Information Privacy/Information Property

Jessica Litman*

From most objective standpoints, protecting information privacy though industry self-regulation is an abject failure. The current political climate has been hostile to proposals for meaningful privacy regulation. Privacy advocates have been casting around for some third alternative and a number of them have fastened on the idea that data privacy can be cast as a property right. People should own information about themselves, and, as owners of property, should be entitled to control what is done with it. The essay explores that proposal. I review the recent enthusiasm for protecting data privacy as if it were property, and identify some of the reasons for its appeal. I examine the model and conclude that a property rights approach would be unlikely to improve matters; indeed, it would tend to encourage the market in personal data rather than constraining it. After critiquing the property model, I search for a different paradigm, and explore the possibility that tort law might support a workable approach to data privacy. Current law does not provide a tort remedy for invasion of data privacy, but there are a number of different strands in tort jurisprudence that might be extended to encompass one. In particular, a rubric based loosely on breach of confidence might persuade courts to recognize at least limited data privacy rights. I conclude, however, that while the tort solution is preferable to a property rights approach, it is likely to offer only modest protection. Common law remedies are by their nature incremental, and achieving widespread adoption of novel common law causes of action is inevitably a slow process. Even established common law remedies, moreover, are vulnerable to statutory preemption. Although a rash of state tort law decisions protecting data privacy might supply the most compelling impetus to federal regulation we are likely to achieve, the resulting protection scheme is unlikely to satisfy those of us who believe that data privacy is worth protecting.

> What we offer our advertisers, is an audience delivered with unprecedented precision. An Audience that welcomes your message because we show you how to make it relevant to their interests. An audience that we know intimately because they allow us to follow them wherever they roam on the Internet.
>
> —Advertisement for NetZero™[1]

Almost everything each of us does seems to generate transactional information. Walks round the block are still unrecorded, except in those communities with cameras. Interactions that begin and end and stay within the home are still largely unreported, although everything entering and leaving by way of the phone lines, cable lines, satellite dishes or wireless, non-

* Professor of Law, Wayne State University. I want to thank Jon Weinberg for his insightful comments on earlier drafts of this essay. All Internet citations were current as of May 22, 2000.

1. Copy on file with author.

broadcast spectrum is documented.[2] Non-cash purchases are memorialized and toted up. Large cash purchases are memorialized and turned in. Cash withdrawals and deposits are recorded and saved. Visits to the doctor, diagnoses, prescriptions, and referrals are coded and passed along. Everything we look at on the Internet is noted and retained.[3] All of this information is collected, aggregated, and stored on computers. Anyone with reason to do so can correlate the information stored on one computer with the information stored on another, and another, and another.[4] The resulting dossier may be used, sold, published, or correlated with other sources of data.[5] In the United States, that's completely legal.

At some level we know that this is happening, although few of us really appreciate it.[6] Sometime in the past dozen or so years, most of us became gradually aware of the fact that businesses were collecting information about us to use in marketing products to us. At some moment it became impossible not to add up all the little hints. That check cashing card we'd applied for at the supermarket in order to write checks for groceries gave the supermarket the ability to track our purchases; when supermarkets began accepting credit cards, that gave them the same ability. The sweater we ordered from a catalog arrived in the mail along with umpteen new glossy catalogs for people who wear sweaters. That cooking magazine we subscribed to seemed to show up along with a score of apparently independent special offers for folks interested in cooking.

People react to this in different ways. Some (although fewer than the Direct Marketing Association would have us believe)[7] seem to appreciate the

---

2. *See* NATIONAL TELECOMM. AND INFO. ADMIN., U.S. DEP'T OF COMMERCE, PRIVACY AND THE NII: SAFEGUARDING TELECOMMUNICATIONS-RELATED PERSONAL INFORMATION (1995) <http://www.ntia.doc.gov/ntiahome/privwhitepaper.html>.

3. *See, e.g.*, Diane Anderson & Keith Perine, *Privacy Issue Makes DoubleClick a Target*, THE STANDARD, Feb. 3, 2000 <http://www.thestandard.com/article/display/0,1151,9480,00.html> (reporting on Web advertising firm that tracks online activities); Bob Tedeschi, *Net Companies Look Offline for Consumer Data*, N.Y. TIMES CYBERTIMES, June 21, 1999 <http://www.nytimes.com/library/tech/99/06/cyber/commerce/21commerce.html> (describing use of data gathered offline to enhance online marketing).

