. For example, the telephone company maintains, if temporarily, calling records identifying the originating number—the individual—destination number—the ISP—and, possibly, the time and length of the call. The ISP, on the other hand, will likely keep logs that identify the individual user, the remote computer contacted—in this case, the merchant's Web server—and the date and time of contact. Depending on the technological set-up, the ISP may also have transactional data of files uploaded or downloaded, and e-mail messages sent and received.[169]

The above example assumes that the individual accessed cyberspace through a home connection, but individuals often jack into cyberspace through equipment provided by their employers. In this regard, employers thus may function as a sort of communication provider, by footing the bill for cyberspace access. In exchange for providing that access, employers often feel entitled to collect information about their employees' use of cyberspace. For example, many employers reserve and exercise the right to read their employees' e-mail.[170] Employers also use various software and network management tools to track employee cyber-activity, such as the Web sites visited and files downloaded.[171]

Communications providers—Legal map. Communications providers, as all persons, must abide by the Electronic Communications Privacy Act of 1986 ("ECPA").[172] The rough logic of the grossly complicated ECPA is to

---

168. This data might include: the customer's name; the customer's mailing address; the credit card type, number, and expiration date (for automatic monthly billing by the ISP); and the telephony and computer hardware/software configurations.

169. *See, e.g.*, *Man Accused of Getting Child Porn from Internet*, AP, Aug. 13, 1997, *available in* 1997 WL 4879262 (describing the arrest of a person for possession of child pornography after a tip from the person's ISP). For a review of the privacy policies of the four major on-line services, see CENTER FOR DEMOCRACY AND TECH., *Privacy Policy Chart—Online Service Providers* (visited Nov. 5, 1997) <http://www.cdt.org/privacy/online_services/chart.html>; *see also* CNET, INC., *Privacy Policies of Online Services* (visited Nov. 5, 1997) <http://www.cnet.com/Content/Features/Dlife/Privacy/ss01c.html> (summarizing the privacy policies of three ISPs).

170. One study concluded that 36% of firms surveyed look at employee e-mail. *See* CNET, INC., *Who's Watching You?* (visited Nov. 5, 1997) <http://www.cnet.com/Content/Features/Dlife/Privacy/ss01.html> (observing that "digital technologies . . . enable supervisors to monitor employees"). *See generally* Larry O. Natt Gantt II, *An Affront to Human Dignity: Electronic Mail Monitoring in the Private Sector Workplace*, 8 HARV. J.L. & TECH. 345 (1995) (discussing various theories of liability for employer e-mail surveillance).

171. *See, e.g.*, SEQUEL TECHNOLOGY, *Sequel Net Access Manager Data Sheet* (visited June 9, 1997) <http://www.sequeltech.com/product/snam/sheet.htm>.

172. *See* Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510-2522, 2701-2709, 3121-3126 (1988 & Supp. V 1994).

break down electronic communications into two temporal periods, one during transmission and the other during storage. Title I governs the former;[173] Title II governs the latter.[174] During transmission, the ECPA proscribes the interception[175] of an electronic communication and the subsequent disclosure[176] and use[177] of its contents. But the handling of an electronic communication by a communications provider, in the ordinary course of business, does not constitute an "interception."[178] Similarly, the ECPA proscribes the "unauthorized access"[179] of an electronic communication while in storage in an electronic communication service facility. But again, access approved by the electronic communications provider is not deemed "unauthorized."[180]

The ECPA also has specific confidentiality rules for communication providers that serve the general public. These providers cannot divulge the contents of the communications during transmission[181] or while in storage.[182] Although this may seem to bar communication providers from peddling personal information in the marketplace, such privacy protections are illusory. The above bar applies solely to the contents of communications, not to transactional records, which may be freely disclosed to anyone "other than a governmental entity."[183]

---

173. Title I updated the general antiwiretapping statute, Title III of the Omnibus Crime Control & Safe Streets Act, to include electronic communications. *See* Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended at 18 U.S.C. § 2510-2522 (1988 & Supp. V 1994)).

174. *See* Pub. L. No. 99-508, 100 Stat. 1860 (1986) (codified as amended at 18 U.S.C. §§ 2701-2710 (1988 & Supp. V 1994)). The ECPA contains a third title, which addresses the use of pen registers—recording the numbers of outgoing calls—and trap-and-trace devices—recording the numbers of incoming calls. *See* Pub. L. No. 99-508, 100 Stat. 1868 (1986) (codified as amended at 18 U.S.C. §§ 3121-3126 (1988 & Supp. V 1994)).

175. *See* 18 U.S.C. § 2511(1).

176. *See id.* § 2511(1)(c).

177. *See id.* § 2511(1)(d).

178. "Interception" of an electronic communication requires the use of an "electronic, mechanical, or other device." *Id.* § 2510(4). This provision excludes equipment employed by the individual user or the communications provider in the ordinary course of business. *See id.* § 2510(5)(a). The standard maintenance of transaction logs by communications providers would likely fall within this exclusion. In addition, there is a broad communications-provider exception. This exception permits the interception, subsequent disclosure, and use of electronic communications when it is a "necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service." *Id.* § 2511(2)(a)(i).

179. *See id.* § 2701(a).

180. *See id.* § 2701(c)(1).

181. *See id.* § 2511(3). Unlike section 2511(1), this section does not turn upon whether the communication is "intercepted."

182. *See id.* § 2702(a)(i). Disclosure, however, is permitted when it is "necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service." *Id.* § 2702(b)(5); *see also* § 2702(b)(2) (incorporating the section 2511(2)(a) exception). The disclosure of communications during transmission is governed by section 2511(3)(b)(i) (incorporating the section 2511(2)(a) exception).

183. *Id.* § 2703(c)(1)(A). The rationale for disparate treatment is that content poses a greater privacy risk than transactional records. The Supreme Court offered this explanation when it de-

Unfortunately, the line is not bright between the contents of a communication and the transactional data about that communication. According to the ECPA, content "includes any information concerning the substance, purport, or meaning of that communication,"[184] whereas transactional records are implicitly defined as "a record or other information pertaining to a subscriber to or customer of such [electronic communication] service."[185] The legislative history adds little light, except to make clear that "contents" do not include "the identity of the parties or the existence of the communication."[186] The upshot of this analysis is that the ECPA constrains a communication provider's exploitation of personal information in only limited ways. Although electronic communications providers to the public must keep the contents of communications confidential, they have almost[187] no such obligation regarding transactional records.[188]

---

cided that law enforcement's seizure of telephone toll records did not constitute a search under the Fourth Amendment because toll—i.e., transactional—records are not on par with the content of the telephone conversation. *See* Smith v. Maryland, 442 U.S. 735, 741-44 (1979). Justice Stewart, dissenting, argued that transactional telephone records should be afforded the same protection as the telephone conversations themselves:

> The numbers dialed from a private telephone—although certainly more prosaic than the conversation itself—are not without "content." Most private telephone subscribers may have their own numbers listed in a publicly distributed directory, but I doubt there are any who would be happy to have broadcast to the world a list of the local or long distance numbers they have called. This is not because such a list might in some sense be incriminating, but because it easily could reveal the identities of the persons and the places called, and thus reveal the most intimate details of a person's life.

Id. at 748 (Stewart, J., dissenting).

184. 18 U.S.C. § 2510(8).

185. *Id.* § 2703(c)(1)(A).

186. S. REP. NO. 99-541, at 13 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3567. The ECPA "thus distinguishes between the substance, purport or meaning of the communication and the existence of the communication or transactional records about it." *Id.* For an argument that "contents" should be read broadly, see NTIA WHITEPAPER, *supra* note 19, at 18 & n.77.

187. I say "almost" because of the Telecommunications Act of 1996 protection of Customer Proprietary Network Information ("CPNI"). CPNI is defined as

> (A) information that relates to the quantity, technical configuration, type, destination, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier[,]

but it excludes White Pages information. 47 U.S.C. § 222(f)(1). Subject to various exceptions, a telecommunications carrier "shall only use, disclose, or permit access to individually identifiable customer proprietary network information in its provision of (A) the telecommunications service from which such information is derived, or (B) services necessary to, or used in, the provision of such telecommunications service, including the publishing of directories." *Id.* § 222 (c)(1).

188. Finally, the robust privacy protections of the 1984 Cable Act only apply to cable systems, which is a small subset of our national information infrastructure. *See* Cable Communications Policy Act of 1984, 47 U.S.C. § 522(7) (Supp. V 1994). It is even questionable whether the Act would apply to advanced interactive communications networks built out of the current cable television infrastructure. The privacy provisions of the Act apply only to "cable service," which is defined as video programming similar to current television broadcasts. *See id.* § 522(6)(A)(B).

Payment providers—Technical map. Another sort of transaction facilitator is the payment provider, which, in this example, is the credit card company.[189] As with the communication providers, the credit card company collects subscription data—in this case through a credit card application. For any specific purchase, the company would have the transactional data that appear on monthly billing statements: merchant name, city, and state; date of purchase; and amount of purchase.

Payment providers—Legal map. As to credit providers, an important federal law that may appear relevant is the Fair Credit Reporting Act ("FCRA").[190] Unfortunately, the FCRA does not effectively constrain what these payment providers can do with the data that they have collected. The FCRA attempts to maintain the confidentiality and quality of "consumer reports," which are defined as any communication by a "consumer reporting agency" regarding "a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living"[191] that is used for credit, insurance, employment, or other "legitimate business need."[192]

The privacy rules of the FCRA are not likely to apply to payment providers because the data that they collect and subsequently disclose to others do not constitute "consumer reports" within the meaning of the Act. First, the payment providers are not themselves consumer reporting agencies, because they do not regularly engage "in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties."[193] Second, the definition of "consumer report" explicitly excludes "any report containing information solely as to transactions or experiences between the consumer and the person making the report."[194] Finally, even if these definitional hurdles were cleared, courts have read the term "legitimate business

---

Limited subscriber interaction is included in the definition of "cable service," but only to the extent of selecting video programming from a menu typical of pay-per-view. Truly interactive multimedia services may not be considered "cable services" because they involve a qualitatively higher level of subscriber interactivity than today's one-way video programming.

189. In addition to credit cards, some payment providers issue debit cards, which immediately subtract the amount spent at the time of purchase from the holder's bank account. Anonymous electronic cash systems are also being developed. *See* RAVI KALAKOTA & ANDREW B. WHINSTON, FRONTIERS OF ELECTRONIC COMMERCE 296-331 (1996) (discussing various types of electronic payment systems); Konvisser, *supra* note 6, at 326-30 (discussing the benefits of electronic cash and describing a proposed system of "E-Cash"); *see also* notes 222-223 *infra* and accompanying text.

190. Fair Credit Reporting Act of 1970, 15 U.S.C. §§ 1681-1681(u) (1994).

191. *Id.* § 1681a(d).

192. *Id.* § 1681b(3)(E).

193. *Id.* § 1681a(f).

194. *Id.* § 1618a(d)(3)(A).

need" so broadly that the practice of exchanging credit reports could be justified by any number of reasons, including database marketing.[195]

* * *

I offered the software purchase example to suggest a generic architecture with which to conceptualize transactions—an architecture that divides participants into transacting parties and transaction facilitators. This framework does not provide a model for all current transactions. For example, many cyberspace transactions are not so "commercial": In many Web browsing transactions, neither server nor client is exchanging information to turn a profit, and no payment provider is involved. Think of the many Web sites we browse to gather news, financial reports, humor, and scholarship—all without payment. Further, this architecture cannot model all future cyberspace transactions; their diversity defies prediction. For example, there may be numerous transacting parties in complex, multilateral deals. There may be other types of transaction facilitators, such as time-stamp authorities,[196] certification authorities,[197] anonymous remailers,[198] and electronic malls that handle accounting, shipping, and inventory for their merchandisers. Indeed, some of these facilitators may operate without ongoing human intervention; rather, they may be pieces of advanced software or "intelligent agents."[199] To complicate matters further, the distinction between transaction facilitators and transacting parties—already hazy in many cases—may dissolve further as merchandisers, communications providers, and payment providers vertically integrate. Nevertheless, the architecture provides a useful vocabulary,

---

195. *See* Gandy, *supra* note 79, at 80-82 (discussing the breadth of the "business interest" and whether it is always legitimate).

196. A time-stamp authentication is the cyber-analogue to a certified mail receipt.

197. A certification authority is required to produce a secure communications environment through public key cryptography. In brief, a secure commerce environment requires: confidentiality—e.g., that no unauthorized party can intercept the credit card number or software transmission; authentication—e.g., that no third party can impersonate the merchant; and integrity—e.g., that the communication has not been altered in any way through the transmission. Public key encryption, a technology based on a field of mathematics called cryptography, makes all three requirements possible in cyberspace. *See* text accompanying notes 214-223 *infra.* However, to provide authentication—to make sure that the merchant is who it claims to be—a trusted third party called a "certification authority" must vouch for the merchant's identity. Various certification authorities are already in operation. For example, Netscape has a subsidiary that acts as a certification authority. It certifies to the consumer that she is, in fact, communicating with her intended merchant. Most certification authorities verify only the merchant's identity, not the consumer's; thus, they collect no personal information on the consumer. Certification authorities should be a powerful force against Internet fraud. *See Internet: Novel Forms of Traditional Fraud Emerging on Internet, Study Shows*, DAILY REP. FOR EXECUTIVES (BNA), May 5, 1997, at A-6 (detailing numerous forms of Internet fraud and emphasizing the importance of authentication services).

198. *See* text accompanying notes 217-219 *infra*.

199. One could say that the current Web search engines are primitive precursors of these future agents.

one that connotes the magnitude and complexity of personal information triggered by quotidian cyberspace transactions.

C. *Data Mining*

As cyberspace becomes the preferred medium to complete the day's innumerable tasks, it will generate for each individual a mother lode of personal information, recorded dutifully—and often invisibly—by computers that know no sleep. These tasks include not only the sort of cyber-commerce that my software purchase example illustrates. They also include the plain old reading, e.g., for research, entertainment, or current awareness, of the Web pages we browse. They include each and every communication we have with friends, colleagues, organizations, and governmental agencies. They include interactions with pharmacists, financial institutions, and political parties. This mother lode of personal information will be mined for all its value.[200] The postindustrial economy generally and the telecommunications sectors particularly are seeing increased competition. This will prompt firms to exploit every competitive advantage, including the use of personal information.

For instance, firms may create entirely new revenue generating services from the manipulation of personal information, such as Caller ID.[201] Or firms may collect and process personal information to insure that they receive full payment for the consumption of copyrighted goods.[202] Or, less creatively, firms may find marketing uses for personal information, as they enter lines of business previously forbidden.[203] For example, most LECs currently use customer toll records only to route calls and bill customers. But as LECs begin to enter the long-distance market, as the Telecommunications Act of 1996 allows,[204] they will face increased incentives to use this toll record information for marketing their own long-distance services.[205]

---

200. For primers on consumer profiling, see Gandy, *supra* note 18, at 60-94, and A. Michael Froomkin, *Regulation and Computing and Information Technology: Flood Control on the Information Ocean: Living with Anonymity, Digital Cash, and Distributed Databases*, 15 J.L. & COM. 395, 482-88 (1996).

201. Caller ID is a technology that displays the telephone number of the incoming caller.

202. *See* Cohen, *supra* note 42, at 983-85.

203. *See* NTIA WHITEPAPER, *supra* note 19, at 10 (noting that market deregulation is a force that is "dissolving traditional distinctions between communications providers").

204. *See* Thomas G. Krattenmaker, *The Telecommunications Act of 1996*, 49 FED. COMM. L.J. 1, 18-21 (1996) (discussing the motivations behind and provisions of the 1996 Telecommunications Act).

205. Here is another example: Since the LECs know the telephone numbers assigned to the ISPs, they can determine which of their customers access the Internet from their homes. LEC-affiliated ISPs can then use this information to target these potential Internet customers. Long-distance carriers can also determine where and how often their customers travel by examining calling card records. They can then sell this information to other businesses. *See* ERIK LARSON, THE

The consumption preferences and behavioral patterns of individuals—as revealed by cyber-activity—will be widely used for database marketing.[206] This form of marketing is premised on the fact that the more information one has about a potential consumer, the easier it is to target advertisements for products and services to that person. A sophisticated database marketing initiative thus acquires as much data on potential customers as legally possible.[207] Through database marketing, firms can now generate surprisingly detailed personal profiles.[208] When such data are overlaid onto specific transactional data generated by cyberspace transactions—what we read, what

---

NAKED CONSUMER: HOW OUR PRIVATE LIVES BECOME PUBLIC COMMODITIES 7 (1992) (explaining how Sprint sold a list of frequent travelers to hotel companies and airlines).

206. *See generally* Kathleen A. Linert, Note, *Database Marketing and Personal Privacy in the Information Age*, 18 SUFFOLK TRANSNAT'L L. REV. 687 (1995). According to Ann Branscomb, "the average person is on a hundred mailing lists and at least fifty databases." BRANSCOMB, *supra* note 21, at 11. According to one study, the total revenues for the data-mining market will hit $8.4 billion by the year 2000. *See* Joy Russell, *Data-Mining Dollars Expected to Skyrocket*, InternetWEEK (Nov. 4, 1997) <http://www.techweb.com/se/directlink.cgi?INV1997110404>.

207. Sometimes, data are obtained from the firm's own dealings with the individual. Other data are obtained from public records, which cyberspace makes more accessible. *See generally* VINCENT PARCO, RESEARCHING PUBLIC RECORDS: HOW TO GET ANYTHING ON ANYBODY (1994). Numerous types of public records are available on the Internet. The California Courts Web site includes recent opinions, court calendars, and judicial rules. *See* JUDICIAL COUNCIL OF CALIFORNIA, *California Courts: The Judicial Branch of California* (visited Nov. 5, 1997) <http://www.courtinfo.ca.gov/>. One can even obtain a complete list of women on Florida's death row. *See* FLORIDA DEPT. OF CORRECTIONS, *Women Who Have Received the Death Penalty in Florida* (visited Jan. 28, 1998) <http://www.dc.state.fl.us/security/womendr.html>.

Still other data come from firms that specialize in providing information about individuals. These firms, called reference services, provide "'one-stop shopping' for anyone looking for information about a person." *See* FEDERAL RESERVE REPORT, *supra* note 84, at 8-9; *see also* LARSON, *supra* note 205, at 60 (alleging that TRW, a credit reporting company, keeps "monthly tabs on 165 million consumers" and recounting Wiland Services' claim that it stores 1000 variables on 215 million individuals in its "ULTRAbase"); JEFFREY ROTHFEDER, PRIVACY FOR SALE: HOW COMPUTERIZATION HAS MADE EVERYONE'S PRIVATE LIFE AN OPEN SECRET 1-78 (1992) (discussing credit bureaus and black markets in data).

208. They contain "name, gender, address, telephone number, age, estimated income, household size and composition, dwelling type, length of residence, car ownership, pet ownership, responsiveness to mail offers, contributor status, credit card ownership, lifestyle, hobbies, interests, and neighborhood characteristics including average education, house value, and racial composition." NTIA WHITEPAPER, *supra* note 19, at A-4; *see also* BRANSCOMB, *supra* note 21, at 3-4 ("A great deal of information we consider to be highly personal . . . is now being sold on the open market to anyone who believes he or she might be able to use such information to turn a profit. These transactions usually take place without our knowledge or consent."); Bernstein, *supra* note 82, at A1 (describing Metromail's data on a litigation opponent as "25 closely printed pages of spreadsheets" listing "her income, marital status, hobbies and ailments . . . whether she had dentures, the brands of antacid tablets she had taken, how often she had used room deodorizers; sleeping aids and hemorrhoid remedies"). For a general discussion of profiling methodology, see generally Roger Clarke, *Profiling: A Hidden Challenge to the Regulation of Data Surveillance*, 4 J.L. & INFO. SCI. 2 (1993).

we view, what we buy, to whom we speak—a rich and telling portrait of the individual is possible.[209]

These portraits have substantial economic value, and developers of advanced interactive networks have already expressed keen interest in wedding database marketing to cyberspace.[210] Moreover, such portraits pose a synergistic threat to privacy—synergistic in that the privacy threat of the profile is greater than the sum of the privacy threats associated with each individual bit of information considered in isolation.[211] In the near future, then, we may witness what Gary Marx has predicted:

> Purchasers of pregnancy-testing kits may receive solicitations from pro- and anti-abortion groups . . . . Purchasers of weight-loss products or participants in diet programs may be targeted for promotional offers from sellers of candy, cookies and ice cream, or, conversely, those whose purchases of the latter exceed the average may receive offers for weight-loss products and services. Subscribers to gay and lesbian publications may be targeted by religious and therapeutic organizations, or face employment denials, harassment, and even blackmail. Frequent travelers and those with multiple residences may receive

---

209. Psychographic profiling expands on mere demographic profiling by adding data about individual attitudes and preferences. *See, e.g.*, Rebecca Piirto Heath, *Psychographics: Qu'est-Ce Que C'est?: Marketing Tools* (visited Feb. 11, 1998) <http://www.demographics.com/publications/mt/95_mt/9511_mt/MT388.htm> ("A psychographic study joins consumers' measurable demographic characteristics with the more abstract aspects of attitudes, opinions and interests."). There are many industry claims that psychographic profiling improves predictive efficiency. According to Affinicast, demographic variables predict only about 3% of an individual's choice of media content. When alloyed with psychographic profiling of media attitudes, collected by asking 15 questions, and lifestyle indicators, collected by asking another 15 questions, predictive efficiency rises to 21.9%. *See* Bruce MacEvoy, *Validation of Affinicast Rating System* (visited Feb.11, 1998) <http://www.affinicast.com:8080/about/validate.html>. In this example, media attitudes and lifestyle indicators were collected through a voluntary survey. But there is every reason to believe that such information could be culled from our cyber-activities.