4. *See, e.g.*, U.S. GEN. ACCOUNTING OFFICE, SOCIAL SECURITY: GOVERNMENT AND COMMERCIAL USE OF THE SOCIAL SECURITY NUMBER IS WIDESPREAD 7-12 (1999) (describing use of social security numbers to aggregate personal information).

5. *See* ELLEN ALDERMAN & CAROLINE KENNEDY, THE RIGHT TO PRIVACY 323-32 (1995) (describing widespread use of personal information to create personal data profiles).

6. This subject gives new meaning to the saying "the devil's in the details." Before beginning work on this paper, for example, I was unaware that the Home Shopping Network had deployed a system using voice print analysis to identify frequent shoppers from their voices alone. *See* Leander Kahney, *Giving Voice to Net Security*, WIRED NEWS, June 29, 1999 <http://www.wired.com/news/technology/0,1282,20460,00.html>.

7. *See* Direct Marketing Assoc., *Consumer FAQs* <http://www.the-dma.org/consumers/consumerfaqs.html> ("For many people advertising mail is fun, informative and a convenience."); *see also* Experian Info. Solutions, Inc., *Visitor Insight*[SM] *Revolutionizes Online Marketing* (Oct. 21,

individual attention.[8] Others find it chilling. If one is a member of the latter class, though, there isn't too much one can do. The gradual dawning of the realization that folks have been collecting personal information about one means that, almost invariably, by the time one realizes that there is a problem, the cat is out of the bag. A variety of different businesses have already collected a sea of details about one's income, interests, employment history, health, purchases, and preferences. Even if one never supplied a single further datum, anyone with access to all the details could assemble a frighteningly precise dossier.

So, many people understandably try to rejoin the category of folks who, on balance, like, or at least really don't mind, the individualized attention. They, we, seek reassurance in the notion that, as unimportant peons with no public profile, our personal information is not of sufficient interest to anyone to collect, compile or correlate. "*Someone who tailed me all day long could find out all sorts of personal things, but nobody is going to bother, so I don't worry about it. This is like that.*"

It's a lie, of course, and increasingly people realize it. The information that *you* (insert name, address, age, income, and social security number here) read both *Newsweek* and your daily horoscope; buy Häagen-Dazs® ice cream; travel annually to New Mexico; have a standing prescription for Prozac® and buy a variety of different OTC antacids as well as a number of different brands of lubricated condoms; have joined three different health clubs for short sojourns over the past two years; always order a salad in restaurants; never joined Weight Watchers® (and, in fact, have a 31" waist and a body mass index of 25); and give money to public television, is exceedingly valuable for the crassest of reasons: Anyone who has that information can sell it.

Some people adopt silly but vaguely reassuring tactics: confuse the collectors by using different variations of your name;[9] make up several different assumed middle initials; choose your favorite merchants and fill out their information cards so that they will reap the extra cents from selling you to the data banks; trade your shopper's advantage cards with your neighbors; open bank accounts at different banks; fill in forms with your work address and phone number rather than your home address and phone number, and pay your bills using different credit cards. None of these maneuvers, of

---

1999) <http://www.experian.com/corporate/press_releases/102199.html> ("[M]ost consumers prefer the personalized product offers and individual service made possible by Visitor Insight . . . .").

8. *See, e.g.*, Katie Hafner, *Do You Know Who's Watching You? Do You Care?*, N.Y. TIMES, Nov. 11, 1999, at G1 (describing L.L. Bean's use of caller ID and its exchange of customer information with other companies).

9. *See, e.g.*, Avrahami v. U.S. News & World Report, Inc., at law No. 95-1318, in chancery No. 96-203,1996 WL 1065557, at *2 (Va. Cir. Ct. June 13, 1996) (finding that defendant used at least 19 different names in making purchases).

course, is likely to be of any help to any particular individual who wants to protect her privacy: If there are six different dossiers out there for someone with her name, she'll just get six times the junk mail, and data miners have invented effective strategies for dispatching their computers to sort through the data mines to figure out just who is really whom. Nonetheless, these tactics seem to undermine the reliability of the data, just a little, making this game a little more expensive, and offering a thin but ultimately unpersuasive illusion of control.