210. *See* LOUIS HARRIS & ASSOCIATES, INC., INTERACTIVE SERVICES, CONSUMERS, AND PRIVACY: A NATIONAL SURVEY xv (1994).

211. The Supreme Court has not clearly recognized a constitutional right to information privacy. It has, however, acknowledged the privacy threat of detailed personal profiles generated by computers:

> [T]he issue here is whether the compilation of otherwise hard-to-obtain information alters the privacy interest implicated by disclosure of that information. Plainly there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information.

United States Dept. of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 764 (1989). In *Reporters Committee*, the Supreme Court decided whether the release of FBI "rap sheets" constituted an invasion of privacy within the meaning of the privacy exemption of the Freedom of Information Act. *See id.* at 751. The Court recognized the threat to privacy from compilations of public conviction information that would otherwise fade into obscurity. It noted the vast distinction "between scattered disclosure of the bits of information contained in a rap sheet and revelation of the rap sheet as a whole." *Reporters Committee*, 749 U.S. at 764; *see also* 5 U.S.C. § 552(b)(7)(C) (1994) (exempting records or information compiled for law enforcement purposes if the production of such information "could reasonably be expected to constitute an unwarranted invasion of personal privacy").

> solicitations from sellers of home-security products, and such lists would be a boon to sophisticated burglars. A list of tobacco users might be of interest to potential employers and insurance companies.[212]

For some, this data processing raises nary an eyebrow; for others, it shocks the conscience. Who is right, and how do we decide?

D. *Encryption*

Before trying to answer these questions, an aside on technology is warranted. Above, I described how the new technologies of cyberspace threaten privacy. A balanced view also requires an understanding of how new technologies can protect privacy.[213]

1. *Possibilities.*

The principal privacy-protecting technology is encryption. In basic terms, encryption uses a cryptographic algorithm and a key to encode a message—plaintext—into something incomprehensibly garbled—ciphertext. Once communicated to the intended recipient, the ciphertext is decoded back into plaintext. If the cryptographic algorithm is strong, and the key properly selected and kept secret, it is infeasible for an unauthorized party to intercept the ciphertext and decrypt it back into plaintext. This basic concept of encryption lies at the heart of multiple privacy-promoting technologies.[214]

---

212. Gary T. Marx, *Privacy and Technology*, WHOLE EARTH REV., Winter 1991, at 90, 92.

213. In certain respects, modern life and its attendant technological advances have led to greater, not less, privacy. *See, e.g.*, Ferdinand Schoeman, *Privacy: Philosophical Dimensions of the Literature*, *in* PHILOSOPHICAL DIMENSIONS OF PRIVACY, *supra* note 22, at 1, 1-2 (arguing that we have more privacy than our ancestors due to urban life and architecture); Stigler, *supra* note 95, at 623 (arguing that ordinary citizens have more privacy than ever before).

214. Encryption schemes fall into two basic categories: private key, or symmetric, and public key, or asymmetric. Private key encryption utilizes a single key to encode plaintext into ciphertext and to decode ciphertext back into plaintext. If A wants to send B an encrypted message, both A and B must have the same private key. The difficulty arises in that A and B must be able to exchange that private key, lest someone else get hold of it. But such a secure channel is difficult to find, which is why encryption is sought in the first place. As one commentator quipped, "[I]t is impossible to send someone a secret message [with private key cryptography] unless you already have the ability to send her a secret message." SIMSON GARFINKEL, PGP: PRETTY GOOD PRIVACY 45 (1995).

Public key encryption solves this problem. In this type of encryption, two keys are involved: a complementary pair consisting of one public key and one private key. Whatever is encoded with one key can be decoded only with its complement. Thus, if a message is encoded with A's public key, it can be decoded only with A's private key. To use public key encryption, each person produces a public/private key pair. The private half is kept secret and the public half is released to the entire world. If A wants to send a secure message to B, A simply locates B's public key, which has been publicly released, and uses it to encrypt the message. A then sends the ciphertext to B. This ciphertext can be decoded only by the complementary private key, which should be in B's exclusive possession.

Obviously, cryptography can be used to promote the confidentiality of a communication. Consider, for instance, how public key cryptography is integrated into standard Web browsers, such as Netscape's Navigator, to enable confidential transmission of credit card numbers over the Internet.[215] Besides protecting the confidentiality of communications, encryption is also useful in creating robust anonymity, which cuts the link between personal information and the person to whom it relates.[216]

Two aspects of anonymity are important here: anonymous communications and anonymous payment systems. Anonymous communications are made possible through, for example, the use of anonymizing intermediaries, such as anonymous e-mail remailers. These intermediaries are computers that, upon receipt of a communication, remove any information identifying the sender of the communication, then send it along to the recipient. With an e-mail message, for instance, an anonymous remailer strips off header information identifying the sender, replaces it with the information identifying the remailer, then sends the message to the intended recipient.[217]

One weakness of this arrangement is that certain intermediaries maintain lists matching the message and the original sender, in part to allow easy replies to anonymous communications.[218] In such cases, anonymity is put at

---

The critical advantage of public key encryption is that a secure channel is no longer needed to exchange a private key between parties to a communication. Indeed, one can send an encrypted message to a total stranger. Of course, no encryption scheme is perfect, and public key systems suffer certain weaknesses—most importantly, the difficulty in being sure that the public key you locate really belongs to the person to whom you want to send the message. This is why certification authorities are necessary. *See* note 197 *supra*.

215. When the consumer and the merchant are about to exchange sensitive data, Netscape invokes a secure communications protocol. This involves the following basic steps: (1) the consumer creates a random session key; (2) the merchant sends the merchant's public key to the consumer in the clear with a certificate signed by some trusted third party, such as Netscape, confirming that the merchant is who it claims to be; (3) the client verifies the signature on the certificate and authenticates the merchant's public key; (4) the consumer encrypts the session key with the merchant's public key and sends it to the merchant; (5) the merchant decrypts the session key with its private key; and (6) henceforth, all messages between consumer and merchant are encrypted with that session key.

216. For one of the best law review commentaries on anonymity in cyberspace, see Froomkin, *supra* note 200.

217. Web browsing can also be conducted through an anonymizing proxy. Such a proxy receives the desired Uniform Resource Locator, e.g., Web site address, from the individual, reads the requested Web page, disclosing to the server only information about the anonymizer site, not the individual, then relays the Web page back to the individual. *See* ANONYMIZER, INC., *Anonymizer* (visited Feb. 6, 1998) <http://www.anonymizer.com> (describing anonymous Web browsing).

218. Michael Froomkin emphasizes the difference between anonymity and pseudonymity. The latter connects information to a fabricated persona, a nom de plume. Many "anonymous" remailers, which allow easy replies back to the message sender, are in fact "pseudonymous" remailers. *See* Froomkin, *supra* note 200, at 421-24 (describing the many remailers that operate pseudonymously); *see also* Andre Bacard, *Anonymous Remailer FAQ* (visited Nov. 5, 1997) <http://www.well.com/user/abacard/remail.html> (distinguishing truly anonymous and pseudo-anonymous remailers).

risk because the person maintaining the intermediary may be compelled to disclose the identity of the message sender.[219] One way to bolster anonymity is to use an intermediary that does not keep any traces of information that identify the sender. In addition, one can use a successive chain of anonymous intermediaries. One's anonymity would then be sacrificed only if every machine in the chain kept identifying information and agreed to disclose that information. This technique is facilitated by encryption.[220] When one considers the fact that an e-mail can be routed through twenty anonymous intermediaries—all through the help of computer automation—and that many remailers exist in foreign countries, far beyond the jurisdictional reach of U.S. courts and law enforcement agencies, it becomes clear that one can have nearly absolute anonymity of communications.

Public key encryption also allows for the possibility of anonymous payment systems much like cash. Today, when one purchases ice cream at the local mall with cash, there is no record identifying the individual's purchase. However, if the same purchase is made via credit card, debit card, or check, transactional data linking the individual to the purchase may be recorded. A privacy-promoting payment technology would allow secure electronic payment through cyberspace, while disclosing no more personal information than cash.[221] The cryptographic technology of blind digital signatures makes

---

219. The Church of Scientology did just this and effectively shut down the popular remailer anon.penet.fi. *See Anon.penet.fi Is Closed!* (visited Apr. 27, 1998) <http://www.penet.fi/>.

220. Even if the remailer discloses the identity of the immediately previous sender and the immediately subsequent recipient, each and every remailer along the chain must do the same before anonymity is destroyed.

For the technologically curious: If A wants to send to B an anonymous e-mail message through three different remailers—say, X, Y, and Z—A first writes a message to B, adding a line that says "please mail to B." Then A encrypts this message and instruction with Z's public key and adds a line that says "please mail to Z." Next, A encrypts everything with Y's public key, including the previously encrypted material and the new instruction, and then adds yet another line that says "please mail to Y." Finally, A encrypts everything with X's public key. When X receives this message, it will decrypt it using its private key. It will see two things: a line of plaintext that says "please mail to Y" and ciphertext. X will follow the instruction and forward the ciphertext to Y. Y will decrypt the message using its private key, only to find a line of plaintext that says "please mail to Z" and some ciphertext. Y will then mail the ciphertext to Z. Finally, Z will decrypt the message using its private key, only to find a message that says "please mail to B," which Z will do. This scheme is called a cypherpunk remailer. *See* OBSCURA INFORMATION SECURITY, *Mixmaster & Remailer Attacks* (visited Nov. 5, 1997) <http://www.obscura.com/~loki/remailer/remailer-essay.html> (describing even more advanced "mixmaster" remailers).

221. Consider what an electronic cash scheme might look like. A consumer would transfer money from her bank to her electronic cash wallet, which could be on a hard drive or a smart card. She could then dispense electronic cash to cyberspace savvy merchants just as she would spend normal greenbacks. For this scheme to work, the bank must first be certain that there was no fraud when the cash was originally withdrawn. In other words, the bank must make sure that the consumer, and not an impostor or thief, withdrew the money. Also, the merchant must be sure that the electronic cash it receives is cash that will be honored by its bank. *See* Froomkin, *supra* note 200, at 453-71 (surveying forms of electronic cash).

this possible;[222] we can have what David Chaum calls absolutely unforgeable and untraceable electronic cash.[223]

2. *Limitations.*

There is a vein of thinking about cyberspace that discounts policy and law making as quaint but moot, made irrelevant by technology, especially strong cryptography. But this techno-anarchist view is pollyanish. First, the continuing legality of these technologies is uncertain in the United States. For example, the executive branch and certain members of Congress[224] have vigorously advocated various forms of key escrow systems. Under these systems, a private key is not kept by the individual alone; an extra copy is kept by either a government agency or a private sector third party. In addition, the export of strong encryption remains substantially regulated.[225]

Second, even when the technologies are permitted, they are limited. Consider the limits of using encryption to maintain confidentiality. While encryption may guarantee the confidentiality of communicative data during

---

222. A digital signature involves just the reverse of the public key cryptography process discussed above. Recall that a message encrypted by one half of the public/private key pair can be decrypted only by the other half. To scramble messages, one would encrypt a message with the recipient's public key, so that only the recipient's private key would be able to decode the message. One creates a digital signature by encrypting a message with one's own private key, which no one else should have. If the message decodes with that person's public key, which has been released to the world, then one can be confident that the message in fact came from that specific person. Indeed, a digital signature is far harder to forge than a handwritten signature.

With digital signatures, the bank can be certain that a consumer who withdraws electronic cash is who she claims to be. When the bank sends the cash to the consumer, the bank signs it with its own signature. When the cash is transferred to the merchant, the merchant can verify the bank's signature to ensure that the cash will be honored. This scheme protects privacy because the merchant need not and will not learn the identity of the consumer. The merchant is only concerned with getting paid; as long as the cash bears the bank's unforgeable signature, then the merchant's interests are secure. *See generally* David Chaum, *Achieving Electronic Privacy*, SCI. AM., Aug. 1992, at 96.

223. *See id.* at 96, 98 (discussing digital signatures and their relation to electronic cash). Now, there is the concern that an individual will simply copy his electronic cash and spend it repeatedly—like copying a one dollar bill with a color copier. But an attempt to spend the same electronic cash twice can be made to "reveal[] enough information to make the payer's account easily traceable. In fact, it can yield a digitally signed confession that cannot be forged even by the bank." *Id.* at 98.

224. For instance, Senators John McCain (R-Ariz.), Bob Kerrey (D-Neb.), and Earnest Hollings (D-S.C.) recently introduced The Secure Public Networks Act, S. 909, 105th Cong. (1997), which would require all federally funded communication networks to use key escrow encryption. It would also require certification authorities to keep a copy of an individual's private key before issuing a certificate. *See id.* §§ 205, 401, 405.

225. Encryption designed for military use remains on the U.S. Munitions List, regulated by the State Department and subject to regulations under the International Traffic in Arms Regulation, 22 C.F.R. §§ 120-130 (1994). Since October 1996, commercial encryption has been regulated by the Commerce Department. *See* Stewart A. Baker, *Government Regulation of Encryption Technology: Frequently Asked Questions*, *in* DOING BUSINESS ON THE INTERNET 287, 292-93 (1996).

electronic transmission, it often does nothing to prevent the collection of transactional data. For example, with e-mails, although an information collector may not be able to read the contents of an encrypted e-mail message, it may be able to read all the data incident to its transport between sender and receiver. Moreover, once the communication is received, the recipient must decrypt the message in order to process the communication. After the communication has been converted into "plaintext," encryption's role in ensuring privacy comes to an end.[226] Similarly, consider the limitations of anonymous payment schemes. Although anonymity can be preserved in a purchase of information or informational product, e.g., software, by combining an anonymous communication and anonymous payment system, the same cannot be said of purchases of physical objects, which require delivery to some physical address. And from that physical address, one has an entry point to a potential wealth of additional data.

Third, relying upon technologies alone may have unfavorable distributional consequences, which favor the computer savvy and well-educated. Although these technologies are not difficult to use, they are hardly effortless. Only those sophisticated enough to take advantage of public key encryption and anonymity filters may do so, with the rest of the population left defenseless due to ignorance.

Fourth, investing in privacy apparatus may be a waste of resources. Cyberspace and its related technologies make possible more privacy-invasive data acquisition; they also make possible more privacy-protecting shields. In a laissez-faire regime with a "survival of the cryptographically fittest" mindset on privacy, what we may soon have is an arms race between these two technologies.[227] A significant expenditure of resources by those who would take personal information and by those who would safeguard it may, in the end, result in a final level of privacy no different from the level that existed before such expenditures. Surgical state intervention may allow us to avoid such waste.[228]

---

226. *Cf.* Mark A. Lemley & David W. O'Brien, *Encouraging Software Reuse*, 49 STAN. L. REV. 255 (1996) (discussing means for protecting software). This is true unless the recipient re-encrypts the message.

227. For example, a handful of programs already respond to the privacy threat posed by cookies. *See* Charles Rejonis, *Opening the HTTP Cookies Jar* (visited Nov. 5, 1997) <http://www.netscapeworld.com/netscapeworld/nw-07-1996/nw-07-cookies.html> (listing cookie blocking tools).

228. *See* Murphy, *supra* note 159, at 2397 ("Presumably, stronger legal protection of privacy would reduce these socially wasteful costs."). A fully elaborated example of "surgical state intervention" appears in the Appendix.

III. THE MARKET SOLUTION

In this second half of the article, my goal and scope change. My goal changes from descriptive mapping to normative problem-solving. At the same time, my scope narrows from the general nexus of privacy and cyberspace to the particular problem of personal data generated through cyber-activity.[229] Let me frame the problem. All cyber-activity, even simply browsing a Web page, involves a "transaction" between an individual and a transacting party. Sometimes these transactions involve standard electronic commerce, such as the software purchase example. At other times, these transactions involve more sensitive exchanges, such as e-mail between patient and therapist. In the course of these mutual interactions, personal information is inevitably generated.[230] The transacting party and any transaction facilitators are potential information collectors.

Both the individual and the information collector value control of the information. The individual may not want the information collector to process the data—perhaps to avoid embarrassment, construct intimacy, or avert information misuse. The information collector may want to process the data—perhaps for database marketing. Both sides lay conflicting claims to the personal data. At this point of the analysis, privacy enthusiasts insist that the individual self-evidently owns her personal information. Therefore, the information collector should not be able to make use of that "property" without permission. Unfortunately, what is self-evident for some is question-begging for others. Information collectors retort that the information was generated in a mutual interaction, in which the individual and the information collector were equal participants. Why then should the individual have preferred rights over what was jointly produced? We are left with a genuinely hard choice. What shall be done?

A. *Default Rules*

I start with the market solution of cyberspace privacy. One might reasonably view personal information as a valuable commodity that should be exchanged on the free market.[231] Once personal information is produced, its

---

229. I discuss my reasons for limiting the scope at length in Part IV.A below.

230. The lion's share of these data will be personal in the descriptive or instrumentally mapped sense, but not in the authorship sense.

231. I use the term "free market" advisedly. *See* Pauline T. Kim, *Privacy Rights, Public Policy, and the Employment Relationship*, 57 OHIO ST. L.J. 671, 709 (1996) ("[I]n a sense, there is no such thing as a truly 'unregulated market': every market is based on legal rules—rules that establish the parties' starting positions and the bargaining ground rules."); *see also* CASS R. SUNSTEIN, FREE MARKETS AND SOCIAL JUSTICE 5 (1997) ("The notion of 'laissez-faire' is a grotesque misdescription of what free markets actually require and entail. Free markets depend for their existence on law.").

pricing and consumption can and should be governed by the laws of supply and demand. On this view, competing interests for personal information will simply be incorporated into its price.[232] On the one hand, if the individual is a privacy zealot or the information is particularly sensitive, then the individual may value it more than the information collector and pay the collector not to process it in problematic ways. On the other hand, if the individual cares little about privacy, then the firm may value it more and will process it in whatever ways it thinks profitable. Either way, through offers and counteroffers between individual and information collector, the market will move the correctly priced personal data to the party that values it most—as gauged by the willingness and ability to pay.[233]

This solution is pushed by economics-minded analysts on efficiency grounds.[234] It is supported by the private sector, which generally prefers market discipline and self-regulation to governmental interference. It is embraced by government policymakers in the current antiregulatory environment because the market solution displaces collective ordering by state action with private ordering by individual decisions.[235] In other words, it shifts responsibility for difficult global privacy questions onto local decisions made by the individual. The allure of the market solution is reflected in the executive branch's *IITF Principles*, which observe that "an individual's privacy can often be best respected when individuals and information users come to some mutually agreeable understanding of how personal information will be

---

232. *See, e.g.*, Steven A. Bibas, *A Contractual Approach to Data Privacy*, 17 HARV. J.L. & PUB. POL'Y 591, 604-05 (1994) (arguing that pricing reflects different consumer preferences about privacy).

233. *See* Stigler, *supra* note 213, at 627 ("[I]n voluntary transactions there is no reason to interfere to protect one party provided the usual conditions of competition prevail; the efficient amount of information will be provided in transactions, given the tastes of the parties for knowledge and privacy.").

234. *See, e.g.*, Bibas, *supra* note 232, at 604-05 (arguing that pricing privacy in the marketplace produces more efficient solutions); Kenneth C. Laudon, *Markets and Privacy*, 39 COMMS. OF ACM 92 (1996), *available in* 1996 WL 9011971 (advocating the creation of property rights over personal information to be traded on a regulated national information market); Scott Shorr, Note, *Personal Information Contracts: How to Protect Privacy Without Violating the First Amendment*, 80 CORNELL L. REV. 1756, 1818-46 (1995) (arguing for property rights in a data profile governed by contracts between individuals and credit reporting agencies).

235. *Cf.* Andrew L. Shapiro, *Privacy for Sale: Peddling Data on the Internet (*visited June 23, 1997) <http://www.TheNation.com/issue/970623/0623shap.htm> ("But in the current deregulatory climate, the Clinton administration and some privacy defenders . . . [are] calling for the creation of a market for privacy to compete with or complement the growing market for personal information."). For another example of promarket discourse in the context of cyberspace governance, see William J. Clinton & Albert Gore, Jr., *A Framework for Global Electronic Commerce* (visited July 1, 1997) <http://www.iitf.nist.gov/elecomm/ecomm.htm> ("Principle #2: Government should avoid undue restrictions on electronic commerce; Principle #3: Where governmental involvement is needed, its aim should be to support and enforce a predictable, minimalist, consistent and simple legal environment for commerce."). *See generally* MICHAEL J. TREBILCOCK, THE LIMITS OF FREEDOM OF CONTRACT (1993) (discussing the benefits of private ordering over collective ordering).

acquired, disclosed, and used."[236] This statement embodies the hope that individuals and the parties with whom they transact in cyberspace can come to mutually acceptable agreements about how personal information will be processed—all without substantial state refereeing. This is the essential faith of the market solution.[237]

Of course, what the market solution formally envisions we do not actually see. For numerous reasons, such as transaction costs, individuals and information collectors do not generally negotiate and conclude express privacy contracts before engaging in each and every cyberspace transaction. Any proposed market-based solution that does not acknowledge this economic reality is deficient. Moreover, a comprehensive market solution should specify the proper default rule for governing personal information in the absence of any express or implied-in-fact agreement.[238] I turn to that task now.

---

236. IITF PRINCIPLES, *supra* note 19, at 5. For background on the IITF and its privacy principles, see note 40 *supra*.

237. Information economists and intellectual property scholars will immediately wonder how the market will respond to the "public good" aspect of personal information. A public good has the qualities of nonrivalrous consumption and difficulty in excluding nonpaying beneficiaries. *See* ROBERT COOTER & THOMAS ULEN, LAW AND ECONOMICS 46, 112 (1988). Information often has these qualities to some extent, and personal data generated in cyberspace are no exception. Indeed, the digitalized environment promotes nonrivalrous consumption—because copies are as good as the original—and makes exclusion harder because information is collected and shared cheaply.

The standard concern with public goods is that the market will underproduce them because free-riders cannot be excluded from consuming them. This is the economic rationale for much of intellectual property law. This rationale does not, however, neatly resolve issues of privacy. First, increased production of copyrightable materials may be an unmitigated good, but increased production of personal information is decidedly mixed. In particular, it threatens individual privacy. Second, the likelihood of underproduction is uncertain. Personal information is jointly produced by an individual and the information collector interacting in cyberspace. The individual does not spend any resources for the express purpose of generating personal data; instead, the data are generated as an unavoidable by-product of cyberspace activity. The only way that the individual can stop producing personal information is by leaving cyberspace. The individual may do so for privacy reasons, but it is unlikely that she will do so because free-riders are not paying her sufficiently for the use of her personal data. In contrast, the information collector does expend resources to capture personal data in the course of the interaction, but much of this information must be collected and processed to execute the transaction successfully. For such data, an inability to exclude free-riders will not materially alter the incentives for information collection. Anyway, it is wrong to think that excluding free-riders is so difficult: Free-riders can be excluded through data security, contract, and perhaps new intellectual property laws. *See* J.H. Reichman & Pamela Samuelson, *Intellectual Property Rights in Data?*, 50 VAND. L. REV. 51 (1997) (discussing European and U.S. initiatives to create property rights over noncopyrightable databases).

238. For recent commentary adopting a similar approach, see generally Schwartz, *supra* note 94; Keith Sharfman, Comment, *Regulating Cyberactivity Disclosures: A Contractarian Approach*, 1996 U. CHI. LEGAL F. 639.

1. *Market talk: Efficiency.*

For the moment, let us keep squarely within the economic paradigm and ask what sort of default rule would maximize efficiency.[239] There are two default rules that society might realistically adopt. First, unless the parties agree otherwise, the information collector may process the personal data anyway it likes. I describe this default rule as "plenary use" and will designate it as "D_1." This rule represents the status quo. When information is generated in the course of a cyberspace interaction between an individual and an information collector, that information is effectively in the public domain. Unless some agreement suggests otherwise, or some specific body of confidentiality law applies, either party may exercise plenary control over the information. Note that this default rule was not set after considered analysis of competing interests and values. Instead, it came into being by historical happenstance, through a confluence of uncoordinated background laws and technological developments.

In the alternative, the ground rule could be that unless the parties agree otherwise, the information collector may process the personal data only in functionally necessary ways. I describe this second default rule as "functionally necessary use" and will designate it as "D_2." This rule allows the information collector to process personal data on a need-only basis to complete the transaction in which the information was originally collected.[240]

---

239. Law and economics literature tends to use "efficiency" in two senses. First, Pareto efficiency asks whether a transaction makes somebody better off while making no one else worse off. Second, Kaldor-Hicks efficiency—or potential Pareto efficiency—asks whether a transaction would generate sufficient gains so that beneficiaries could, although they need not, make losers whole and still have some gain left. "[T]his second approach is effectively a form of cost-benefit analysis." TREBILCOCK, *supra* note 235, at 7 (offering general summary explanations of the concepts of Pareto efficiency and Kaldor-Hicks efficiency). Frank Michelman refers to this as "value maximization." *See* Frank I. Michelman, *Norms and Normativity in the Economic Theory of Law*, 62 MINN. L. REV. 1015, 1019-20 (1978). Unless noted otherwise, I use "efficiency" in the Kaldor-Hicks sense.

240. This functional necessity concept is not novel; it appears in various incarnations throughout privacy statutes. For example, the 1984 Cable Act generally bars the collection of personal information through a cable system without prior consent, but it allows information collection if necessary to "render a cable service or other service provided by the cable operator to the subscriber," Cable Communications Policy Act of 1984, 47 U.S.C. § 551(b)(2)(A) (1995), and to "detect unauthorized reception of cable communications," *id.* § 551(b)(2)(B). The Act also bars the general disclosure of personal information without prior consent unless it is "necessary to render, or conduct a legitimate business activity related to, a cable service or other service provided by the cable operator to the subscriber." *Id.* § 551(c)(2)(A).

The VPPA generally bars disclosure of personal information, but allows it if "incident to the ordinary course of business," Video Privacy Protection Act of 1988, 18 U.S.C. § 2710(b)(2)(E) (1994), which is defined to include "only debt collection activities, order fulfillment, request processing, and the transfer of ownership," *id.* § 2710(a)(2). Debt collection and transfer of ownership are well-defined, but request processing and order fulfillment are vague. The legislative history explains that these terms contemplate "mailing houses, warehouses, computer services and similar companies for marketing to their customers." S. REP. NO. 100-599, at 14 (1988).

Unless some agreement suggests otherwise, the information collector could not, for instance, process personal data for marketing purposes or sell the information to third parties. Which default rule, D_1 or D_2, is more economically efficient?

If we lived in a world with perfect information, perfect competition, and zero transaction costs,[241] Coase's theorem teaches that either default rule would produce efficiency equally well.[242] But Coase recognized—indeed clamored—that we did not live in such a world.[243] In particular, high transaction costs may convert a theoretically "default" rule into a practically "immutable" rule, which could prevent an efficient result.[244] Moreover, even if transaction costs are not large enough to transform default rules into im-

---

Finally, the ECPA makes it clear that an employee of a wire or electronic communication service may "intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service." Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2511(2)(a)(i) (1995); *see also id.* § 2702(b)(5) (allowing electronic communications provider to the public to disclose the contents of communications if "necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service").

241. The following is a generally accepted explanation of transaction costs: "In general, transaction costs include the costs of identifying the parties with whom one has to bargain, the costs of getting together with them, the costs of the bargaining process itself, and the costs of enforcing any bargain reached." A. MITCHELL POLINSKY, AN INTRODUCTION TO LAW AND ECONOMICS 12 (2d ed. 1989).

242. *See* R.H. Coase, *The Problem of Social Cost*, 3 J.L. & ECON. 1, 6-8 (1960) (arguing that, in the absence of transaction costs, economically rational players will transact in a manner that produces a long-run equilibrium that maximizes value regardless of the initial assignment of entitlements); *see also* Daniel J. Bussel, *Liability for Concurrent Breach of Contract*, 73 WASH. U. L.Q. 97, 100 (1995) (describing Coase's theorem). To be more careful, one could add that there should be no wealth effects, which create a spread between bid and ask prices. *See* Alan Schwartz, *The Default Rule Paradigm and the Limits of Contract Law*, 3 S. CAL. INTERDIS. L.J. 389, 398 n.13 (1993).

Here is a clarifying example of Coase's insight. Imagine for argument's sake that the use of Customer's personal information is worth $1 to Firm. The prevention of such use, however, is worth $2 to Customer. Assuming no externalities, it would be efficient for the information not to be used for marketing because the benefit of use ($1) is less than the cost ($2). Even if society incorrectly set the default rule to "firm can use" (plenary use), Customer, behaving rationally in a world with zero transaction costs, would simply buy back control of her personal information from Firm for some amount between $1.01 to $1.99. In other words, regardless of the default, the personal information will not be used for database marketing.

243. On the reality of transaction costs, Coase writes:

> In order to carry out a market transaction it is necessary to discover who it is that one wishes to deal with, to inform people that one wishes to deal and on what terms, to conduct negotiations leading up to a bargain, to draw up the contract, to undertake the inspection needed to make sure that the terms of the contract are being observed, and so on.

Coase, *supra* note 242, at 15; *see also* Guido Calabresi & A. Douglas Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, 85 HARV. L. REV. 1089, 1094-95 (1972) (emphasizing that in order to reach an efficient result regardless of the initial allocation of entitlements, there must be zero transaction costs).

244. *See* Calabresi & Melamed, *supra* note 243, at 1101 (noting that where transaction costs are high, an initial entitlement may effectively become inalienable).

mutable ones, the default rule still matters because "it determines who will bargain and at what cost."[245] Consequently, even if one is concerned exclusively with efficiency, the default matters.

The conventional law and economics wisdom is that society should pick the default rule that a majority of the parties "would have agreed to if they could have costlessly planned for the event initially."[246] The appeal of this majoritarian rule stems from the reasonableness of the following assumption: The reason why the parties did not contract explicitly on privacy is that specifying terms for every contingency is too costly. By implementing what a majority of contracting parties would have wanted, a majoritarian default guesses right in most cases and forces only a numerical minority to incur the costs of contracting around the default rule.[247]

To apply the simplistic majoritarian rule to our problem, we would have to identify the set of all cyberspace transactions and count the number of cases in which the parties—with perfect information and no transaction costs—would have agreed on plenary use as opposed to functionally necessary use. If the former number is greater than the latter, then we would adopt D_1, and if not, D_2. The majoritarian rule, however, suffers two difficulties—one empirical, the other theoretical. First, we lack good data about which number is larger. Second, the conventional wisdom is not what it used to be. In fact, since the late 1980s, the conventional wisdom has taken a pounding.

In their seminal 1989 article,[248] Ian Ayres and Robert Gertner detailed why the majoritarian rule does not necessarily maximize efficiency. As they demonstrated, a one-size-fits-all default rule will be efficient for some number of transactions but inefficient for others. Those parties for whom the default rule is inefficient will either contract around the default rule—the "flip"—or they will stay with the default rule—the "stick"—and accept the inefficiencies.[249] Thus the social cost of a default rule equals the sum of the aggregate transaction cost of contracting around the rule—the "flip

---

245. Jason Scott Johnston, *Strategic Bargaining and the Economic Theory of Contract Default Rules*, 100 YALE L.J. 615, 624 (1990).

246. POLINSKY, *supra* note 241, at 27.

247. *See* Ian Ayres & Robert Gertner, *Filling Gaps in Incomplete Contracts: An Economic Theory of Default Rules*, 99 YALE L.J. 87, 92-93 (1989) (introducing default rules and the majoritarian approach).

248. *Id.*

249. One reason for "sticking" may be transaction costs. Consider why in the real world transaction costs may not be zero or even de minimis. In order for Customer to buy back her privacy, she would have to spot the issue, inquire about the privacy practices of Firm, wait for a response, then negotiate with Firm toward some mutually acceptable set of privacy terms. Suppose, then, these efforts would cost at least $3 for Customer. Since the $2 gain to Customer is less than the $3 cost, a rational Customer will not engage in such bargaining. The existence of transaction costs thus freezes the initial default, regardless of its efficiency. This is not an empirical claim about actual transaction costs; it is a demonstration of the stick effect when transaction costs are high enough to deter subsequent exchanges.

cost"—plus the aggregate inefficiency cost of not contracting around the rule even when it would be more efficient to do so—the "stick cost".

This can be restated in more symbolic terms. Assuming that all cyberspace transactions involve bilateral transactions between two transacting parties, let "" designate the total number of cyberspace transactions in which a given default rule is inefficient. The average cost of sticking with this inefficient rule is "f." Now, let "$" be the total number of transactions in which the parties flip out of the inefficient default rule. Finally, the average transaction cost to negotiate around the inefficient rule is "c." With these definitions, the flip cost equals the number who flip ($) multiplied by the average transaction cost per flip (c). The stick cost equals the number of transactions in which the parties stick to an inefficient default rule (-$) multiplied by the average inefficiency associated with the wrong default (f).[250]

At once we see that focusing solely on —which is what the majoritarian rule does—ignores other relevant variables. The three key factors that are overlooked are the comparative costs of contracting around different default rules (the c's), the comparative number of parties who will actually contract around different default rules (the $'s), and the comparative inefficiencies associated with parties who will not contract around the different default rules (the f's).[251] As Ayres and Gertner put it, "Implementing a complete theory of default choice requires attention to:

1) what the parties want (the 's);

2) whether they will get it (the $'s); and

3) the costs associated with getting it (the c's) or not getting it (the f's).[252]

Already complex, these observations about efficient default rules have been amended, challenged, and further complicated.[253] The one consensus arising from these analyses is that the conventional wisdom is only crudely correct. Unfortunately, the literature has distilled no simple counterwisdom to take its place. Indeed, theoretical complexity and lack of data leave policymakers in an unenviable position. As Ayres and Gertner put it, while a default rule may be shown to be efficient in theory, "there is small hope that

---

250. My terminology and use of variables track Ayres and Gertner's use, with minor differences. To avoid confusion, let me clarify, however, that I am using and $ as gross numbers, whereas Ayres and Gertner use them as percentages. Also, the neologisms "flip cost" and "stick cost" are, to my knowledge, my creations, and not standard terms of art.

251. *See* Ayres & Gertner, *supra* note 247, at 113-15 (providing the more comprehensive general cost model for default rules). The authors perceptively demonstrate that the majoritarian rule is efficient only in two special cases. In one case, transaction costs must be low enough that there is no sticking whatsoever, and the costs of contracting around either default rule must be identical. In the other case, transaction costs must be so high that there is total sticking, and the inefficiencies associated with either default rule must be identical. *See id.* at 114.

252. *Id.* at 116.

253. *See, e.g.*, Sharfman, *supra* note 238, at 641 n.13 (collecting literature on default rules).

lawmakers will be able to divine the efficient rule in practice."[254] In light of this, what should policymakers pursuing efficiency do? In my view, the best approach would be to adopt an attitude of modest skepticism—modest in that we reject any claims to mathematical certitude, skeptical in that we rebuff any quick-and-dirty formulae, such as the majoritarian rule. This approach would try to think through what equilibria would likely result from adopting one default or another, all the while paying attention to the different sources of contractual incompleteness. It would then examine the entire range of relevant variables identified above to make a well-informed, although still uncertain, judgment.

With modest skepticism then as our state-of-mind, let us start the analysis by assuming that D_1—i.e., plenary use—is in place. In this world, those individuals who value the personal information more than the information collector must buy back control from the collector. What sort of equilibria will result? Will these individuals mostly flip out of the default—as would be efficient in a perfect information, zero transaction cost world—mostly stick to the default, or do a lot of both? I believe that most will stick.

Consider what the individual would have to do to flip out of the default rule. First, she would face substantial research costs to determine what information is being collected and how it is being used. That is because individuals today are largely clueless about how personal information is processed through cyberspace. Transacting parties and transaction facilitators do not generally provide adequate, relevant notice about what information will be collected and how it will be used.[255] What is worse, consumer ignorance is sometimes fostered by deceptive practices.[256]

---

254. Ian Ayres & Robert Gertner, *Strategic Contractual Inefficiency and the Optimal Choice of Legal Rules*, 101 YALE L.J. 729, 733 (1992).

255. According to the Privacy Rights Clearinghouse, "[Our] major finding . . . is that consumers suffer from a serious lack of knowledge of privacy issues. Many consumers are unaware of personal information collection and marketing practices. They are misinformed about the scope of existing privacy law, and generally believe there are far more safeguards than actually exist." PRIVACY RIGHTS CLEARINGHOUSE, SECOND ANNUAL REPORT 21 (1995) [hereinafter PRC REPORT].

For instance, instead of asking customers to volunteer their addresses, certain merchandisers use "reverse appending" to identify the names and addresses of customers who pay by credit card. The credit card account numbers are captured by the merchant in the course of a purchase, sent to a credit reporting company, and used by the merchant to uncover both the name and address of the credit card holder without the individual's knowledge. *See* PRC REPORT, *supra*, (identifying Eddie Bauer as one such merchant and Trans Union as one such credit reporting company); *see also* Bernstein, *supra* note 82, at A1 (reporting how individuals who had completed surveys felt deceived when they learned that the surveys would be processed by prisoners). *See generally* SMITH, *supra* note 18, at 148-50 (discussing focus group research revealing widespread ignorance of privacy practices in the credit, medical insurance, and life insurance industries); ELECTRONIC PRIVACY INFORMATION CENTER, *Surfer Beware: Personal Privacy and the Internet* (visited Jan. 26, 1998) <http://www.epic.org/reports/surfer-beware.html> ("We found that few Web sites today have ex-

Second, the individual would run into a collective action problem. Realistically, the information collector—the "firm"—would not entertain one person's idiosyncratic request to purchase back personal information because the costs of administering such an individually tailored program would be prohibitive.[257] This explains the popular use of form contracts, even in cyberspace,[258] that cannot be varied much, if at all. Therefore, to make it worth the firm's while, the individual would have to band together with like-minded individuals to renegotiate the privacy terms of the underlying transaction. These individuals would suffer the collective action costs of locating each other, coming to some mutual agreement and strategy, proposing an

---

plicit privacy policies . . . and none of the top 100 Web sites meet basic standards for privacy protection.").

256. One major list compiler once conducted a telephone survey identifying itself only as a "Survey Research Bureau in Lincoln, Nebraska" and asked various questions about ice cream. The final question asked for the ages of everyone in the household. In truth, the list compiler had no interest in ice cream data; it was interested solely in ascertaining the ages of household members. *See* Rick Wartzman, *Information, Please: A Research Company Got Consumer Data from Voting Rolls*, WALL ST. J., Dec. 23, 1994, at 1; *see also* LARSON, *supra* note 205, at 12 (describing a study in the *Journal of Business Ethics* that found "recent [marketing MBA] graduates to be far more willing [than their counterparts in the early 1980s] to deceive the subjects of a marketing research poll in order to gain their cooperation").

Sites targeting children present special dangers. For instance:

> At the Batman Forever Web site, supplying personal information becomes a test of loyalty. "Good citizens of the Web, help Commissioner Gordon with the Gotham Census," children are urged. Although the survey uses the guise of a virtual city's census, much of the information sought pertains to purchasing habits and video preferences. For example, respondents are asked how likely they are to buy *Batman Forever* and *Apollo 13* on video.