Actual control seems unattainable. It's just barely possible that one could regain some measure of data privacy by moving to Europe.[10] In Europe, it is illegal to release personal data to a third party, or even to use it for a purpose unrelated to the reason for which it was collected, without the subject's consent.[11] The European Union has been pressing the United States to enact similar restrictions to protect data privacy, and has even threatened to stop the international data flow if necessary to protect its citizens' privacy rights, but a data privacy protection law seems unlikely.[12] The direct marketing industry has apparently persuaded the foreign affairs folks in the administration to view the negotiations with Europe over data privacy protection as a test of national manhood. The object seems to be to get the other government to blink first. Instead of some law, the industry insists, self-regulation will result in more than adequate protections.[13] Industry self-

---

10. *But see* Simon G. Davies, *Re-Engineering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity*, *in* TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE 143, 156-57 (Philip E. Agre & Marc Rotenberg eds., 1997) (arguing that "data-protection law [in the European Union] does almost nothing to prevent or limit the collection of information").

11. *See* Council Directive 95/46 of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, art. 6, 7, 1995 O.J. (L 281) 31. For a comprehensive comparative analysis of the regulation of personal information in the U.S. and Europe, see PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW (1996).

12. *See generally The Role of Standards in Growth of the Global Electronic Commerce: Hearings Before the Subcomm. on Science, Tech. and Space of the Senate Comm. on Commerce, Science and Tech.*, 106th Cong. (1999) (statement of Hon. Andrew J. Pincus, General Counsel, Dep't of Commerce); *Privacy on the Internet: Hearings on S. 809, The Online Privacy Protection Act of 1999, Before the Subcomm. on Communications of the Senate Comm. on Commerce, Science, and Transp.*, 106th Cong. (1999) [hereinafter *Senate Privacy Hearing*] (opening statement of John McCain, Chairman, Senate Comm. on Commerce, Science, and Transp.; statement of Marc Rotenberg, Director, Electronic Privacy Information Center; statement of Christine Varney, Senior Partner, Hogan & Hartson) <http://www.senate.gov/~commerce/hearings.htm>.

13. *See Privacy: Industry Pleads Case (Again) for Opportunity to Prove Effectiveness of Self-Regulation*, 4 ELECTRONIC COM. & L. REP. (BNA) 479 (June 2, 1999); Stephen Altobelli, *Direct Marketers Make Industry-Wide Commitment: 'Privacy Promise to American Consumers' to Build Trust*, DMA NEWS (July 7, 1999) <http://the-dma.ispi.net/texis/scripts/news/newspaper/+DwwBm+emE7vwwwr/displayArticle.html> (reporting that the Direct Marketing Association now requires its members to follow a set of consumer privacy protection practices); Declan McCullagh, *Feds Tackle Online Privacy*, WIRED NEWS, July 20, 1999 <http://www.wired.com/news/politics/0,1283,20832,00.html>.

regulation, of course, has got us where we are today.[14] Studies of how well it is working confirm what one would expect: It works far better at enhancing commerce in personal data than it does in protecting personal data privacy.[15] Despite those studies, government actors insist that self-regulation is the American way, and it is enough.[16] And, in the long run, the market for personal data will be a global one. If, as the U.S. negotiators assure us is likely, Europe blinks first,[17] then data transfers will continue without meaningful restriction on the uses made of personal information.[18] If personal data moves freely around the world and is unregulated in the United States, nobody will have significant data privacy.

Is there any realistic solution? Self-regulation is an abject failure; meaningful privacy regulation appears to be unenactable as a political matter; and accepting that privacy is an outmoded notion from a bygone age seems unacceptable. The proposal that has been generating the most buzz, recently, is the idea that privacy can be cast as a property right. People should *own* information about themselves and, as owners of property, should be entitled to control what is done with it.[19]

---

14. *See* Joel R. Reidenberg, *Restoring Americans' Privacy in Electronic Commerce*, 14 BERKELEY TECH. L.J. 771, 773-81 (1999) ("[T]he American experience during the last two decades shows that the theory of self-regulation is pure sophistry.").