Shelley Pasnik & Mary Ellen R. Fise, *Children's Privacy and the GII*, *in* NTIA REPORT, *supra* note 11, at ch. 1, §H. The FTC conducted a spot review of children's Web sites. It found that approximately 86% collected personal data such as "names, e-mail addresses, postal addresses and telephone numbers," approximately 30% posted a privacy policy, and approximately 4% asked the children to get parental permission. FEDERAL TRADE COMM'N, *FTC Surfs Children's Web Sites to Review Privacy Practice* (visited Jan. 26, 1997) <http://www.ftc.gov/opa/9712/kids.htm>.

257. As a Citicorp official noted:

> It is true that privacy policies of this sort are not separately negotiated with each individual consumer. Most companies, even in a highly competitive market such as consumer financial services, must obtain and use certain data in relatively standard ways in order to provide the requested services efficiently, and it would be wholly impractical for such companies to collect and process data according to a large number of variable protocols, depending on variations in particular contractual arrangements reached with individual customers. But companies can inform their customers about their data handling practices and allow customers to make choices from a menu of standard options with respect to particular uses of customer data (such as marketing).

Duncan A. MacDonald, *Privacy, Self-Regulation, and the Contractual Model: A Report from Citicorp Credit Services, Inc.*, *in* NTIA REPORT, *supra* note 11.

258. The cyberspace analogue to the "shrinkwrap" license common to software packaging is the "click-on" license. *See generally* Mark Lemley, *Shrinkwraps in Cyberspace*, 35 JURIMETRICS J. 311 (1995); Gary H. Moore & J. David Hadden, *On-Line Software Distribution: New Life for "Shrinkwrap" Licenses?*, COMPUTER LAW., Apr. 1996, at 1.

offer to the information collector and negotiating with it—all the while discouraging free riders.[259]

But perhaps this collective action story is exaggerated, especially if we assume competitive markets. After receiving a few requests to buy back control of personal data, the firm might spot a profit opportunity and offer a menu of privacy options with differing premiums attached to each option. This menu would not be so complicated as to be unadministrable, but sufficiently varied to satisfy a large percentage of individual preferences. Further, the firm could present this menu cheaply through the interactive technologies of cyberspace, for example, as a check-off option in a dialog box.[260] Perhaps it would not be so expensive to flip out of D_1 after all.

Richard Murphy, however, has explained why this privacy menu may not appear. Providing a menu of privacy options, with the necessary detail to comprehend them, would draw attention to unsavory privacy practices that the collector may not want to highlight.[261] As just mentioned, many individuals currently do not know how personal information is harvested and processed, especially in cyberspace. Accordingly, firms can get something for nothing because individuals do not realize that they are losing anything. Put another way, firms are "strategically withhold[ing] information that would increase the total gains from contracting . . . in order to increase [their] private share of the gains from contracting."[262] The privacy menu would change that, by alerting individuals to a privacy cost that they had previously ignored in calculating the benefits and costs of cyberspace transactions. This disclosure would generate more accurate pricing by the individual, which in turn may prompt certain individuals to forgo the transaction entirely or to demand price concessions from the collector-firm. If this would decrease the firm's private share of the gains, the firm rationally would not offer the privacy menu.

In conjunction, as Murphy has suggested, privacy options may not appear because individuals will not take advantage of such options if they ap-

---

259. *See* Peter P. Swire, *Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information*, *in* NTIA REPORT, *supra* note 11, at text accompanying note 6 (no pagination in electronic copy) (noting the costs of bargaining).

260. *See* Murphy, *supra* note 159, at 2413.

261. *See id.* at 2414 ("[M]erchants cannot tell which consumers value privacy highly without asking all consumers. Raising the privacy issue may evoke negative reactions in consumers who otherwise would not have thought about the issue."). Some anecdotal support is found in SMITH, *supra* note 18, at 51-54 (discussing difficulties of getting businesses to agree to a privacy case-study notwithstanding express support from the Harvard Business School and repeated offers to sign confidentiality agreements).

262. Ayres & Gertner, *supra* note 247, at 94; *see also id.* at 99 (emphasizing the importance of information). Ayres and Gertner note that in such cases, it may be efficient to establish a penalty default rule—which is not what most parties would want—in order to force the disclosure of information. *See id.* at 91.

pear in isolation. Over a period of time, an individual will complete numerous transactions with numerous firms in cyberspace. With D_1, each firm can do what it likes with the personal information collected in the course of that transaction. Now imagine that one firm breaks with convention and offers a privacy menu. Will the individual take advantage of this offer? Quite possibly not. An individual knows that even if she buys control over this particular batch of personal information, she will not have control over innumerable batches of similar data coursing through cyberspace. Accordingly, the value of control over this batch is substantially reduced unless the individual can buy control over similar batches of data from other firms.[263] Therefore, a rational individual may not pay the premium for the privacy option offered by the vanguard firm. As a result, little competitive pressure will fall on other firms to follow the vanguard's lead. In sum, for these two reasons, it is unlikely that detailed privacy menus that allow individuals to pay for different degrees of privacy will broadly appear; thus, the collective action problem remains.[264]

In the end, the high research costs of learning the firm's data processing practices and collective-action problems make it likely that D_1 will be sticky. In this equilibrium, individuals who value personal information more than the firm, and for whom a functionally necessary rule would thus be more efficient, will nevertheless stick to the default rule of plenary use.[265]

By contrast, I believe that D_2—i.e., functionally necessary use—would not be sticky at all. With this default, if the firm valued personal data more than the individual, then the firm would have to buy permission to process the data in functionally unnecessary ways. Note, however, two critical differences in contracting around this default. First, unlike the individual who had to find out what information is being collected and how it is being used, the collector need not bear such research costs since it already knows what

---

263. It is possible that this phenomenon may also apply to information collectors: If they cannot get all the information from all persons, they may not want any of it from anyone. I believe this is not the general case for information collectors in cyberspace. For a limited defense, see note 266 *infra*.

264. And this is, in fact, what we see in the world today. Simply ask yourself how often you have seen a meaningfully detailed privacy notice or menu in cyberspace—or elsewhere for that matter. *See* PRIVACY & AMERICAN BUSINESS, COMMERCE, COMMUNICATION AND PRIVACY ONLINE 37 (1997) [hereinafter P&AB SURVEY] (reporting that 25% of those surveyed did not know whether their on-line service collected personal information, and of those who believed that they did, 71% were unaware of the service's particular practices). For those who think that this is because no one cares about privacy, I contend that the surveys conducted by Equifax, GVU, and Boston Consulting Group, not to mention the uproar caused by the Lexis P-TRAK and the Social Security Administration's PEBES initiatives, suggest otherwise. *See* note 12 *supra*; *see also* P&AB SURVEY, *supra*, at viii (reporting that 53% of Internet users and 57% of on-line service users are either very or somewhat concerned about the tracking and disclosing of cyber-activity data).

265. Even if I am only partly right, as long as some sizable number of parties ends up sticking to an inefficient default rule, my ultimate conclusion would not change. *See* note 268 *infra*.

its information practices are. Second, the collector does not confront collective action problems. It need not seek out other like-minded firms and reach consensus before coming to the individual with a request. This is because an individual would gladly entertain an individualized, even idiosyncratic, offer to purchase personal information. In addition, there will be no general "holdout" problem because one individual's refusal to sell personal information to the collector will not generally destroy the value of personal information purchased from others.[266] Thus, D_2 will generate an equilibrium in which the firms who value personal information more than the individual—and thus for whom a plenary use rule would be more efficient—would likely flip out of the default rule of functionally necessary use.

Now, the task is to compare the two equilibria to see which minimizes costs. For D_1's "sticky" equilibrium, the cost of the default rule is approximately the stick cost; the flip cost approaches zero since few parties will flip. In other words,

$Cost(D_1)$ = Flip Cost + Stick Cost

$Cost(D_1) = (\$_2)(c_2) + (\"_2\text{-}\$_2)(f_2)$, where

- $\$_2$ = number of transactions in which the parties flip out of D_1 to D_2
- c_2 = average transaction cost to flip out of D_1 to D_2
- $\"_2$ = number of transactions in which the individual values functionally unnecessary processing of personal information *more* than the information collector
- f_2 = average inefficiency of sticking to D_1[267]

If $\$_2$ is approximately equal to 0, then $Cost(D_1)$ is approximately $(\"_2)(f_2)$[268]

---

266. One case in which there could be a holdout problem is the census, an example offered by Richard Posner. Posner argues that it would be foolish to require the Census Bureau to purchase personal information from individuals. If the Bureau offered the same price for data from each individual, it would receive a skewed sample. To correct the sample, the Bureau would have to offer different prices to each individual according to a complicated pricing algorithm, which would be prohibitively costly. *See* Posner, *supra* note 56, at 398. Therefore, the default rule should favor government use.

The persuasiveness of this argument turns on two peculiar aspects of the census. First, its value requires across-the-board participation, or its statistically sampled equivalent; a partial census is no census at all. This is not generally the case, however, with personal information collected in cyberspace by the private sector, for, say, marketing purposes. For example, the marketing database of Ford Motors Online, based on Web browsing of its site, is not destroyed if Ford cannot acquire marketing data on those passionate about their privacy. To be sure, its total value may be reduced proportionally by having fewer records in its database, but this is not an all-or-nothing scenario like the census. Second, the rhetorical force of Posner's example stems from the civic-natured and public-good qualities of an accurate census. But private sector databases, produced by recording cyberspace transactions, lay far weaker claims to these qualities.

267. This formula first appeared in Ayres & Gertner, *supra* note 247, at 113.

268. Even if I am wrong about $\$_2$ being a relatively small number, the flip cost ($\$_2c_2$) will still be relatively small as compared to the stick cost because, for reasons outlined just below, c_2 is small and will decrease over time. So, as long as $\$_2$ does not approach $\"_2$—which would mean that instead of a "sticky" equilibrium, we would have a "Teflon" equilibrium like D_2—my ultimate con-

For D_2's "Teflon" equilibrium, the cost of the default rule is approximately the flip cost; the stick cost approaches zero since almost all parties for whom it would be efficient to flip will flip. In other words,

$Cost(D_2) = Flip\ Cost + Stick\ Cost$

$Cost(D_2) = (\$_1)(c_1) + ("_1\text{-}\$_1)(f_1)$, where

- $\$_1$ = number of transactions in which the parties flip out of D_2 to D_1
- c_1 = average transaction cost to flip out of D_2 to D_1
- $"_1$ = number of transactions in which the individual values functionally unnecessary processing of personal information *less* than the information collector
- f_1 = average inefficiency of sticking to D_2

If $\$_1$ is approximately equal to $"_1$, then $Cost(D_2)$ is approximately $("_1)(c_1)$

Which default rule is more expensive and thus less efficient? Answering this question requires us to determine whether the cost of D_1—$("_2)(f_2)$—is greater than the cost of D_2—$("_1)(c_1)$. There are some polling data to suggest that $"_2$ is greater than $"_1$.[269] But surveys have limited value because respondents do not have to put their money where their mouths are. So I do not rest on this suggestive comparison. On the other hand, there is strong reason to believe that f_2—the average inefficiency of sticking to D_1—is greater than c_1—the average cost of flipping out of D_2 to D_1. Given how seriously many individuals—even if they are lampooned as "privacy freaks"—feel about their privacy, f_2 will not be a trivial cost. But c_1, the transaction cost for the firm to ask the individual for permission to use information, may well be trivial because cyberspace makes communications cheap. What is more, this inequality will only increase over time. As information processing becomes more sophisticated, people will feel less and less in control of their personal information; accordingly they will value control more and more.[270] Simultaneously, the costs of communication will decrease as cyberspace communications become cheaper. Consider, for example, recent moves toward forming standardized trustmark icons that signify the basic privacy terms of a transaction.[271] Moreover, this privacy "negotiation" could soon become

---

clusions should not change. Although the cost of D_1 will be lower than stated in the body of the text, it should still be greater than the cost of D_2.

269. *See* note 12 *supra* (citing numerous polls which indicate that many Americans rank protection of privacy among their most serious concerns about the Internet); *cf.* P&AB SURVEY, *supra* note 264, at xi (reporting that only 26% of those surveyed were very or somewhat "interested in a customized Internet service that would provide tailored offers of products and services").

270. This is the drift suggested by the *GVU Seventh Study* and the *GVU Eighth Study*. *See* note 12 *supra*; *see also* SMITH, *supra* note 18, at 5 (graphing the rise of the privacy concern from 1977-1992).

271. One example is TRUSTe, a nonprofit organization, founded by the Electronic Frontier Foundation and the CommerceNet Consortium as a global initiative for establishing consumer trust and confidence in electronic transactions. The TRUSTe system is an independent ranking system with logos that designate a merchant's information practices. Upon seeing the "trustmark" at a

automated between, say, Web browser and server, with the browser configured to accept standard offers for information processing at certain prices.[272]

In conclusion, I believe that it is more likely than not that Cost(D_1) is greater than Cost(D_2) and that this inequality will grow over time. Therefore, an efficiency analysis borne of modest skepticism recommends implementing D_2. Unless the parties agree otherwise, the information collector should process personal data only in functionally necessary ways.[273]

2. *Nonmarket talk: Dignity.*

Many readers will have found the above discussion profoundly unsatisfying for they explicitly reject market-talk. They deny that market-talk enjoys the precision or determinacy that it often touts.[274] They also find human

---

participating Web site, the individual can choose for herself whether to deal with a particular company. The three marks are "No Exchange," "One-to-One," and "Third Party." *See* TRUSTE, *TRUSTe* (visited June 11, 1997) <http://www.truste.org>. One commentator has remarked that by converting detailed privacy practices into just one of three possible trustmark icons, this system risks oversimplification—nearly all information collectors may bunch up in the middle category. *See* Jim Seymour, *Whom Can You Trustmark*?, PC MAG., June 24, 1997, at 93 (endorsing the TRUSTe rating system). *See generally* INTERNET PRIVACY WORKING GROUP, *The Empowered User: Implementing Privacy Policy in the Digital Age, Written Comments Before Federal Trade Commission* (visited June 11, 1997) <http://www.cdt.org/privacy/970611_FTC_IPWG.html> (discussing the creation of a uniform vocabulary to describe personal information practices).

272. The P3 project—Platform for Privacy Preferences—would allow individuals to set the privacy preferences of their browser. If a server's privacy practices differ, then the individual is warned. The individual need not rely upon the "privacy practices" ratings presented by the server itself. Rather, she could use ratings produced by third parties. *See* Courtney Macavinta & Tim Clark, *Privacy Advocates Question OPS* (visited Feb. 6, 1998) <http://www.news.com/News/Item/0,4,11412,00.html>.

273. If, for political reasons, we end up stuck with D_1, the above analysis suggests that, at the least, we should teach individuals what the prevailing default rule is. This would involve broad public education about cyberspace privacy, which is advocated by the *IITF Principles*. *See* IITF PRINCIPLES, *supra* note 19, at 10 ("Information users should educate themselves and the public about how information privacy can be maintained.").

274. Let me point out a few familiar indeterminacies in market talk. Efficiency analysis takes place only after fixing the existing wealth distribution and individual preferences as given. If we alter the initial wealth distribution or individual preferences, we also alter what is efficient. *See* EJAN MACKAAY, ECONOMICS OF INFORMATION AND LAW 19 (1982) (explaining that Pareto optimality is only meaningful if an initial distribution of wealth is specified); Baker, *supra* note 106, at 476 (noting that economic analysis must assume an initial wealth and preference distribution); Calabresi & Melamed, *supra* note 243, at 1096 ("Pareto optimality is optimal *given* a distribution of wealth, but different distributions of wealth imply their own Pareto optimal allocation of resources."). But by assigning rights based on an efficiency calculus, we alter the underlying wealth and preference distributions assumed to be fixed in the original calculus. *See* SUNSTEIN, *supra* note 231, at 52 (discussing preference distribution). Thus, implementing the solution alters the problem it was designed to solve. *See* Baker, *supra* note 106, at 491-93 (explaining how the assignment of rights influences preferences); A. Mitchell Polinsky, Comment, *Economic Analysis As a Potentially Defective Product: A Buyer's Guide to Posner's Economic Analysis of Law*, 87 HARV. L. REV. 1655, 1670 (1974) (arguing that the assignment of property rights and liability rules partially determines the initial distribution of income).

values poorly translated, if at all, into efficiency terms. For these readers, the above analysis fails to grapple with the most fundamental reasons for respecting information privacy. Above, I discussed some of these reasons: avoiding embarrassment, constructing intimacy, and avoiding information misuse. Let me add another reason to the list: dignity.[275] I mention this value here, separate from the others, because more than the others, human dignity resists incorporation into market-talk.

Information collection presupposes observation of the individual. I concur with Stanley Benn that observation, when nonconsensual and extensive, is in tension with human dignity. As Benn argues, human beings have dignity because they are moral persons—entities capable of self-determination.[276] In other words, they have the capacity to reflect upon and choose personal and political projects and how best to further them. Extensive, undesired observation—what may be called "surveillance"—interferes with this exercise of choice because knowledge of observation "brings one to a new consciousness of oneself, as something seen through another's eyes."[277] Simply put, surveillance leads to self-censorship.[278] This is true even when the observable information would not be otherwise misused or disclosed.

To avoid overstating my case, I should distinguish surveillance from casual observation.[279] Casual observation does not produce problematic self-censorship. For example, when we walk through public spaces and are observed by various persons through their unaided senses, we do not feel disturbingly constrained in our ability to choose. This sentiment comes from a pragmatic, culturally bound, common sense understanding that social existence involves casual interaction with other people, including strangers, and

---

275. The most passionate proponent of this reason for protecting information privacy is Bloustein, *supra* note 31, at 971 (arguing that protecting dignity is the primary motivation behind the common law protection of privacy).

276. *See* Benn, *supra* note 89, at 228-29 (suggesting that the "general principle of respect for persons . . . is to see him as actually or potentially a chooser").

277. *Id.* at 227. Consider also the impact of a stranger's presence among intimates. The intimates can act as if the stranger were not present, which would violate their sense of appropriate behavior in front of strangers. Or they can act with their public faces, which could interfere with the intimate relationship. *See* Rachels, *supra* note 64, at 295-96 (positing such situations).

278. *See* text accompanying note 29 *supra* (noting this connection between information privacy and decisional privacy). One might argue that Benn's argument only works when a person is aware of the surveillance. This is not entirely true. The fear of surveillance alone could affect choice. *See* Wasserstrom, *supra* note 74, at 324 (arguing that not knowing whether one is being surveilled might be worse than knowing for certain). Benn adds that "[c]overt observation—spying—is objectionable because it deliberately deceives a person about his world, thwarting, for reasons that *cannot* be his reasons, his attempts to make a rational choice." Benn, *supra* note 89, at 230.

279. Benn similarly states that "there is a difference between happening to be seen and having someone closely observe, and perhaps record, what one is doing, even in a public place." Benn, *supra* note 89, at 225.

that in doing so incidental information in "plain view" will be collected about us. However—and here is the critical turn—information collection in cyberspace is more like surveillance than like casual observation.[280] As explained above, data collection in cyberspace produces data that are detailed, computer-processable, indexed to the individual, and permanent. Combine this with the fact that cyberspace makes data collection and analysis exponentially cheaper than in real space, and we have what Roger Clarke has identified as the genuine threat of dataveillance.[281]

But two objections must be heard to my cyber-surveillance-infringes-dignity argument. First, even if we concede that surveillance infringes the observed person's ability to choose, are we not—by prohibiting such surveillance—infringing upon the choice of the information collector to observe? In other words, if respecting human dignity requires respecting people's choices, then what are we to do when choices are mutually exclusive—for example, to avoid surveillance and to surveil? A more careful weighing of the respective burdens placed upon the two parties' ability to choose helps answer the objection. For the target, acutely aware of the surveillant's gaze, surveillance affects not only one choice but all choices by creating a sort of double vision.[282] By contrast, for the surveillant, prohibiting surveillance constrains only one particular choice—to observe systematically—and not the innumerable others the putative surveillant makes. Recall that we are not discussing casual observation but surveillance.

Second, even if data collection in cyberspace amounts to surveillance and not casual observation, surveillance is by-and-large legal in real space. Most private investigators engage in surveillance every day, tailing insurance claimants for fraud, jurors and witnesses for biases, and husbands and wives for infidelity. Why then should it become suddenly illegal in cyberspace? This objection seems powerful only because it papers over important complications. Notice the critical qualifier "by-and-large" in the articulated objection. The forms of surveillance in real space are, in fact, constrained by various laws. Most importantly, the human laws of property—e.g., trespass—conjoined with the natural laws of physics—e.g., the need for physical proximity and/or an unobstructed line-of-sight for unaided sense observa-

---

280. *See* text accompanying notes 201-212 *supra* (concerning the acquisition of information in cyberspace).

281. *See* Roger Clarke, *Introduction to Dataveillance and Information Privacy, and Definitions of Terms* (visited Jan. 28, 1997) <http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html#DV> (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").

282. Wasserstrom has commented on this double vision: "Aware of the observer, I am engaged in part in viewing or imagining what is going on from his or her perspective. I thus cannot lose myself as completely in the activity." Wasserstrom, *supra* note 74, at 324.

tion—substantially confine the limits of surveillance.[283] And when technology makes surveillance possible without trespassing, without physical proximity, without clear line-of-sight—in other words, when technology puts more and more into "plain view"—society has regularly intervened with privacy laws to limit such technologies. The celebrated example is *Katz v. United States*,[284] which reoriented the Fourth Amendment's privacy protections from places to people when eavesdropping technologies made walls—and glass telephone booths—more porous to surveillance.[285] The Electronic Privacy Communications Act is another example.[286] In fact, even the generally limp common law privacy tort of intrusion upon seclusion has at times responded to new technologies of surveillance.[287] On this view, cyberspace can be seen as the next gizmo that warrants response.

What is more, cyberspace surveillance is or will soon be far more common than physical surveillance because cyberspace alters the economics of surveillance. Because cyberspace has radically decreased the cost of collecting data, what might have been economically justified only for the targets of extraordinary investigations is now justified for the average Jane. Once the surveillance programming and infrastructure are laid, the data are harvested automatically by computers, at a fine resolution, as the individual navigates cyberspace. To return to the cyber-mall example, this information then can be cheaply exchanged from mall to mall, from "road" company to

---

283. In fact, states often require private investigators to be licensed. *See generally* John C. Williams, Annotation, *Regulation of Private Detectives, Private Investigators, and Security Agencies*, 86 A.L.R.3D 691 (1996).

284. 389 U.S. 347 (1967). Ken Gormley explains that one impetus for the *Katz* decision was the widespread increase during the 1940s and 1950s in the government's use of sophisticated surveillance technologies. *See* Gormley, *supra* note 24, at 1362-63.

285. The Court, per Justice Brandeis, explained that "once it is recognized that the Fourth Amendment protects people—and not simply 'areas'—against unreasonable searches and seizures, it becomes clear that the reach of that Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure." *Id.* at 353. He continued, "The fact that the electronic device employed to achieve that end did not happen to penetrate the wall of the booth can have no constitutional significance." *Id.*

286. The legislative history of the ECPA remarks:

> Most importantly, the law must advance with the technology to ensure the continued vitality of the fourth amendment. Privacy cannot be left to depend solely on physical protection, or it will gradually erode as technology advances. Congress must act to protect the privacy of our citizens. If we do not, we will promote the gradual erosion of this precious right.

S. REP. NO. 99-541, at 5 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3559.

287. *See* RESTATEMENT (SECOND) OF TORTS (1989) § 652B, cmt. b, illus. 2 (1997) (noting that it is tortious for "A, a private detective seeking evidence for use in a lawsuit, [to] rent[] a room in a house adjoining B's residence, and for two weeks [to] look[] into the windows of B's upstairs bedroom through a telescope taking intimate pictures with a telescopic lens"); *id.* illus. 3 (noting that it is tortious under "[t]he same facts as in Illustration 2, except that A taps B's telephone wires and installs a recording device to make a record of B's conversations").

"cash" company, from any information collector to inquiring people who want to know.[288]

For readers still unpersuaded that surveillance is in tension with human dignity, I offer one final set of arguments that shifts the axis from observation to touch.[289] Starting from the premise that we own our own bodies, I begin by asking: What precisely is wrong with a nonconsensual touch? Such a touch is socially unacceptable and sometimes tortious or criminal. But what exactly is wrong with touching a person without her permission? Surely, some instrumental concerns exist about physical health and safety. The touch in the form of a proper sidekick will break ribs; similarly, an unclean touch may transmit disease or sickness. But what if the touch is both gentle and clean, causing no physical harm?

In explaining why this touch is still unwarranted, many would appeal to some fundamental faith in self-determination and human dignity.[290] Even if the touch is physically harmless, a person should presumptively enjoy the sovereignty to determine who may touch her and under what circumstances, unless some competing interest or value undermines that presumption.[291] What would it mean to respect a person as a chooser if we refused to respect this basic choice about her own body without any countervailing interests? Nothing would change by specifying that the stranger desires to touch the person to collect tactile information, in order to recommend body wash. The reason for the touch fails to marshal any competing social interest that trumps the person's desire not to be touched. What if the toucher argued that his freedom to touch should trump the touched person's freedom to avoid the touch? Most of us would reject this argument for it so bizarrely departs from current mores: It would then be socially and legally acceptable for a com-

---

288. This exchange will become even cheaper when data structures become standardized, allowing information held in one database to be assimilated seamlessly into another database. *See* PHILIP AGRE, *Introduction to* TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE 15-16 (Philip E. Agre & Marc Rotenberg eds., 1977) (describing the power and value of standardized data models); *see also* NRENAISSANCE COMM., NAT'L RESEARCH COUNCIL, REALIZING THE INFORMATION FUTURE: THE INTERNET AND BEYOND 157 (1994) (noting how data, generated by computers for computers, can be processed and stored easily).

289. These arguments were catalyzed by Judith Jarvis Thomson's claim that if you own something, it is your prerogative not to allow anyone else to view it, subject to some basic realities of social existence. *See* Thomson, *supra* note 22, at 275-76. This goes for widgets, as well as our bodies.

290. *Cf.* Union Pac. Ry. Co. v. Botsford, 141 U.S. 250, 251 (1891) ("No right is held more sacred, or is more carefully guarded, by the common law, than the right of every individual to the possession and control of his own person, free from all restraint or interference of others, unless by clear and unquestionable authority of law.").

291. *See, e.g.*, Bennett v. Norban, 151 A.2d 476, 479 (Pa. 1959) (recognizing a right to bodily sovereignty where a suspected shoplifter was searched by a private individual).

plete stranger to touch an unwilling person—as long as he does not cause physical harm—for any purpose, including sexual gratification.[292]

What is interesting is that the physical "touch" may not be critical to our intuitions. If, through some high-tech glove, someone could collect the same tactile data by waving her hand near my body, my reaction would not change. If some stranger walked up to me on a public street and started moving a strangely gloved hand around my body at one inch distance, which I knew to be physically harmless, I would personally protest, and—what is important—social norms would likely be on my side. To sharpen the point, imagine not a glove requiring close proximity for the collection of data but a sophisticated machine that can do the same work through walls and clothing, from a block away.[293] Moreover, imagine that this machine not only can collect the tactile information, but also can "play it back" so that a "viewer" can himself experience the tactile data, as if he were touching the person's body.[294] The machine would inflict no physical harm upon the person. Indeed, the target may never know that she is being scanned. Now imagine how the person would react if she were told that this machine was aimed at her and that tactile information was being collected invisibly for others' use. She would object vociferously. How would society react? If the machine owner and happy "viewers" complained that their freedom was being infringed, would society perform some balancing test between the competing liberties? Would an economic analysis of efficiency be requested? In my estimation, no. Again, note how we are not talking about the sort of casual touching and bumping, akin to casual observation, that is incident to walking down a busy street.

This "touch" line of argument connects back to my "surveillance" comments through a link suggested by the "machine" hypothetical. Touching is a form of sensory observation. Conversely, if sufficiently intrusive, observation is a form of, or functionally equivalent to, touching. With this link,

---

292. For a disturbing discussion of virtual rapes committed by a character in a Multi-User Domain ("MUD"), see Julian Dibbel, *A Rape in Cyberspace*, VILLAGE VOICE, Dec. 23, 1993, at 36.

293. My science fiction imagination is provoked by the use of thermal imagers to detect marijuana growing operations. A number of courts have considered whether the use of this device, which detects and records the infrared radiation emitted by heat sources, constitutes a "search" within the meaning of the Fourth Amendment. *See* United States v. Cusumano, 67 F.3d 1497 (10th Cir. 1995) (finding that a thermal imaging scan constitutes a "search" under the Fourth Amendment), *vacated* 83 F.3d 1247 (10th Cir. 1996) (upholding probable cause for search without reaching the issue of whether thermal imaging constitutes a "search" requiring a warrant); United States v. Ishmael, 48 F.3d 850 (5th Cir. 1995) (holding that the warrantless use of a thermal imager did not violate the Fourth Amendment); United States v. Myers, 46 F.3d 668 (7th Cir. 1995) (finding that a thermal imaging scan is not a "search" within the meaning of the Fourth Amendment).

294. Authors of futuristic novels have envisioned similar devices. For example, Aldous Huxley anticipated a new form of entertainment called "Feelies," which are similar to movies but perceived by all five senses. *See* ALDOUS HUXLEY, BRAVE NEW WORLD 198-202 (Harper & Row 1946) (1932).

the argument completes: Just as systematic, unwanted touching is in tension with an individual's dignity, so may be systematic, unwanted observation. This is not to say that all information acquisition presents such problems. For example, de minimis collection of personal information does not diminish dignity in worrisome ways. But personal data collection in cyberspace cannot be pooh-poohed as trivial. Sometimes, even full-blown surveillance may be warranted, for instance, in legitimate law enforcement investigation of serious crimes. But in general, some such important public interest must exist to reverse the policy presumption against surveillance. Note how this compelling public interest is generally unavailable to the private sector's acquisition of personal information, in which commercial interests are profit-driven and noncommercial interests are less than compelling.

B. *The Market Unleashed*

Both market and nonmarket talk recommend adopting a default rule that allows personal information collected in the course of a cyberspace transaction to be processed only in functionally necessary ways. With this default rule justified, a comprehensive market solution can be put into effect. But before doing so, we might inquire whether our dignity analysis—in nonmarket terms—advises against adopting the market solution at all. Perhaps taking human dignity seriously requires an outright ban or additional constraints on the exchanges of personal information in the market.

The strongest challenge to the market solution is that "consent" is coerced and not truly voluntary in the marketplace.[295] The fear is that, in the market, an individual confronted with electronic contracts of adhesion will be forced to give up control of personal information, even though she would rather not.[296] For some, this last sentence is unintelligible since the very fact that she made the choice refutes the claim that "she would rather not." But this view fails to recognize that the background circumstances surrounding the choice may argue against respecting or enforcing such "agreements." This critique is the foundation of the venerable doctrines of duress, unconscionability, and the general concerns of unequal bargaining power.[297]

---

295. *See, e.g.*, MILLER, *supra* note 17, at 185-87 (noting that "complex factors" can combine to "subvert the subject's freedom of choice"); Karst, *supra* note 76, at 344-45 (emphasizing the danger of relying on consent); Simitis, *supra* note 76, at 736-37 (arguing that consent "depends entirely on the social and economic context of the individual activity").

296. *See* Froomkin, *supra* note 200, at 492.

297. The coercion problem was not lost on the IITF drafters, who noted specifically that "in certain cases—for example, if the individual lacks sufficient bargaining power—purely contractual arrangements between individuals and information users may fail to respect privacy adequately." IITF PRINCIPLES, *supra* note 19, at 5; *see also id.* at 7. However, the *IITF Principles* neither explain how to identify those "certain cases," nor, more importantly, what to do once those cases are found.

But it is unclear what concrete recommendations flow from this line of reasoning. We could, for instance, adopt an inalienability rule.[298] Just as we cannot sell ourselves into slavery, we could conclude that we should not be able to sell our personal information for what the sale might do to our dignity. This approach would view the right to privacy as less like a property right—which we comfortably peddle away in the marketplace—and more like a civil or human right.[299] But an inalienability rule, as much as it may shore up privacy against private sector attack, risks surrendering control over information privacy to the state.[300] Recall that control is at the heart of information privacy. If the individual wants to exercise that control by disclosing information for various reasons including monetary compensation, then the state should hesitate to proscribe information flow on some parentalistic theory.[301]

Perhaps we could adopt a rule that cyberspace transactions can never be conditioned absolutely on the individual's surrender of information privacy. This solution, however, would not prevent information collectors from taking the next step—charging costly penalties to individuals who would not consent. Although service would not be conditioned formally on privacy surrender, the end result would be the same. In response, we could say that individuals cannot be monetarily penalized for insisting on their privacy, but then information collectors would likely reframe the penalty against privacy zealots as a reward for privacy agnostics. If in frustration, we finally conclude that individuals simply cannot benefit or suffer as a function of their privacy decisions, we have then come full circle back to the inalienability stance, which we have already rejected. For these reasons, a nonmarket, dignity-centered inquiry does not seem to counsel generally against the mar-

---

298. Margaret Jane Radin notes that there are two different meanings of inalienability. Something can be inalienable in the sense that a human right is inalienable, meaning it cannot be "canceled or forfeited." MARGARET JANE RADIN, CONTESTED COMMODITIES 17 (1996). Or something can be inalienable in the sense that it cannot be transferred to another. *See id.* I use "inalienable" in this second sense.

299. The European Union Data Protection Directive states that its goal "is to protect fundamental rights and freedoms, notably the right to privacy, which is recognized both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and in the general principles of Community law." Directive 95/46/EC of the European Parliament and of the Council, 1995 O.J. (L 281), at 31 [hereinafter Directive].

300. Moreover, strict enforcement of an inalienability rule could require the state to engage in substantial surveillance of private interactions, thereby invading individual privacy. *See* Eli Noam, *Privacy and Self-Regulation: Markets for Electronic Privacy*, NTIA REPORT, *supra* note 11, at ch. 1, § B.

301. Parentalistic intervention would be justified, for instance, if individuals systematically overvalued the short-term benefit of disclosing personal information, such as receiving a $0.15 discount on dry pasta at the local grocery store, and undervalued the long-term harm of detailed profiles, such as having recorded one's grocery and household purchases, in addition to one's browsing behavior over a decade. My intuition is that we generally suffer from this evaluative bias, but I have no empirical research to support my intuition.

ket solution. I remain open, however, to claims that certain narrow categories of personal data should be either entirely inalienable or substantially more insulated from market forces.[302] By advocating the market solution, I do not mean to end the discussion or to bar carefully chosen amendments.

We are finally ready to unleash the market. Of course, as the market does its magic, we must keep a watch out for monopoly power. My point here is not to make an empirically justified claim about the distribution of market power in any specific cyberspace sector. Instead, I merely want to raise a general warning based on reasonable fear. Consider, for example, the electronic communication providers that facilitate each transaction through cyberspace. Although competition is on the rise, many electronic communication providers, such as various telephone local exchange carriers or cable television companies, enjoy de jure or de facto monopolies.[303] In addition, the handful of major on-line services seem to be consolidating, with America Online buying out portions of CompuServe. Given that we will not have perfectly competitive markets, we should maintain a skeptical understanding of an individual's "consent"[304] when confronted with limited privacy choices. That means consumer protection laws and venerable contract doctrines such as unconscionability must be applied vigilantly. This is especially true because cyberspace will soon—if it has not already—become integral to modern life. Neither toy nor luxury, cyberspace will soon become as essential to full economic, political, and social membership in the information age as plain old telephone service is today.

IV. A MODEST PROPOSAL

In this final part, I try to implement our accumulated insights into a concrete legislative proposal. At once we see how many details have still been left unexamined. For those impatient for the final work product, please see the Appendix, which features a proposed Cyberspace Privacy Act (the "Act"). It is drafted as a uniform federal law,[305] applicable to the United

---

302. Take, for example, the sale of emergency room medical data to insurance companies and personal injury lawyers. I also believe that individuals should always maintain reasonable rights of access and correction. *See* Appendix § 5(a) *infra*.

303. Historically, most LECs that now provide telephony and will soon provide video carriage have enjoyed monopoly status in their service areas. Cable television operators also often enjoy monopoly status in their local service areas. Advanced interactive networks, which will require significant capital investment, are being constructed mainly by today's LECs and cable operators.

304. *See* MILLER, *supra* note 17, at 185-87 (commenting on "consent and waiver placebos"); Karst, *supra* note 76, at 344-45 (questioning the usefulness of consent).

305. Implementing my proposed Act at the federal level makes sense, given the need for uniformity and the dictates of the dormant commerce clause. *See, e.g.*, American Libraries Ass'n v. Pataki, 969 F. Supp. 160 (S.D.N.Y. 1997) (holding the New York Internet decency law unconstitutional on dormant Commerce Clause grounds).

States.[306] At its heart, the Act implements a default rule for all personal information collected from the individual in the course of executing a cyberspace transaction: Such personal information may be processed in only functionally necessary ways. Parties are, of course, free to contract around the default rule. The Act is heavily annotated to explain my policy judgment and wordsmithing. Decisions that warrant more elaborate defense are addressed below.

A. *Narrowing the Scope: Cyberspace Collection*

As a threshold matter, I have confined the legislation's scope to personal information collected from an individual in the course of executing a cyberspace transaction. In other words, I am bracketing off personal information collected through any means other than a cyberspace transaction, even if the information is subsequently processed by a computer and distributed over networks. Thus, mailing address data, credit ratings, Social Security numbers, whatever sort of personal information—to the extent that they were not originally collected in the course of executing a cyberspace transaction with the individual—lie outside the statute's purview, even if they are later made available, for example, on the Internet. The reasons for this choice can be best understood by my addressing two immediate objections.

First, by excluding personal information collected in real space, am I not arbitrarily treating identically sensitive information differently simply because it originated in a different medium? Why should the same data be treated differently because it was communicated, for instance, through a face-to-face interview instead of a Web page form?

The answer is that the medium affects the message.[307] Recall the distinction I made between surveillance and casual observation. A general law governing the flow of all personal information, regardless of its connection to cyberspace, would constrain too often even casual observation. That is because information collected through real space is comparatively less specific, less computer-processable, less linked to a unique identifier of the individual, and less permanent. The comparison contained in the Introduction between mall visits in real space and cyberspace explored just this differ-

---

306. Like most issues in cyberspace, privacy is a global problem—but one must start somewhere. *Cf.* note 307 *infra*.

307. Recognizing a cyberspace line may also make sense more generally, to govern phenomena that are not be geographically localized, and therefore raise thorny questions about whose law governs. David Post has written most thoughtfully on this point. *See, e.g.*, David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1378-80, 1381 (1996) (arguing that cyberspace should be taken seriously and considered a separate and distinct "place" from real space); David Post, *Governing Cyberspace*, 43 WAYNE L. REV. 155, 159 (1996) ("Cyberspace, however, does not merely weaken the significance of physical location, it destroys it . . . .").

ence. If we were to regulate personal information flows generically in real space, consider what might happen. Suppose I meet Jane at a party and see her wearing a smart silk scarf, which I later note in my spiral notebook. The next day, in conversation with a friend, I mention my having met Jane and relay what she wore. Because I am processing personal information descriptive of Jane, a generic privacy law that knew no cyberspace boundary might apply to what I wrote in my journal and what I said to my friend. But should Jane have control over what is written in my journal even if it does concern her? If she asked me to delete it, I would not feel any obligation, besides courtesy, to obey. A fortiori, I would not vote for a law that would exact my obedience. My guess is that most readers—even privacy Luddites—would agree.[308]

By drawing some cyberspace/real space boundary, we substantially decrease regulation of "casual observation." Of course, the cyberspace/real space boundary is not coterminous with the surveillance/casual observation boundary. Surveillance can and does take place in real space; conversely, casual observation can and does take place in cyberspace. Since my cyberspace proposal does not repeal the privacy laws in real space, I am not wracked by the first point. I accept the statute's lack of comprehensiveness in exchange for limiting its intrusiveness.[309] As for the second, converse point, I carve out from the statute's purview certain cyber-interactions that cannot amount to surveillance.[310]

My response to the first objection thus rests on the claim that cyberspace poses a greater surveillance threat than real space. But this response invites a second objection. Even if one agrees with this claim, one might argue that the surveillance threat arises principally from the computer-processability of

---

308. This intuition can be explained through a triangulation of (1) the individual, (2) the personal information, and (3) the information collector. First, consider the individual. Jane is fully aware of the information that fellow partygoers might collect from her through sight and casual conversation. It should be no surprise to her that people noticed her silk scarf. That is probably the exact reason she wore it—to be noticed. Second, consider the type of personal information acquired. It is different from information collected in cyberspace in four crucial ways: It is relatively impermanent (human memory or journal entry); it is general (information in plain view); it is not immediately computer-processable (handwritten journal entry); and it is not indexed (at least not by a unique identifier such as a Social Security number). Third, consider the information collector. To assert rights over my memory or script is to shackle my observational and mental faculties in offensive ways. In effect, I am told to block my natural senses, such as seeing a silk scarf, to forget my memories, to abstain from recording them, and to muzzle myself with family and friends.