15. *See, e.g.*, Center for Media Educ. & Consumer Fed'n of Am., Shelley Pasnik & Mary Ellen R. Fise, *Children's Privacy and the GII*, *in* PRIVACY AND SELF-REGULATION IN THE INFORMATION AGE 78 (U.S. Dep't of Commerce ed., 1997) [hereinafter INFORMATION AGE] <http://www.ntia.doc.gov/reports/privacy/selfreg1.htm>; FEDERAL TRADE COMM'N, SELF-REGULATION AND PRIVACY ONLINE: A REPORT TO CONGRESS 6-7 (1999) (reporting that most online businesses do not have satisfactory privacy policies); U.S. GEN. ACCOUNTING OFFICE, *supra* note 4, at 12-14 (explaining that businesses claim to have responded voluntarily to concerns about the disclosure of social security numbers, but nonetheless insist that any legal restriction on disclosure would negatively impact their business).

16. *See, e.g.*, FEDERAL TRADE COMM'N, *supra* note 15, at 12-14 (recommending against enacting privacy legislation).

17. *See, e.g.*, David L. Aaron, Undersecretary of Commerce for Int'l Trade, Remarks Before the Information Technology Association of America Fourth Annual IT Policy Summit (Mar. 15, 1999) <http://www.itaa.org/news/source/aaron.htm> (describing his efforts to persuade the EU to accept U.S. approach as adequate); David L. Aaron, Remarks at E-Commerce Mexico (Sept. 29, 1999) <http://www.ita.doc.gov/media/Mexico_speech929.htm> (reporting success in persuading EU to accept U.S. self-regulation).

18. The Commerce Department posts progress reports on the data privacy negotiations, along with drafts under consideration. *See* Electronic Commerce Task Force, U.S. Dep't of Commerce, *International Trade Administration Electronic Commerce Task Force* <http://www.ita.doc.gov/ecom/menu.htm>. None of the proposals under serious consideration have imposed significant constraints on the commercial use or reuse of consumer transaction data.

19. *See, e.g.*, Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1246-94 (1998) (suggesting privacy be treated in Cyberspace as a marketable commodity subject to default rules designed to permit an individual to impose limits on data reuse); Kenneth C. Laudon, *Extensions to the Theory of Market and Privacy: Mechanics of Pricing Information*, *in* INFORMATION AGE, *supra* note 15, at 43 (suggesting that individuals should be deemed to own their own personal information and have the right but not the obligation to sell it to institutional users or information brokers); Lawrence Lessig, The Architecture of Privacy 16-18 (Apr. 3, 1998)

This essay explores that proposal. In Part I, I review the recent enthusiasm for protecting data privacy as if it were property, and identify some of the reasons for its appeal. In Part II, I examine the model and conclude that a property rights approach would be unlikely to improve matters; indeed, it would tend to encourage the market in personal data rather than constraining it. In Part III, I search for a different paradigm, and suggest that tort law might support a workable approach to data privacy. Part IV, therefore, explores the possibility of a solution based in tort. Current law does not provide a tort remedy for invasion of data privacy, but there are a number of different strands in tort jurisprudence that might be extended to encompass one. In particular, a rubric based loosely on breach of confidence might persuade courts to recognize at least limited data privacy rights. Part V concludes that while the tort solution is preferable to a property rights approach, it is likely to offer only modest protection. Common law remedies are by their nature incremental, and achieving widespread adoption of novel common law causes of action is inevitably a slow process. Even established common law remedies, moreover, are vulnerable to statutory preemption. Although a rash of state tort law decisions protecting data privacy might supply the most compelling impetus to federal regulation we are likely to achieve, the resulting protection scheme is unlikely to satisfy those of us who believe that data privacy is worth protecting.

I

> One of the most facile and legalistic approaches to safeguarding privacy that has been offered to date is the notion that personal information is a species of property. If this premise is accepted, the natural corollary is that a data subject has the right to control information about himself and is eligible for the full range of legal protection that attaches to property ownership.