309. Let me not sugarcoat too much. My proposed Act does not govern the substantial "look-up" database industry to the extent that the information was not originally collected in the course of executing, or facilitating the execution of, a cyberspace transaction, as defined within the Act. That industry has recently staved off regulation by Congress and the FTC by adopting a self-regulatory industry code. *See* Katharine Q. Seelye, *A Plan for Database Privacy, but Public Has to Ask for It*, N.Y. TIMES, Dec. 18, 1997, at A1 (describing the voluntary agreement of 14 companies to limit access to the personal data they keep).

310. *See* text accompanying note 361 *infra*.

the underlying data. In other words, once data—however collected—are entered into some computer-readable format, e.g., as a database, spreadsheet, or word processing file, they become searchable, indexable, mergeable, and shareable over computer-mediated networks regardless of the data's origin. And it is this data plasticity and accessibility that pose the central privacy threat. Therefore, the second objection asks, why do I focus on how personal data are collected instead of whether personal data are processed by computers or distributed over networks? Put another way, why not adopt an alternative scope that governs personal data in cyberspace—regardless of how it got there—and leaves real space data alone.

This is a serious alternative. It is, however, impracticable because this cyberspace/real space border cannot be enforced. As a technological matter, information, personal and otherwise, moves freely back and forth across this ephemeral boundary. For example, handwritten notes can be scanned onto a Web page; conversely, Web pages can be printed on paper. Thus, if a law governed only personal data in cyberspace, then an individual would be able to circumvent the law simply by printing the data outside of cyberspace, onto paper. In addition, this alternative invites constitutional challenge. Take, for example, public records. Under this alternative, privacy legislation would leave public records out of cyberspace unrestrained but regulate public records maintained in or distributed through cyberspace. But this differential treatment confronts serious First Amendment objections.[311] My approach avoids these border problems because it does not worry about how the information is distributed or maintained, whether as pits on a compact disc, hypertext mark-up language, or ink on parchment. Instead, it concerns itself solely with how the information was originally collected from the individual, which is a decidedly determinate inquiry. Moreover, it does not institute dual standards for public records in and out of cyberspace. Information collected outside of a cyberspace transaction—whether deemed a public record or not—is not governed by the Act simply because it is moved on line.

Let me be clear. Importing data into cyberspace—even if not originally collected in a cyberspace transaction—raises important privacy concerns. A good example is the Lexis P-TRAK case,[312] which involved the distribution of data, such as Social Security numbers (temporarily) and home addresses, that were likely collected independently of anyone's cyberspace transactions. What made this a "cyberspace" problem was that communication and computing technologies made access to and distribution of this personal infor-

---

311. *See* Cheryl M. Sheinkopf, Comment, *Balancing Free Speech, Privacy and Open Government: Why Government Should Not Restrict the Truthful Reporting of Public Record Information*, 44 UCLA L. REV. 1567, 1568-69 (1997) (arguing that the restriction of "truthful, for-profit reporting of public record information [is] unconstitutional"); *see also* notes332-360 *infra* and accompanying text.

312. *See* note 12 *supra.*

mation easier; the threat did not relate to information collection. Problems such as P-TRAK may be viewed as "first generation" cyberspace privacy problems. They are created when new data analysis and distribution technologies are applied to the sorts of personal information that have long been collected. Make no mistake: These are serious problems. But I am even more concerned about the "second generation" problems that will arise from the collection of cyberspace transactional data. These second generation problems will be even more daunting because the powerful data analysis and distribution technologies that give rise to first generation problems will be applied to data that until now were not collected about the average Jane. Never before in human history did it make any economic sense to do so. Soon, if we do nothing, it will become routine. Fortunately, these second generation problems seem much more amenable to a market solution, which can establish a "terms of trade" for information collection that transacting parties can bargain around through the communicative technologies of cyberspace. Moreover, since this next-generation problem has not yet metastasized, we may be able to intervene surgically in time.

B. *Implementing the Default Rule*

Having explained the statute's scope, I turn to implementing the default rule. To repeat, unless the parties agree otherwise, personal data collected in the course of executing a cyberspace transaction can only be used in ways that are functionally necessary to the successful execution of that transaction. To draft the statute, we need to confront the vagueness inherent in the term "functionally necessary." In this task, we must navigate between two extremes. On the one hand, we must avoid defining the term so narrowly that the individual will be forced to consent expressly to information processing that is obviously incident and necessary to the cyberspace transaction. This would serve no purpose, either in efficiency or dignity terms. From an efficiency standpoint, an unduly restrictive definition would create unnecessary transaction costs without facilitating the disclosure of helpful information. Moreover, an overly narrow definition would not further dignity, which is not especially threatened by the processing of personal information on a need-only basis. On the other hand, we must avoid defining the term so broadly that the information collector effectively has plenary permission to process personal data in whatever ways it finds useful. A lamentable history exists of privacy statutes drafted with good intentions but gaping loopholes.[313] We should resist repeating this mistake.

Between these two extremes, I would identify the following uses as functionally necessary to executing a cyberspace transaction: successful

313. *See, e.g.*, SCHWARTZ & REIDENBERG, *supra* note 18, at 94-100 (discussing the federal 1974 Privacy Act's "routine use" exception).

communication between parties; successful payment and delivery between parties, including accounting and debt collection through independent contractors; successful dispute resolution between parties, e.g., for a defective exchange of information, goods, or services; warnings to the individual of any defect or danger; maintenance of the information collector's cyberspace infrastructure; protection of the collector from fraud and abuse; and adherence to governmental recordkeeping regulations, e.g., those required by tax laws. By contrast, processing of personal information for any form of advertising—even when that advertising is done by the information collector—is not functionally necessary. Disclosing personal information to third parties to do the same would, a fortiori, not be functionally necessary. For my purposes, it is not especially important that the reader agrees with all the details of my judgment. Indeed, the entire task of defining the exact parameters of "functionally necessary" processing could be delegated to an independent agency, such as the Federal Trade Commission or the Federal Communications Commission. I offer my judgment as a starting point for further discussion.

If an information collector seeks to process personal information beyond these identified ways, it must contract around the default rule with the individual.[314] For an agreement to be genuine, a clear and conspicuous[315] offer has to be made. In my view, a small icon at the bottom of a Web page would not suffice. By contrast, a click-through dialog box with some meaningful information—not some overly general disclaimer—may suffice. Thereafter, if information is processed in a way inconsistent with this agreement, then the information collector must be subject to sanction through civil action in federal court and administrative enforcement by the Federal Trade Commission.[316]

---

314. There is no special exemption for employers who collect personal information in the course of facilitating an employee's cyberspace transaction. Of course, an employer's need to collect limited information to protect against fraud and abuse of its network may be "functionally necessary" within the meaning of section 2(12) of my Act. *See* Appendix § 2(12) *infra*. Further, an employer often will have substantial leverage in garnering consent from the employee to process personal information in functionally unnecessary ways. *See id.* § 4. For a discussion of employee privacy, see Kim, *supra* note 231, at 698-709.

315. A "clear and conspicuous" standard appears throughout the federal code. *See, e.g.*, 11 U.S.C. § 524 (1994) (part of the Bankruptcy Code); 15 U.S.C. § 1602 (1994) (the Truth in Lending Act); 42 U.S.C. § 7671(j) (1994) (part of the Stratospheric Ozone Protection statute). More on point, this phrase is used in the 1984 Cable Act, which requires a cable operator to inform the subscriber "clearly and conspicuously" about its privacy policies. *See* Cable Communications Policy Act of 1984, 47 U.S.C. § 551(a)(1) (1991). "Clear and conspicuous" means meaningful notice, reasonably understandable to the subscriber. *See* Scofield v. TeleCable of Overland Park, Inc., 973 F.2d 874, 879-80 (10th Cir. 1992) (defining "clear and conspicuous" under the Truth in Lending Act as a "common sense approach").

316. Agency enforcement is necessary because individuals may not know when or by whom their privacy has been violated. Uncovering these facts may require the investigative resources of an enforcement agency. As an aside, the question of enforcement raises another round of theoreti-

Here, it is useful to clarify the connection between personal information exchanged in primary and secondary markets. By "primary market" I mean information collected directly from the individual in the course of a cyberspace transaction. "Secondary market" refers to subsequent information exchanges between two information users, without any direct involvement of the individual.[317] It is crucial to note that personal information cannot generally be exchanged in a secondary market, for it is generally a functionally unnecessary use, unless the individual and the original information collector in the primary market expressly agreed to do so.[318] Moreover, that contract could be drafted so that personal information could not be disclosed to third parties in the secondary market unless those third parties contractually agreed to some sort of processing limitation. If a third party then broke its promise to the original information collector, then the individual would have grounds to sue the third party on an intended beneficiary-like basis.[319]

C. *Mustering Political Support*

Politically moderate, the proposed legislation should enjoy broad appeal. First, it should be attractive to Congress. As a policy matter, this Act should be viewed as a natural extension of the privacy provisions of the Cable Communications Policy Act (the "Cable Act") passed in 1984. The legislative history of that section reveals that Congress was especially concerned

---

cal complexity regarding whether entitlements should be protected by "liability" or "property" rules. *See, e.g.*, Ian Ayres & J.M. Balkin, *Legal Entitlements As Auctions: Property Rules, Liability Rules, and Beyond*, 106 YALE L.J. 703 (1996); Ian Ayres & Eric Talley, *Solomonic Bargaining: Dividing a Legal Entitlement to Facilitate Coasean Trade*, 104 YALE L.J. 1027 (1995); Calabresi & Melamed, *supra* note 243, at 1089; Louis Kaplow & Steven Shavell, *Property Rules Versus Liability Rules: An Economic Analysis*, 109 HARV. L. REV. 713 (1996). I do not discuss these complexities; however, I do note that, given the proposed Act's penalty structure, I am protecting privacy through a "property" rule. *See* Ayres & Balkin, *supra*, at 705 ("Property rules set the exercise price so high that no one is likely to exercise the option to take nonconsensually, while the lower exercise prices of liability rules presuppose that some people will take nonconsensually."). Note that property rules fully protect subjective valuations; accordingly, privacy zealots will have their interests as well protected as privacy agnostics.

317. *See* FEDERAL RESERVE REPORT, *supra* note 84, at 10 (making the same distinction between primary and secondary information markets); Patricia Mell, *Seeking Shade in a Land of Perpetual Sunlight: Privacy As Property in the Electronic Wilderness*, 11 BERKELEY TECH. L.J. 1, 5-6 (1996) (noting that primary information markets involve voluntary disclosure, whereas secondary markets may involve uses "which the individual could not have foreseen").

318. The drafters of the IITF have addressed this concern:

> Inherent in this [Fairness] principle is the requirement that whenever personal information is transferred from information user to user, the individual's understanding of how that personal information will be used must also be conveyed. Because all information users must abide by the Fairness principle, both information transferor and transferee bear a responsibility to ensure that the individual's understanding is transferred along with the information.

IITF PRINCIPLES, *supra* note 19, at 9.

319. For my attempt to address the bona fide purchaser complication, see Appendix § 4(b) *infra*.

with interactive, or "two-way," cable systems.[320] This is in fact what cyberspace provides—interactive communications of increasing bandwidth. It makes sense to extend the policy judgment reflected in the Cable Act to cyberspace, which poses the same threat that originally concerned Congress. As a political matter, surveys—for what they are worth—suggest that legislation to protect cyberspace privacy would be wildly popular.[321]

Second, the Act should be attractive to the executive branch since it is a concrete and faithful implementation of the hortatory *IITF Principles*. A review of these principles reveals that at their crux stand the Notice and Fairness Principles. The Notice Principle requires information collectors to provide individuals with sufficient information for them to exercise sound judgment about their privacy.[322] The Fairness Principle requires information users "not [to] use personal information in ways that are incompatible with the *individual's understanding* of how it will be used, unless there is a compelling public interest for such use."[323] Elsewhere I have explained how the Notice and Fairness Principles—which are cardinal to fair information practices generally[324]—implement a contractual approach to protecting personal

---

320. *See* H.R. REP. NO. 98-934, at 29 (1984), *reprinted in* 1984 U.S.C.C.A.N. 4655, 4666. It states:

> Cable systems, particularly those with a 'two-way' capability, have an enormous capacity to collect and store personally identifiable information about each cable subscriber. Subscriber records from interactive systems can reveal details about bank transactions, shopping habits, political contributions, viewing habits and other significant personal decisions.

Id.

321. *See* P&AB SURVEY, *supra* note 264, at 59 (reporting that when respondents were provided three choices—(1) legislation now, (2) government recommended privacy standards, or (3) voluntary guidelines—58% chose (1), 24% chose (2), and only 15% chose (3)); note 12 *supra* (compiling similar results from other surveys).

322. It states:

> Information users who collect personal information directly from the individual should provide adequate, relevant information about:
>
> 1. Why they are collecting the information;
>
> 2. What the information is expected to be used for;
>
> 3. What steps will be taken to protect its confidentiality, integrity, and quality;
>
> 4. The consequences of providing or withholding information; and
>
> 5. Any rights of redress.

IITF PRINCIPLES, *supra* note 19, at 7-8.

323. *Id.* at 9 (emphasis added).

324. For an analogue to the Notice Principle, see Organization for Economic Co-operation and Development: Council Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, Sept. 23, 1980, 20 I.L.M. 422, 424, *reprinted in Data Protection, Computers, and Changing Information Practices: Hearing Before the Gov't Info., Justice, and Agric. Subcomm., House Comm. on Gov't Operations*, 101st Cong. (1990) [hereinafter Privacy Guidelines] ("The purposes for which personal data are collected should be specified not later than at the time of data collection . . . .").

For analogues to the Fairness Principle, see HEW REPORT, *supra* note 20, at xx ("[T]here must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent."); Privacy Guidelines,

information.[325] The *IITF Principles* recognize, however, that this is a stylized description of cyberspace transactions; for instance, explicit notices before information processing will not always be feasible or useful.[326] Accordingly, "the individual's understanding" of how personal information will be processed will often be unclear.[327] A clear default rule is necessary to specify more precisely what that understanding is until the parties agree otherwise. This, the Act provides.

Third, the average cyberspace participant, who incidentally collects personal information, need not fear any burden. As an example, consider an individual who puts up a home page on the Web through an Internet Service Provider and collects no personal information about those who browse her site. Under the Act, the individual would not have to do anything until queried, at which time she would have to respond in some convenient and reasonable manner that she collects no personal information through her home page. For practical reasons, Congress could also deem even the collection of standard Web server statistics to be functionally necessary as long as that

---

supra note 324, at 425 ("Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with [the Purpose Specification Principle] except: (a) with the consent of the data subject; or (b) by the authority of law . . . .").

325. *See* NTIA WHITEPAPER, *supra* note 19, at 20-27. The Notice Principle requires information collectors to tell individuals what personal information will be collected and how it will be used. In contract law parlance, this notice resembles an offer. By going through with the transaction, the individual can be said to accept the offer. The Fairness Principle then requires the information collector to abide by the terms of the contract. Thus, for any cyberspace transaction, one can say that two offers are in play: (1) the main offer regarding the widget, program, or information being exchanged; and (2) the auxiliary offer, often implicit, concerning the flow of personal information.

326. *See* IITF PRINCIPLES, *supra* note 19, at 8 ("What counts as adequate, relevant information to satisfy the Notice Principle depends on the circumstances surrounding the collection of information. . . . In some cases, the ordinary and acknowledged use of personal information is so clearly contemplated by the individual that providing formal notice is not necessary.").

327. The *IITF Principles* try to finesse this issue by relying on "the individual's objectively reasonable contemplation and scope of consent when the information was collected." IITF PRINCIPLES, *supra* note 19, at 9. But this language provides little guidance. The individual's "objectively reasonable contemplation" invites interpretation according to the doctrinally elaborated "legitimate expectation" standard of Fourth Amendment jurisprudence. The Fourth Amendment protects only legitimate expectations of privacy, which requires (1) a subjectively held expectation of privacy that (2) society finds objectively reasonable. *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). But this analogy has critical limits. An individual's "objectively reasonable contemplation" regarding a particular transaction need not be an expectation of privacy that society would find objectively reasonable in a general sense An example will clarify. Under *United States v. Miller*, 425 U.S. 435 (1976), a bank depositor has no "legitimate expectation of privacy" over records of cleared checks and deposit slips. *Id.* at 442-43. However, if a bank promised its customers that it would keep such information confidential, then it would be within an individual's "objectively reasonable contemplation" that the information would not be disclosed.

data is not used to target potential consumers who are unrelated to the transaction.[328]

Fourth, the private sector should not oppose the Act if its recent privacy proclamations are genuine. The Act's underlying principles do not differ materially from, for instance, the Open Profiling Standard ("OPS"), which Netscape, Microsoft, and Firefly have proposed.[329] The Act is also consistent with important aspects of the recently adopted Information Technology Industry Council's privacy principles.[330] Moreover, the "terms of trade" established by the default rule in no way choke off electronic commerce in cyberspace. The Act does apply brakes to certain forms of unusually detailed data collection, sophisticated database mining, and the sharing of personal information with third parties, but these brakes can be released simply by obtaining the consent of the customer. Moreover, express federal privacy protections would promote consumer confidence in—and thereby encourage—electronic commerce. Finally, multinational corporations working in Europe might have an independent reason to accept the Act. By applying the Act to data received from the European Union, these corporations could credibly assert that they have begun to adopt "adequate" privacy protections

---

328. Standard Web logs record identity information—e.g., the IP address and domain name if looked up, the username if the user is authenticated, the login name if the identd program is running on both client and server—the time and date of the request, the URL of the requested resource, the byte length of the resource, the referer variable, and the user-agent variable. *See* text accompanying notes 125-167 *supra*. I believe it is not unreasonable to consider the collection of this information as functionally necessary to maintain the information collector's cyberspace infrastructure and to improve Web content. I come to this conclusion with some regret in part out of pragmatic necessity: To conclude otherwise would require the reprogramming of tens of thousands of servers currently in existence. The resistance to such an approach would be substantial. This demonstrates nicely how technology developing without considered policy guidance can create conditions that make future reconsideration either impossible or limited. However, I would draw the line here. For instance, I would consider it functionally unnecessary to collect client e-mail addresses blanketly if offered in the request-header. To clarify further, just because these logs can be collected does not mean that they can be disclosed or used any way that the information collector desires.

329. OPS is a uniform data template for individuals to provide personal profiles to transacting parties on the Internet. An individual has complete control over her own OPS profile, which means that she can make it as detailed or as incomplete as she wishes. A Web site supporting OPS will request information from the individual's Personal Profile upon her first visit. The user can control the extent to which her information is released. The OPS standard is guided by three principles—informed consent, value exchange, and control by source—which are entirely consistent with the Act. *See* MICROSOFT CORP., *Firefly, Netscape and Microsoft Cooperate to Build Upon Previously Proposed OPS Standard for Personalization with Privacy* (visited June 20, 1997) <http://www.microsoft.com/cor-pinfo/press/1997/Jun97/firfly2.htm>).

330. *See* INFORMATION TECHNOLOGY INDUSTRY COUNCIL, *The Protection of Personal Data in Electronic Commerce* (visited Dec. 9, 1997) <http://www.itic.org/pp_privprin.html> ("At the time of collection of personal data, collectors and users should furnish individuals with information on the intended use of such data and with mechanisms permitting the exercise of choice on its disclosure.").

necessary to maintain transborder flows under the recent European Union data protection directive.[331]

D. *A Final Objection: The First Amendment*

While the Act may please the more political branches of government, will it satisfy the judiciary? An obvious tension exists between information privacy and unconstrained speech. One need not be a free speech diehard to bristle at the thought of giving the individual complete control over the disclosure of her personal information.[332] Does the Cyberspace Privacy Act, then, pass First Amendment muster?[333] To focus our discussion, imagine the following controversy. A cyberspace merchant collects detailed data of every consumer who visits her cyber-store. The merchant would like to sell that information to a direct marketer. Since the sale is not "functionally necessary," the Cyberspace Privacy Act requires the merchant to have the individual's express consent to the data transfer. The merchant sues to strike down the statute as an unconstitutional restraint on the transmission of truthful information.

1. *The* Florida Star *challenge.*

Central to the merchant's argument would be *Florida Star v. B.J.F.*,[334] in which the Supreme Court held that if personal information is truthful, lawfully acquired, and of public interest, it may be disclosed absent a state interest of the highest order.[335] In *Florida Star*, a newspaper obtained a rape victim's name from an inadvertently released police report.[336] Although state law prohibited such a release, the Court concluded that the information was

---

331. The European Union Data Protection Directive allows the sending of personal information only to countries with "adequate" privacy protection, which is to be determined contextually and on a case-by-case basis. *See* Directive, *supra* note 299, § 25(2). A detailed but highly readable explanation of the Directive's impact can be found in Swire & Litan, *supra* note 154.

332. "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." Jerry Kang, *A Privacy Primer for Policy Makers*, 1 UCLA BULL. L. & TECH. 3 (Jan. 23, 1996) <http://www.law.ucla.edu/Student/Organizations/BLT> (written testimony by Jerry Kang before the FTC hearings on the FTC's consumer protection role in the emerging high-tech, global marketplace).

333. What follows is a strictly doctrinal defense of the constitutionality of the proposed Act. It does not explore the complicated philosophical or doctrinal interrelations between privacy and the First Amendment. For such approaches, see generally Gormley, *supra* note 24; Sean M. Scott, *The Hidden First Amendment Values of Privacy*, 71 WASH. L. REV. 683 (1996).

334. 491 U.S. 524 (1989).

335. *See id.* at 533 (citing Smith v. Daily Mail Publ'g Co., 443 U.S. 97, 103 (1979)).

336. 491 U.S. at 527.

still lawfully received.[337] Because it was so received, accurate, and of public interest, the Court concluded that strict scrutiny was warranted and that subsequent disclosure of the information through publication was constitutionally protected.[338] Invoking this holding, the cyber-merchant would argue that the information it seeks to disseminate is truthful, of public interest, and lawfully acquired; therefore, strict scrutiny is warranted. With rhetorical force, the merchant would add that if information as sensitive as being raped can be disclosed, then surely so can transactional records of cyber-purchases.[339]

I have two responses, one internal to *Florida Star*'s own logic, the other external. First, in distilling the doctrinal principle applied in the case—what the Court called the *Daily Mail* principle—the Court emphasized that the information had to be lawfully acquired."[340] The Court noted that through

---

337. An incident report identifying B.J.F. by her full name was placed in the Sheriff's Department pressroom. A *Florida Star* reporter-trainee subsequently copied the police report verbatim. *See id.* at 527. The Court reasoned that these events constituted lawful acquisition. *See id.* at 538-39. Justice White, in dissent, argued that the information was not "lawfully" received and noted that signs in the very room where the police reports were made available stated that the names of rape victims were not to be published. *See id.* at 546 (White, J., dissenting).

338. *See* 491 U.S. at 533.

339. The merchant is not engaged in commercial speech simply because it is selling information to turn a buck. Commercial speech is speech that does "no more than propose a commercial transaction." Pittsburgh Press Co. v. Pittsburgh Comm'n on Human Relations, 413 U.S. 376, 384 (1973). For a devastating critique of the commercial speech doctrine, see Alex Kozinski & Stuart Banner, *Who's Afraid of Commercial Speech?*, 76 VA. L. REV. 627 (1990).

340. *See* 491 U.S. at 533.

The seminal antecedent of *Florida Star* is *Cox Broad. Corp. v. Cohn*, 420 U.S. 469 (1975). In *Cox*, a state statute created a cause of action against anyone who published the name of a sexual assault victim. The father of a deceased rape victim sued a television station for reporting the victim's name, which had been obtained lawfully from judicial records available for public inspection. Striking down the statute, the Supreme Court held that a state may not impose liability for disseminating true information of public interest, derived from public court records. *See id.* at 496. If privacy interests must be protected, the state must do so by not making the information available to the public in the first place. *See id.*; *see also* Landmark Communications v. Virginia, 435 U.S. 829 (1978); Oklahoma Publ'g Co. v. Oklahoma County Dist. Court, 430 U.S. 308, 310-11 (1977).

In *Landmark*, state law imposed criminal sanctions for the breach of confidentiality of certain judicial misconduct proceedings. Nonetheless, once a newspaper received such confidential information, the state could not penalize its publication. *See Landmark*, 435 U.S. at 843-45. In *Oklahoma*, the Supreme Court held that a state could not enjoin the media from publishing a youth's name in connection with a juvenile proceeding that reporters had attended. Consistent with the reasoning in *Cox*, the Court explained that because the reporters were lawfully present at the proceedings, they could not be punished for publishing what they saw. *See Oklahoma*, 430 U.S. at 310-11.

The public record privilege was distilled into a more precise principle in *Smith v. Daily Mail Publ'g Co.*, 443 U.S. 97 (1979). In *Daily Mail*, a newspaper obtained the name of a juvenile suspect by lawfully monitoring a police radio frequency and by questioning witnesses, the police and the local prosecutor. *See id.* at 99. The newspaper then published the juvenile's name in violation of a state statute prohibiting such publication without prior court authorization. *See id.* The Court held the statue invalid: "[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." *Id.* at 103. In other words, once

this requirement, "the government retains ample means of safeguarding significant interests upon which publication may impinge, including protecting a rape victim's anonymity."[341] In particular, "[t]o the extent sensitive information rests in private hands, the government may under some circumstances forbid its nonconsensual acquisition, thereby bringing outside of the Daily Mail principle the publication of any information so acquired."[342] This language suggests one way to ensure an adequate level of privacy without running afoul of the First Amendment: Establish clear, enforceable rules delineating what counts as legitimate information acquisition through cyberspace. This is precisely what the proposed Act does. Unauthorized acquisition through cyberspace would be akin to theft of property, property that happens to be information about the individual.[343] Thus, it would be information "unlawfully obtained" and therefore outside the scope of the *Florida Star* line of cases.[344]

Unfortunately, this response has critical weaknesses. The Court has been exceedingly generous in deciding what is "lawfully obtained." In *Florida Star* itself, the State of Florida had passed a law removing the name of rape victims from public records, had passed a statute forbidding the dissemination of such information through instruments of mass communication, and had posted clear signs in the police department briefing room that such information was not to be recorded and distributed.[345] The newspaper got hold of the information knowing, at least constructively, that but for the police department's negligence, it would not have received the data.[346] Still, the

---

truthful information of public significance is publicly revealed, its dissemination cannot be restrained without a compelling interest.

341. *Florida Star*, 491 U.S. at 543.

342. *Id.* at 534.

343. Diane Zimmerman notes that as a matter of positive law, conceptualizing information as property tends to neutralize First Amendment arguments in favor of unrestricted dissemination. *See* Diane Leenheer Zimmerman, *Information As Speech, Information As Goods: Some Thoughts on Marketplaces and the Bill of Rights*, 33 WM. & MARY L. REV. 665, 665-72 (1992). As a normative matter, Zimmerman is disturbed by this doctrinal trend.

344. One could try to distinguish *Florida Star* by claiming that the information collector, at least in the primary market, acquired the personal data lawfully and merely disclosed it or used it unlawfully. But if information is obtained in accordance with a law that itself restricts the further disclosure and use of that information, then the First Amendment will not necessarily bar the enforcement of those restrictions. *See* Seattle Times Co. v. Rhinehart, 467 U.S. 20, 37 (1984) (applying intermediate scrutiny and enforcing restrictions on information obtained through discovery order that explicitly prohibited publication); FEC v. International Funding Inst., Inc., 969 F.2d 1110 (D.C. Cir. 1992) (validating the Federal Election Campaign Act's prohibition of commercial sale of contributor lists that must be made public). Of course, in both *Seattle Times* and *International Funding Institute*, the state compelled the initial disclosure of information to the opposing party through discovery and to the FEC.

345. *See Florida Star*, 491 U.S. at 526, 536, 546.

346. *See id.* at 546 (White, J., dissenting) (referring to the reporter's admission that she knew she was not permitted to record the rape victim's name).

majority characterized this information as "lawfully obtained."[347] In addition, it seems likely that the "law" in "lawfully obtained" was meant to apply only to laws like trespass, which are not targeted at the communicative impact of speech. Otherwise, Congress could pass a law that makes it unlawful, for example, to acquire highly intrusive information about the President's personal life. Surely this could not have been what the majority in *Florida Star* had in mind.[348]

So, I move to my second response, external to *Florida Star*'s own logic, found in *Cohen v. Cowles Media Co.*[349] In the hoary tradition of political mudslinging, Cohen offered juicy tidbits of information to two newspapers about a political opponent on the condition of source confidentiality.[350] When the tidbits turned out be less newsworthy than first appeared, the newspapers felt the more tantalizing story to be Cohen's squealing to the press.[351] Cohen sued for fraudulent misrepresentation and breach of contract, won at trial, but ultimately lost on First Amendment grounds in the state supreme court.[352]

In the U.S. Supreme Court, the newspapers raised the *Florida Star* defense: Since the information about Cohen was truthful, lawfully obtained, and of public interest, the First Amendment would not countenance liability.[353] The majority, however, was not so certain that the information had been lawfully obtained, at least for the purposes of publication.[354] More importantly, the Court did not find the *Florida Star* line of cases to be on point. It found more relevant a different line of cases standing for the proposition

---

347. *Id.* at 536.

348. Another possible argument, internal to *Florida Star*'s logic, would be that the personal data are solely of private concern, rather than of "public interest." But this would be a losing argument. First, while the Court in *Florida Star* at times emphasized the "public interest" requirement, it did not include the prong in its final statement of the holding. *See Florida Star*, 491 U.S. at 541. Second, courts generally interpret the terms "of public significance" and "newsworthiness" broadly. *See id.* at 536-37 (gauging public significance by looking at the subject matter of the article, not the specific personal information). It would not take much imagination to characterize information about what individuals are doing in cyberspace as a matter of public interest. For commentary lamenting the inchoate quality of "newsworthiness," see Joseph Elford, Note, *Trafficking in Stolen Information: A "Hierarchy of Rights" Approach to the Private Facts Tort*, 105 YALE L.J. 727, 733-37 (1995) (discussing inconsistencies in the application of the "newsworthiness" standard), and Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CAL. L. REV. 957, 995-1006 (1989) (discussing the difficulty of defining "legitimate public interest").

349. 501 U.S. 663 (1991).

350. *See id.* at 665.

351. *See id.* at 665-66.

352. *See id.* at 665-67.

353. *See id.* at 668-69.

354. *See id.* at 671 ("Unlike the situation in *Florida Star*, where the rape victim's name was obtained through lawful access to a police report, respondents obtained Cohen's name only by making a promise that they did not honor.").

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."[355] In the Court's opinion, the application of standard promissory estoppel law to the newspapers did not raise any First Amendment obstacles.

In explaining why it chose the "general applicability" line of cases over the *Florida Star* line of cases, the Court noted that in the latter,

> the State itself defined the content of publications that would trigger liability. Here, by contrast, Minnesota law simply requires those making promises to keep them. The parties themselves . . . determine the scope of their legal obligations, and any restrictions that may be placed on the publication of truthful information are self-imposed.[356]

This is exactly what the proposed Act does.

Although the Act provides a default rule, the rule is mutable—not only in theory, but also in practice. Thus, the parties themselves ultimately determine their legally enforceable obligations. In other words, the central function of the Act is to facilitate clear contracting between individuals and information users. To be sure, that contract is then enforced through state machinery, but that is precisely what took place in *Cohen*.[357] Moreover, this default rule does not somehow compel parties to speak—to flip out of the default rule—in some constitutionally problematic way. All default rules operate this way. Consider, for example, the default rule that compels an offeror to utter an "offer" in a particular manner—with sufficient clarity, detail, and sometimes in writing—before a contract may be created through "acceptance." As another example, consider implied warranties that may be disclaimed.

My purpose here is not to defend either *Cohen* or *Florida Star*.[358] Nor is it to discuss the complicated interrelations between the values undergirding

---

355. *Id.* at 669 (collecting numerous examples of generally applicable rules applied to information collection and disclosure). For an argument that the Court should have applied the *Florida Star* line of cases, see Jeffery A. Richards, Note, *Confidentially Speaking: Protecting the Press from Liability for Broken Confidentiality Promises*—Cohen v. Cowles Media Co., 111 S. Ct. 2513 (1991), 67 WASH. L. REV. 501, 510 (1992).

356. 501 U.S. at 670-71.

357. One of the concerns in *Cohen* was that a law of general applicability would be used to circumvent the "actual malice" defamation standard. *See id.* This is precisely what Jerry Falwell tried to do when he invoked the generally applicable tort of intentional infliction of emotional distress in his case against *Hustler*. *See* Hustler Magazine, Inc. v. Falwell, 485 U.S. 46 (1988). But the Court made clear in *Cohen* that maintaining the defamation standard was simply not at issue. The same is true of the proposed Act, which has nothing to do with defamation and in no way circumvents the "actual malice" defamation standard.

358. For instance, I agree with Peter Edelman's critique that the majority in *Florida Star* was being formalistic in concluding that the information was lawfully obtained. *See* Peter B. Edelman, *Free Press v. Privacy: Haunted by the Ghost of Justice Black*, 68 TEX. L. REV. 1195, 1203 (1990). Also, in the final summary of its holding, the Court neglected to mention the public significance requirement. Instead, it spoke only of lawful acquisition of truthful information. *See* Florida Star v.

privacy and freedom of expression,[359] such as the obvious connection between information privacy and the ability to engage in unpopular expressive activity. Instead, my purpose is to argue narrowly, staying close to the surface, that as a matter of current positive constitutional law, the proposed Act passes scrutiny. For those who remain skeptical, consider the fact that from a First Amendment perspective, the proposed Act does not differ materially from the privacy provisions of the Cable Act or the Video Privacy Protection Act. Neither act has been successfully challenged on First Amendment grounds. For those who wonder about the prudence of letting "freedom of contract" be the talismanic answer to First Amendment worries, consider that this talisman works its magic on both sides of the cyberspace transaction. Here, we are concerned that contract undermines the information collector's freedom of expression, but, just above, we were concerned that contract undermines the individual's dignity. There is symmetry, if not justice.[360]

B.J.F, 491 U.S. 524, 541 (1989) ("We hold only that where a newspaper publishes truthful information which it has lawfully obtained, punishment may lawfully be imposed, if at all, only when narrowly tailored to a state interest of the highest order . . . ."); Edelman, *supra*, at 1223 n.147 (noting the Court's omission). If this was anything other than carelessness, then the Court is inviting some odd results. Consider, for instance, the "Marilyn Monroe case," in which a woman's skirt was unexpectedly blown upward in a county fair and captured on film. *See* Daily Times Democrat v. Graham, 162 So. 2d 474 (Ala. 1964). Although the photographer acquired the "information" lawfully in plain view, should the press have a right to distribute it in anyway it wants? *See id.* at 476-77 (answering in the negative by holding that the photograph had no legitimate news value and violated the plaintiff's right to privacy); Edelman, *supra*, at 1205 n.60 (arguing that the capture of this brief, albeit public, occurrence on film transformed a few seconds of embarrassment into an event that thousands of people could share and remember).

359. For articles that discuss these interrelations, see, for example, Edward J. Bloustein, *The First Amendment and Privacy: The Supreme Court Justice and the Philosopher*, 28 RUTGERS L. REV. 41 (1974); Bloustein, *supra* note 54.

360. The merchant might also raise a Fifth Amendment takings argument—that the default rule somehow takes away its property—personal data—without just compensation. Of course, this begs the essential question of who owns the personal data in the first place. Moreover, this would be a weak argument under Supreme Court precedent. In *Rowan v. United States Post Office*, 397 U.S. 728 (1970), the Court addressed a statute that allowed an individual, at her sole discretion, to determine that certain mailing advertisements were sexually offensive and thus unwelcome. At the request of the individual, the mailer was required to stop future mailings and to remove the individual's name from all mailing lists. The Court wrote:

> The appellants also contend that the requirement that the sender remove the addressee's name from all mailing lists in his possession violates the Fifth Amendment because it constitutes a taking without due process of law. The appellants are not prohibited from using, selling, or exchanging their mailing lists; they are simply required to delete the names of the complaining addressees from the lists and cease all mailings to those persons.
>
> Appellants next contend that compliance with the statute is confiscatory because the costs attending removal of the names are prohibitive. We agree with the conclusion of the District Court that the "burden does not amount to a violation of due process guaranteed by the Fifth Amendment of the Constitution. Particularly when in the context presently before this Court it is being applied to commercial enterprises."

Id. at 740.

2. *Second thoughts.*

Even if the Act passes First Amendment scrutiny, let me address one final free expression concern as a matter of prudence. A principal reason why I limit the Act to cyberspace versus real space data collection is to avoid governing casual observation as in the silk scarf party hypothetical. But the cyberspace line is not perfectly tailored; many examples of information collection through cyberspace cannot be considered akin to surveillance. To see why, consider two more hypotheticals. First, imagine that I am a designer who teaches at a fashion institute. Jane, the friend of a student, sends me an e-mail asking me what might match her silk scarf. I suggest, cleverly, a silk jacket. Over dinner, I relay the gist of this e-mail exchange to my partner. Should the Act constrain what I said over dinner? My intuition is no. If I talk too much, in too great detail, I should be shunned as a gossip or bore; that does not mean, however, that I should be held legally liable for violating a privacy statute. Second, imagine that Jane posts the same fashion question to a Usenet newsgroup. I am a silk clothing retailer who responds directly to Jane's e-mail address, inviting her to visit my store for a nice silk jacket on sale. I also record Jane's name and e-mail address in my mailing list. This personal information was acquired through cyberspace. Yet, again, I am uneasy about applying privacy restrictions on this information because of the way the data were collected. To be sure, they were collected through cyberspace, but through a forum intentionally designated as a public place in which untold numbers of people have access to the messages posted.

Part of what underlies these intuitions is the degree to which the information collector's communicative liberties are unduly constrained when competing concerns of surveillance are minimal. The information collector can hardly be faulted for reading and responding to a message that was sent to her if the message was part of some noncommercial exchange of mail. Similarly, the collector cannot be faulted for reading and responding to a message expressly posted for public consumption. To constrain the reader in this context from recording or sharing this information would, in my view, amount to an unwarranted burdening of her free expression values.

Since the cyberspace/real space distinction is too blunt, I would sharpen it by excluding any portion of a message from an individual either to an individual in a noncommercial context[361] or to a publicly accessible forum. By

361. Messages sent to individuals in a "noncommercial context" pose a low surveillance threat. By contrast, constraining what we do with these messages exacts a high cost on free expression. I add the "noncommercial context" restriction because otherwise firms would invite e-mails from the unsuspecting public with the purpose of developing prospect mailing lists. Low-tech versions of this marketing strategy are already prevalent:

> [H]alf a million viewers in 16 states called a toll-free number on a TV commercial to find out the pollen count in their zip-code area. As a result . . . many callers received sales pitches for allergy medicine from Warner Lambert, the ad's sponsor. Using a similar approach, Johnson

"message," I mean an electronic communication authored by an individual with the intent that it be delivered to someone, not the sort of transactional information released automatically by an individual's computer in the course of Web browsing.

This fix has the bonus of avoiding interference with the cyberspace copyright debate. Since work I create can be personal information in the authorship sense, the flow of this work can theoretically be governed under privacy law as much as copyright law. Accordingly, even if a retransmission of personal information would be fair use under copyright law, it could conceivably be unfair under privacy law. Note how the message-to-publicly-accessible-forum exception prevents this overlap and keeps privacy law from interfering with copyright law. This can be seen by answering the following question: When a person puts up an essay on a Web page, does it violate the proposed Act for me to download it and distribute copies to others? At first glance, the Act seems to apply because (1) the article is personal information that is (2) collected through a cyberspace transaction. However, because the essay is a message from the author to a publicly accessible forum, it falls outside of the definition of a "cyberspace transaction." Therefore, the legality of making copies would be left to copyright law.