(unpublished manuscript, available at <http://cyber.law.harvard.edu/works/lessig/architecture_priv.pdf>) (suggesting that a combination of property rights, encryption technology, and intelligent agents could protect privacy); Eli M. Noam, *Privacy and Self-Regulation: Markets for Electronic Privacy*, *in* INFORMATION AGE, *supra* note 15, at 21 (describing several applications of the market-based approach); Pamela Samuelson, *A New Kind of Privacy? Regulating Uses of Personal Data in the Global Information Economy*, 87 CAL. L. REV. 751, 769-73 (1999) (book review) (identifying advantages of a market approach to personal information, including elimination of government intervention); *Developments in the Law—The Law of Cyberspace*, 112 HARV. L. REV. 1574, 1644-48 (1999) (arguing that the property entitlement to personal information could be shifted through computer coding rather than law); *see also House Telecom Subcommittee Holds Hearing on Online Privacy*, TECH L.J., July 14, 1999, ¶ 14 <http://www.techlawjournal.com/privacy/19990713b.htm> (reporting that Rep. Chris Cox proposed establishing a property right in personal information at the House Telecommunications Subcommittee hearing on online privacy). *But see* Rochelle Cooper Dreyfuss, *Warren and Brandeis Redux: Finding (More) Privacy Protection in Intellectual Property Lore*, 1999 STAN. TECH. L. REV. VS 8 (1999) (suggesting that intellectual property rights in information would not offer effective privacy protection).

—ARTHUR MILLER[20]

Treating privacy as a property right has been a perennial entry in the debate about personal information, but has not received much serious attention until recently. Alan Westin suggested treating personal information as a property right more than thirty years ago,[21] to mixed reviews.[22] The recent upsurge in interest in a property rights approach seems to be fueled by today's anti-regulatory culture. Economists have conceptualized privacy interests in personal data as a species of property for several years because commodified data privacy interests are convenient subjects for market-based models, and market solutions are deemed preferable to government regulation. A 1997 report by the National Telecommunications and Information Administration (NTIA) on *Privacy and Self-Regulation in the Information Age*[23] introduced its subject with a chapter devoted to theory, heavily influenced by economics. In *Economic Aspects of Personal Privacy*, Dean Hal Varian analyzed consumers' data privacy as a property right in private information, in order to explore the possibility of vesting consumers with the ability to control the use of their personal data.[24] In *Extensions to the Theory of Markets and Privacy: Mechanics of Pricing Information*, Professor Kenneth Laudon, building on his own earlier work,[25] argued that the current privacy crisis derived from market failure and could, at least in theory, be addressed by treating personal information as property and then pricing it to better reflect its value.[26]

---

20. ARTHUR R. MILLER, THE ASSAULT ON PRIVACY: COMPUTERS, DATA BANKS, AND DOSSIERS 211 (1971).

21. *See, e.g.*, ALAN F. WESTIN, PRIVACY AND FREEDOM 324-25 (1967). Westin's proposal sought to protect information privacy by combining conventional legal property protection with tort liability based on the doctrine of strict liability for abnormally dangerous or ultrahazardous activites:

> [P]ersonal information, thought of as the right of decision over one's private personality, should be defined as a property right, with all the restraints on interference by public or private authorities and due-process guarantees that our law of property has been so skillful in devising. Along with this concept should go the idea that circulation of personal information by someone other than the owner or his trusted agent is handling a dangerous commodity in interstate commerce, and creates special duties and liabilities on the information utility or government system handling it.

Id.

22. *See* ALDERMAN & KENNEDY, *supra* note 5, at 329 (pointing out that ownership of personal information is inconsistent with the First Amendment); ANNE WELLS BRANSCOMB, WHO OWNS INFORMATION? FROM PRIVACY TO PUBLIC ACCESS 180 (1994) (identifying the legal principles that would likely emerge in a property rights regime); MILLER, *supra* note 20, at 211-12 ("The basic objection to the [property] theory is that real and personal property concepts are irrelevant to the personal values that we are attempting to preserve by recognizing a right of privacy.").

23. INFORMATION AGE, *supra* note 15.

24. *See* Hal R. Varian, *Economic Aspects of Personal Privacy*, *in* INFORMATION AGE, *supra* note 15, at 36.

25. *See* Kenneth C. Laudon, *Markets and Privacy*, COMMUNICATIONS OF THE ACM, Sept. 1996, at 92.

26. *See* Laudon, *supra* note 19.