CONCLUSION

Technology effects change. It changes individual and institutional possibilities. It alters our culture, economics, and politics. The new communications technologies are transforming our society, propelling us further into the Information Age.[362] And as we accelerate into this new era, we slam into new problems or old ones that have morphed into unrecognizable shapes. One such problem is information privacy, which the coming cyberspace threatens.

Fundamentally this entire article has been an exercise in setting a new "reasonable" expectation of privacy for the evolving techno-cultural regime, augured by the new information infrastructure. The distinctions I have made along the way—cyberspace versus real space, data collection versus processing and distribution, functionally unnecessary versus functionally necessary—can be viewed as increasingly finer judgments on where to draw the line marking an appropriate amount of privacy. The relevance and persua-

---

& Johnson compiled a list of 4.5 million women with incontinence who responded to an ad for its Serenity undergarments

Who's Reading Your Medical Records?, CONSUMER REP., Oct. 1994, at 628, 631.

362. *See* Agenda for Action, *supra* note 1, at 49,026 ("[T]wo-thirds of U.S. workers are in information-related jobs."); *see also* Steve Lohr, *Information Technology Field Is Rated Largest U.S. Industry*, N.Y. TIMES, Nov. 18, 1997, at D5 (describing a study based on Commerce Department data that concludes that information technology is the nation's largest industry, ahead of construction, food products, and automobile manufacturing).

siveness of these distinctions—for example, my judgment calls on what counts as surveillance and what counts as casual observation—are technologically and culturally contingent. One can easily imagine another society with a different past and a different technology that would reach radically different conclusions. The fact that these judgments are deeply contingent does not, however, excuse inaction. As a society, we cannot avoid taking some position, for the status quo itself is a position. Moreover, whatever choices we make today based on today's values will remake what our values look like tomorrow.

The proposed Act is a good place to begin a focused discussion on the privacy choices we must make. By probing its ambiguities and its unintended consequences, we can make improvements in order to reach the best possible solutions within current political constraints. Some will complain that the Act goes too far, but it is in fact quite limited in scope and humble in its ambitions. Indeed, as privacy advocates will no doubt flag, good reasons exist to wonder whether a market solution that embraces a disclosure regime will be fully up to the task. Notices may not be sufficiently concise and informative for individuals to read and understand the complicated ways that information flows through cyberspace. Individuals may systematically underestimate the true costs of incrementally moving toward a surveillance marketplace. Who knows if we will regret thirty years from now our agreement to the functionally unnecessary processing of cyberspace transactional data. For such reasons, some privacy advocates have suggested a federal regulatory regime, headed by an independent privacy commission.[363] Such a regime may, in the end, be necessary, but it is pragmatic to start with more limited ambitions. In today's privacy politics, the strong medicine of a privacy commission will be politically infeasible until weaker medicine has been tried. In the meantime, most of us could agree that policymakers and academics alike should work to improve public understanding of cyberspace privacy.

In continuing the privacy conversation, we must recognize that a vision protective of information privacy in cyberspace will be singularly hard to maintain. Cyberspace's essence is the processing of information in ways and at speeds unimaginable just years ago. To retard this information processing juggernaut in the name of privacy seems antitechnology, even antiprogress. It cuts against the hackneyed cyber-proclamation that information wants to be free. Nevertheless, I believe this intentional application of friction to personal information flows is warranted. If profit-seeking organizations are in-

363. *See* IITF OPTIONS PAPER, *supra* note 19, at 28-33 (listing the pros and cons of possible governmental and nongovernmental regulatory regimes). An excellent international comparative analysis, including a critique of the relative effectiveness of data protection agencies, appears in DAVID H. FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES: THE FEDERAL REPUBLIC OF GERMANY, SWEDEN, FRANCE, CANADA, AND THE UNITED STATES (1989).

stituting such friction in the name of intellectual property, individuals should not be chastised for doing the same in the name of privacy. Historically, privacy issues have been an afterthought.[364] Technology propels us forward, and we react to the social consequences only after the fact. But the amount of privacy we retain is—to use a decidedly low-tech metaphor—a one-way ratchet. Once we ratchet privacy down, it will be extraordinarily difficult to get it back.[365] More disturbingly, after a while, we might not mind so much. It may dawn on us too late that privacy should have been saved along the way.

364. *See* AGRE, *supra* note 288, at 18 (characterizing privacy as "a residual category—something left over after other issues have staked their claims").

365. *See* George B. Trubow, *Watching the Watchers: The Coordination of Federal Privacy Policy*, 3 SOFTWARE L.J. 391, 407 (1989) ("The longer we wait, the more difficult it becomes to 'retrofit' information technology so that protocols can provide appropriate protection.").

APPENDIX

A BILL[366]

To protect information privacy in cyberspace

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

Section 1. *Short Title.*

This Act may be cited as the "Cyberspace Privacy Act of ___."

Section 2. *Definitions.*

As used in this act—

(1) "Cyberspace" means any communication service or system that provides computer-mediated access through electronic communications to a computer server. "Cyberspace" explicitly includes, without limitation, any communication service or system that provides or enables electronic communications through the Internet.[367]

(2) "Electronic communications" has the same meaning as in 18 U.S.C. § 2510(12).[368]

---

366. Those readers who conclude that this bill is too vague or radical might want to review the privacy provisions of the Cable Communications Policy Act of 1984, 47 U.S.C. § 551 (1988 & Supp. V 1993), and the Video Privacy Protection Act of 1988, 18 U.S.C. § 2710-2711 (1994).

367. I have not located any especially useful definition of cyberspace in federal or state legislation. The Communications Decency Act makes mention of an "interactive computer service," from which my definition borrows somewhat:

> The term 'interactive computer service' means any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions.

47 U.S.C. § 230(e)(2) (1997).

The Consumer Internet Privacy Protection Act of 1997 also uses the term "interactive computer service," defined as "any information service that provides computer access to multiple users via modem to the Internet." H.R. 98, 105th Cong. § 4(1) (1997). The use of the word "modem" is problematic because, technically speaking, computers do not use modems, which change digital signals from the computer to analog signals carried over analog telephone networks, over fully digital communication networks.

Other attempts at regulating cyberspace have failed to produce crisper definitions. *See, e.g.*, N.Y. PENAL LAW § 235.21(3) (McKinney 1997) (defining a "computer communication system" as one "allowing the input, output, examination or transfer, of computer data or computer programs from one computer to another").

368. It means:

> [A]ny transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include—

(3) "Internet" means the globally distributed network of computers and telecommunications devices, owned both privately and publicly, that support communications through

(A) the Transmission Control Protocol/Internet Protocol ("TCP/IP") suite, or its subsequent extensions; or

(B) any protocols interoperable with the TCP/IP suite or with its subsequent extensions.[369]

(4) "Personal information" means information identifiable, directly or indirectly, to an individual, household, or to a specific computer regularly used by fewer than the same ten individuals. It includes, without limitation, information that identifies said individual, household, or computer as having requested, offered, leased, financed, rented, purchased, sold, or exchanged particular items or general kinds of information, services, or goods.[370]

(A) any wire or oral communication;

(B) any communication made through a tone-only paging device;

(C) any communication from a tracking device (as defined in section 3117 of this title); or

(D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds;

18 U.S.C. § 2510(12) (1994). By excluding wire communications, the Cyberspace Privacy Act does not cover personal information collected through, for example, a traditional telephone conversation.

369. The California Business and Professional Code defines the Internet as:

[T]he global information system that is logically linked together by a globally unique address space based on the Internet Protocol (IP), or its subsequent extensions; and is able to support communications using the Transmission Control Protocol/Internet Protocol (TCP/IP) suite, or its subsequent extensions, or other IP-compatible protocols; and provides, uses, or makes accessible, either publicly or privately, high level services layered on the communications and related infrastructure described herein.

CAL. BUS. & PROF. CODE § 17538(e)(6) (West 1997). My definition differs slightly because (1) the reference to "globally unique address space" is redundant with the specification of the TCP/IP protocol, and (2) the phrase "high level services," which might be a reference to the Open System Interconnection reference model of networks, is vague.

I also prefer my definition over the one that appears in the 1996 Telecommunications Act, which defines the Internet as "the international computer network of both Federal and non-Federal interoperable packet switched data networks." 47 U.S.C. § 230(e)(1) (1997); *see also* Consumer Internet Privacy Protection Act of 1997, H.R. 98, 105th Cong. § 4(2) (adopting the same definition of the Internet); Social Security On-line Protection Act of 1996, H.R. 1287, 105th Cong. § 4(2) (1997) (same); Encrypted Communications Privacy Act of 1997, S. 376, 105th Cong. § 2805(b)(4)(F) (1997) (same). First, the use of the term "packet switched" is unclear. I assume that term is meant to distinguish the Internet from "circuit switched" networks, such as our public telephone system. But what about "cell switched" networks, such as Switched Multimegabit Data Service ("SMDS") or Asynchronous Transfer Mode? *See* HORAK, *supra* note 3, at 223, 293-316 (discussing cell-switching, SMDS, and ATM). Second, this definition fails to capture the heart of the Internet, which is the TCP/IP protocol. Therefore, it includes entirely proprietary networks that are packet switched, but neither interoperable with TCP/IP nor publicly accessible.

370. Notice how I am not focusing solely on sensitive information, leaving nonsensitive information up for grabs. This is not only because drawing a sensitive/nonsensitive distinction is difficult, *see* FEDERAL RESERVE REPORT, *supra* note 84, at 14-15 (discussing the difficulty of de-

(5) "Individual" means a natural human being, regardless of citizenship or residence status.

(6) "Cyberspace transaction" means an interaction with an individual through cyberspace for the purposes of satisfying, accepting, or completing an individual's request, offer, lease, financing, rental, purchase, sale, or exchange of information, services, or goods. A "cyberspace transaction" specifically includes the browsing of a World Wide Web page through the hypertext transfer protocol and its subsequent extensions, regardless of whether any money is exchanged. A "cyberspace transaction" specifically excludes any portion of an interaction that is a message from an individual to an individual in a noncommercial context, or to a publicly accessible forum.

(7) "Message" means an electronic communication—such as electronic mail and its subsequent extensions—whose content is authored or prepared by an individual with the intent that that content be delivered to some person.

(8) "Person" means a nongovernmental individual, partnership, association, limited liability company, cooperative, joint-stock company, trust, or corporation.[371]

---

fining "sensitive"), but also because advanced data mining makes this distinction far less important. It is a common mistake to think that the danger cyberspace poses to privacy is captured in any single bit of personal information. In fact, any such morsel of data is likely to be inconsequential. Instead, the true privacy threat arises from the systematic, detailed aggregation of otherwise trivial data that allows the construction of a telling personal profile. What seems nonsensitive in isolation becomes sensitive in aggregation. As the Supreme Court has recognized, in the context of criminal records:

> [T]he compilation of otherwise hard-to-obtain information alters the privacy interest implicated by disclosure of that information. Plainly there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information.

United States Dep't. of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 764 (1989). In *Reporters Committee*, the Supreme Court decided whether the release of FBI "rap sheets" constituted an invasion of privacy within the meaning of the privacy exemption of the Freedom of Information Act. *See id.*; *see also* 5 U.S.C. § 552(b)(7)(C) (1982). The Court recognized the synergistic risk posed to privacy by profiles compiled from public conviction information that would otherwise enjoy a practical obscurity. It noted the vast distinction "between scattered disclosure of the bits of information contained in a rap sheet and revelation of the rap sheet as a whole." *Reporters Committee*, 489 U.S. at 764; *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 & n.89 (1994) (describing a "mosaic theory" of information, where the whole is greater than the sum of the parts).

371. I add "limited liability company" and "cooperative" to the definition of "person" in the Telecommunications Act of 1996. *See* 47 U.S.C. § 153(32) (1997). I also add "nongovernmental," since this Act is meant to apply only to the private sector. By this limitation, I do not mean to close off further discussion on whether such an Act should also apply to the public sector.

(9) "Noncommercial context" means a context in which the primary purpose of the interaction is not to exchange, or facilitate the exchange of, information, services, or goods for money or money's worth.

(10) "Publicly accessible forum" means any forum available through cyberspace, such as a Usenet newsgroup, listserv, chat room, Multi-User Domain, World Wide Web page, and their subsequent extensions whose audience is not or cannot be readily restricted by the individual sending the message.

(11) "Processing" means any combination of acquisition, disclosure, or use of personal information. The term "use" includes, but is not limited to, storage, organization, analysis, matching, consultation, and destruction.

(12) "Functionally necessary" describes personal information processing that is necessary to execute the cyberspace transaction in which the personal information is originally acquired. This is limited to information processing necessary for successful communication; payment and delivery; dispute resolution; warnings to the individual of any defect or danger; maintenance of cyberspace infrastructure; protection from fraud and abuse; adherence to governmental recordkeeping regulations; and transfer of business ownership.[372] It expressly excludes processing of personal information to target information, services, and goods on the basis of that personal information to the individual.

(13) "Consent" means an individual's fully informed assent manifested by an affirmative act in a written or an electronic communication.

(14) "Law enforcement agency" means any agency of the United States or of a state or political subdivision thereof, that is empowered by law to conduct investigations of, make arrests for, or prosecute criminal offenses.

Section 3. *Notice.*

(a) NOTICE REQUIRED—A person that acquires personal information in the course of executing, or facilitating the execution of, a cyberspace transaction[373] shall provide clear and conspicuous notice about:

---

372. The VPPA includes in its definition of "ordinary course of business" both order fulfillment and request processing. *See* Video Privacy Protection Act of 1988, 18 U.S.C. § 2710(a)(2) (1994). But these terms, according to the legislative history, permit "marketing to their customers." S. REP. NO. 100-599, at 14 (1988), *reprinted in* 1988 U.S.C.C.A.N. 4342-1, 4342-12. Because I do not consider such marketing to be functionally necessary, the phrases "order fulfillment" and "request processing" are absent from my Act's definition.

373. Note that the Act does not apply solely to communications providers or other transaction facilitators. One rationale for such a limitation might be that communications providers act as gatekeepers between the individual and all transacting parties and thus have direct access to the most

(1) why personal information is being collected;

(2) to whom the personal information is expected to be disclosed;

(3) what the personal information is expected to be used for;

(4) what steps will be taken to protect the personal information;

(5) the consequences of providing or withholding the personal information; and

(6) any rights of redress.

(b) TIMING—

(1) Functionally Necessary Processing—For personal information processing that is functionally necessary to the cyberspace transaction, the person that acquires such personal information shall provide convenient and reasonable access to the notice required in Subsection (a) to the individual.

(2) Functionally Unnecessary Processing—For personal information processing that is not functionally necessary to the cyberspace transaction, the person that seeks to acquire such personal information shall provide notice to the individual before any such processing takes place.[374]

---

telling data. A similar argument could be made about electronic payment providers. By regulating electronic communication service and cable service providers, the current ECPA and the privacy provisions of the 1984 Cable Act reflect this sensibility.

Unfortunately, regulating transaction facilitators alone ignores the reality that transacting parties do a substantial amount of data collection in cyberspace. And even if we substantially restrict transaction facilitators' ability to acquire, disclose, and use personal information, that would hardly prevent transacting parties—which include every site we browse and every firm from which we purchase a product—from collecting, mining, and sharing our personal data with others. As noted above, the costs of data exchange will continue to decrease in cyberspace due to advances in telecommunications technology and the standardization of data templates. Transacting parties will therefore be able to share databases with ease. As a long-term solution, it is naive to think that regulating transaction facilitators alone will adequately address cyberspace privacy concerns.

374. These provisions are constructed to avoid redundant or wasteful notices. For functionally necessary processing, individuals will likely—although admittedly not always—have a rough sense of how that information will be used, even without express notice. For these uses, therefore, an information collector need only make its privacy practices reasonably available. For example, when an individual gives her name and address to a pizza parlor through an e-mail, prior explicit notice would unduly burden the consummation of the transaction if the restaurant will only use that information to deliver the right pizza to the right address. On the other hand, if the pizza parlor uses the information in a manner not functionally necessary—for example, to sell lists of high-volume customers to health insurance companies—then express notice is warranted. *See* IITF PRINCIPLES, *supra* note 19, at 7; *cf.* James v. Ford Motor Credit Co., 638 F.2d 147, 150 (10th Cir. 1980) (concluding that too much information in a disclosure "result[s in] a piece of paper which appears to be 'just another legal document' instead of the simple, concise disclosure form Congress intended" (quoting S. REP. NO. 96-73, at 3 (1979), *reprinted in* 1980 U.S.C.C.A.N. 280, 281-82)).

Section 4. *Processing.*

(a) PRIMARY MARKET LIMITATION—In the course of executing, or facilitating the execution of, a cyberspace transaction, a person shall not process personal information in a manner functionally unnecessary to the transaction without the prior consent of the individual.

(b) SECONDARY MARKET LIMITATION—Without the prior consent of the individual, a person shall not process personal information originally acquired from a cyberspace transaction if the person has knowledge or reason to know that such processing is functionally unnecessary to that cyberspace transaction.

Section 5. *Access & Archiving.*

(a) ACCESS & CORRECTION—A person that acquires personal information in the course of executing, or facilitating the execution of, a cyberspace transaction shall provide, upon request of the individual, clarification of the notice provided pursuant to Section 3, Subsection (a), without fee, cost, or charge. Said person shall also provide to the individual access to that personal information in a reasonable time, place, and manner, without fee, cost, or charge. Said person shall also provide to the individual a reasonable opportunity to correct any error in such personal information, without fee, cost, or charge.

(b) DESTRUCTION OF RECORDS—A person that acquires personal information in the course of executing, or facilitating the execution of, a cyberspace transaction shall destroy that personal information when it is no longer functionally necessary to the cyberspace transaction, unless a pending request for the personal information exists under Section 6 or the individual has given consent to keep the information for a longer period.

Section 6. *Disclosure Exceptions.*

Notwithstanding any other section of this Act, it shall be lawful to disclose personal information acquired in the course of executing, or facilitating the execution of, a cyberspace transaction to:

(a) a law enforcement agency pursuant to a court order if, in the court proceeding relevant to such court order—

> (1) such agency offers clear and convincing evidence that the individual to whom the personal information pertains is reasonably suspected of engaging in criminal activity and that the personal information sought would be material evidence in the case; and
>
> (2) the individual is afforded the opportunity to appear and contest such agency's claim.

(b) a law enforcement agency or a medical professional if such information is—

(1) critical to the life, healthy, or safety of the individual; and

(2) exigent circumstances preclude the possibility of obtaining consent from the individual.[375]

Section 7. *Relief & Enforcement.*

(a) CIVIL ACTION—Any individual aggrieved by the processing of his or her personal information by a person in violation of this Act may bring a civil action against that person in a United States district court without regard to the amount in controversy.

(1) The court may award actual damages but not less than liquidated damages computed at the rate of $100 for each separate violation or $5000, whichever is higher. The court may award reasonable attorneys' fees and litigation costs to the plaintiff if the plaintiff prevails. The court may also award punitive damages for purposeful violations of this Act made in exchange for valuable consideration.

(2) The remedies provided by this Section shall be in addition to any other lawful remedy available to the aggrieved individual.

(b) ADMINISTRATIVE ACTION—The Federal Trade Commission shall have the authority to investigate any act or practice to determine whether this Act has been violated. The Federal Trade Commission shall also have the authority to issue cease and desist orders to any person in violation of this Act, as if the person were in violation of section 5 of the Federal Trade Commission Act.

Section 8. *Statute of Limitations.*

No civil action shall be maintained under the provisions of this Act unless it is commenced within four years after the claim accrued.

375. *Cf.* An Act Respecting the Protection of Personal Information in the Private Sector, 1993 S.Q. 507 (Can.) (permitting disclosure "to a person to whom the information must be communicated by reason of the urgency of a situation that threatens the life, health or safety of the person concerned").

Section 9. *Preemption.*

No state or political subdivision thereof shall enact or enforce different statues, regulations, or ordinances[376] concerning the processing of personal information acquired by a person in the course of executing, or facilitating the execution of, a cyberspace transaction.

376. I do not mean to preempt the common law tort of invasion of privacy.