Lawyers, some of whom have assimilated the lingo of economics in self-defense, have picked up the market conception of privacy in order to cast privacy rights as property. Professor Jerry Kang explores a market-property rights model as an opportunity for setting default rules that would enhance consumers' control over their personal information.[27] The American Civil Liberties Union, usually an energetic supporter of the free flow of information, adopted a property rights stance in its 1997 "Take Back Your Data" campaign.[28] Professor Larry Lessig suggested recently that the fact that information is a valuable asset offers an opportunity to harness market methodology in the cause of privacy protection.[29] The Electronic Frontier Federation[30] used the property rights model to assign a price to personal data, in order to quantify the damages from data misuse.[31] Ram Avrahami's (unsuccessful) lawsuit against U.S. News & World Report for renting lists including his name to direct marketers predicated the claim on a property right in his name.[32] Professor Pamela Samuelson, in a recent review of two books on data privacy law, suggested that "[p]ropertizing personal information" would take advantage of the extant market in personal information, and "give members of the public some control, which they currently lack, over the traffic in personal data."[33]

What accounts for the appeal of the private property model? Some of the appeal, undoubtedly, is its aroma of possibility. Other more obvious solutions to the encroachments on data privacy seem impracticable. The United States does not have a federal data privacy law, and the U.S. Congress is unlikely to enact one.[34] The direct marketing industry won't permit it. The United States has no federal privacy agency, and the White House

---

27. *See* Kang, *supra* note 19, at 1246-73; *see also* Jerry Kang, *Cyberspace Privacy: A Primer and Proposal*, A.B.A. HUM. RTS. MAG., Winter 1999 <http://www.abanet.org/irr/hr/winter99_kang2.html> (summarizing Kang, *supra* note 19).

28. *See* Ira Glasser, *The ACLU Launches a Campaign to Protect Your Privacy*, ACLU SPOTLIGHT, Spring 1997, at 1 <http://www.aclu.org/library/spring97.html> ("The details of our personal lives are OUR property—and no one else's business.").

29. *See* Lessig, *supra* note 19, at 16-18.

30. The Electronic Frontier Foundation is a nonprofit organization promoting Internet and computer-related civil liberties. *See* Electronic Frontier Foundation, *About EFF* <http://www.eff.org/abouteff.html>.

31. *See* Renee Deger, *Putting a Price on Our Internet Identities*, RECORDER, June 14, 1999, at 1.

32. *See* Avrahami v. U.S. News & World Report, Inc., at law No. 95-1318, in chancery No. 96-203, 1996 WL 1065557, at *6 (Va. Cir. Ct. Jun 13, 1996) (holding that the defendant "has no property right" in any of the names he falsely used in purchasing goods and services).

33. Samuelson, *supra* note 19, at 771. Professor Samuelson explores the property model more deeply in her contribution to the Symposium, and concludes that despite the model's appeal, "the goals and mechanisms of property law are misaligned with information privacy policy objectives." ***See* Pamela Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L. REV. 1125, 1171 (2000).**

34. *See* note 12 *supra* and accompanying text; Lessig, *supra* note 19, at 14 ("[W]e should not expect [the lack of law protecting privacy] to change dramatically in the short term.").

has no interest in proposing one; it has been seduced by the promise of data commerce as an engine of American economic superiority.[35] The state law privacy torts are narrow.[36] Tort law protects personal data from disclosure only when it conveys embarrassing personal information.[37] Merely gathering data is not actionable, unless the gathering behavior is itself highly intrusive.[38] Tort law provides a remedy for unauthorized commercial exploitation of celebrities' identities,[39] but not for conveying accurate personal information, however lucrative the conveyance.[40] Even the recent token federal efforts to protect data privacy in the context of the regulation of other things have achieved very little.[41] Purveyors of data have challenged these regula-

35. *See* Jessica Litman, *Electronic Commerce and Free Speech*, 1 ETHICS AND INFORMATION TECHNOLOGY 213, 213-14, 216 (1999).

36. *See* Robert Gellman, *Does Privacy Law Work?*, *in* TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE, *supra* note 10, at 193, 209-12 (arguing that tort law remedies are not adequate to address privacy concerns in the computer era).

37. *See* RESTATEMENT (SECOND) OF TORTS § 652D (1965) (stating that publication constitutes invasion of privacy only "if the matter publicized is of a kind that . . . would be highly offensive to a reasonable person"); W. PAGE KEETON, DAN B. DOBBS, ROBERT E. KEETON & DAVID G. OWEN, PROSSER & KEETON ON THE LAW OF TORTS § 117, at 856-63 (5th ed. 1984 & Supp. 1988) (explaining that publication of "highly objectionable" facts may be actionable); Johnson v. Sawyer, 47 F.3d 716, 731-33 (5th Cir. 1995) (en banc); Beaumont v. Brown, 401 Mich. 80, 95-98 (1977).

38. *See, e.g.*, Nader v. General Motors Corp., 25 N.Y.2d 560 (1970) (holding that defendant's action must be intrusive).

39. *See* KEETON ET AL., *supra* note 37, at 851-54 (describing the cause of action for appropriating another's name or likeness); *see also, e.g.*, Cher v. Forum Int'l, Ltd., 692 F.2d 634 (9th Cir. 1982) (holding that California law permits recovery, through the right of publicity, for the unauthorized, commercial use of another's likeness or name).

40. *See, e.g.*, Sidis v. F-R Publ'g Corp., 113 F.2d 806 (2d Cir. 1940) (holding that biographical details may be published without consent); Avrahami v. U.S. News & World Report, Inc., at law No. 95-1318, in chancery No. 96-203, 1996 WL 1065557 (Va. Cir. Ct. June 13, 1996) (holding that sale or rental of subscribers' names and addresses is not actionable).

41. The Gramm-Leach-Bliley Act, Public Law No. 106-102 (1999), for example, incorporates financial privacy provisions in the context of financial services regulation, but those provisions generally permit disclosure of consumers' personal data and financial information without first securing consumer consent. *See* Jeri Clausing, *Revised Banking Legislation Raises Concerns About Privacy*, N.Y. TIMES, Oct. 25, 1999 <http://www.nytimes.com/library/tech/99/10/biztech/articles/25priv.html>; Frank James, *Critics: Bank Bill Imperils Privacy*, CHI. TRIB., Oct. 25, 1999 <http://www.chicago.tribune.com/version1/article/0,1575,SAV-9910250144,00.html>. The Clinton Administration's proposed rules for the privacy of Individually Identifiable Health Information, 64 Fed. Reg. 59118 (Nov. 3, 1999), have been widely criticized for permitting unnecessary and far more extensive disclosure of sensitive health information than is currently customary or legal in many states. *See, e.g.*, American Medical Association, *Comments on Proposed Rule on Standards for Privacy of Individually Identifiable Health Information*, Feb. 17, 2000 <http://aspe.os.dhhs.gov/admnsimp/nprm/comments/231512.pdf>; American Psychological Association, *Comments on Proposed Rule on Standards for Privacy of Individually Identifiable Health Information*, Jan. 20, 2000 <http://aspe.os.dhhs.gov/admnsimp/nprm/comments/227096.pdf>; Idaho Medical Association, *Comment on Proposed Regulations on Patient Privacy*, Jan 3, 2000 <http://aspe.os.dhhs.gov/admnsimp/nprm/comments/205427.pdf>; Dana A Monaco, M.D., Garden City Associates, *Comment on Proposed Privacy Regulation*, Jan. 13, 2000 <http://aspe.os.dhhs.gov/admnsimp/nprm/comments/215317.pdf>.

tions in court; as often as not, the courts have struck them down.[42] A property rights approach seems to have the potential to bypass the apparently insuperable barriers confronting other solutions.[43] To mangle Conan Doyle, if everything else is impossible, what remains, however improbable, might conceivably work.[44]

But why do people think that a property-rights approach could be foisted on opponents of privacy regulation, or achieved over their opposition? A large part of the appeal seems to be the illusion that property ownership is in some way pre-legal and pre-political—or at least can be so sold to anti-regulatory law makers. The story goes like this: Property was privately owned and traded long before legal institutions arose to interfere with it, and therefore treating privacy as a property right is a more natural, non-regulatory approach.

This illusion is one of the most enduring and tenacious in the American mythos,[45] despite the fact that it cannot withstand any serious examination.[46] People who believe that they own private property also seem to believe that their ownership rights are inherent in the natural order and decreed by the laws of God or science.[47] A number of libertarian thinkers rely on this illusion to perform the sleight of hand of advocating an end to all government regulation (at the same time insisting that the distribution of wealth achieved by the current system of regulation survive unchanged in the new era). If ownership of private property is power, however, calling privacy rights

---

42. *See, e.g.*, U.S. West, Inc. v. FCC, 182 F.3d 1224 (10th Cir. 1999) (overturning FCC regulations requiring customer approval of use of personal information for marketing on First Amendment grounds). *But see, e.g.*, Reno v. Condon, No. 98-1464, 2000 WL 16317 (U.S. 2000) (upholding the Driver's Privacy Protection Act).

43. *See, e.g.*, Kang, *supra* note 19, at 1273-77 (arguing that his property rights approach should surmount political barriers).

44. "'You will not apply my precept,' he said, shaking his head. 'How often have I said to you that when you have eliminated the impossible, whatever remains, *however improbable*, must be the truth?'" SIR ARTHUR CONAN DOYLE, THE SIGN OF FOUR (1890), *reprinted in* THE COMPLETE SHERLOCK HOLMES 87, 111 (1930).

45. *See generally* WILLIAM B. SCOTT, IN PURSUIT OF HAPPINESS: AMERICAN CONCEPTIONS OF PROPERTY FROM THE SEVENTEENTH TO THE TWENTIETH CENTURY 53-58, 137-154 (1977) (describing Stephen Field's and William Graham Sumner's natural rights conception of private property).

46. *See* ALAN RYAN, PROPERTY 61-69 (1987) (arguing that property rights are artificially constructed); Jonathan Weinberg, *Questioning Broadcast Regulation*, 86 MICH. L. REV. 1269, 1274 (1988) (book review) ("[I]t is misleading to think that the modes of social ordering that have come down to us from the British common law are so natural that they are not really regulation."); Margaret Jane Radin, *Market-Inalienability*, 100 HARV. L. REV. 1849 (1987) (deconstructing theories of property and inalienability).

47. *See, e.g.*, RICHARD A. EPSTEIN, TAKINGS: PRIVATE PROPERTY AND THE POWER OF EMINENT DOMAIN 5-6 (1985) ("[A]ll theories of natural rights reject the idea that private property and personal liberty are solely creations of the state . . . ."); Roger Pilon, *Property Rights and Regulatory Takings*, *in* CATO HANDBOOK FOR CONGRESS 203, 204-06 (1999) ("Property is the foundation of every right we have, including the right to be free.").

"property rights" offers the promise of magically vesting the powerless with control over their personal data. Because the law of private property is perceived as a-regulatory, this approach seems to answer the objections raised against significant government regulation.

Privacy advocates, further, have good reason to conclude that it is easy to create a property rights regime where none existed before, by simply declaring that one has valuable property to sell. In the last few years, we've seen an epidemic of newly minted property rights asserted on little initial basis beyond wishful thinking. That sort of tactic underlies the controversial Uniform Computer Information Transactions Act,[48] which imagines property rights into existence by encouraging would-be proprietors to exercise control over them by offering licenses constraining their use.[49] It is the basis for the right of publicity, which, in many jurisdictions, springs into being only when it is first licensed.[50] The entire house of cards represented by Hollywood's recognition of property rights in subjects' life stories[51] is an illusory creation impelled by the realities of financing. If one seeks either loans or investors, it helps to have a piece of property to offer as collateral. Producers of works based loosely on truth rather than fiction have no property rights in their subjects. If the central actors in the story can be persuaded to "sell" the exclusive rights to film what happened to them, then those rights become property that a producer can take to the bank, even though no court would enjoin such a production on the ground that its principals lacked such a property right,[52] or had created their production despite the fact that the relevant life story rights had been sewn up by someone else. If enforceable property

---

48. UNIFORM COMPUTER INFORMATION TRANSACTIONS ACT (Proposed Official Draft, Feb. 2000) <http://www.law.upenn.edu/bll/ulc/ucita/ucita200.htm>. UCITA is a proposed uniform state law to facilitate the electronic licensing of rights in information products by allowing proprietors of information products to condition access on the acceptance of a "license" constraining use of the information revealed in the product, without requiring consumers to know the license terms before agreeing to be bound by them. *See generally* Carol A. Kunze, *UCITA Online* (last modified Mar. 14, 2000) <http://www.ucitaonline.com>.

49. *See* Jessica Litman, *The Tales that Article 2B Tells*, 13 BERKELEY TECH. L.J. 931 (1998) (arguing that UCITA, formerly known as Article 2B, makes up rights out of thin air and then characterizes them as well-established).

50. *See, e.g.*, Carson v. Here's Johnny Portable Toilets, Inc., 698 F.2d 831 (6th Cir. 1983) (upholding right of publicity claim where plaintiff had licensed "Here's Johnny" for restaurants, clothing, and cologne); Lerman v. Chuckleberry Publ'g, Inc., 521 F. Supp. 228, 232 (S.D.N.Y. 1981) (explaining that an individual claiming a right of publicity must have commercially exploited his own name or likeness). *See generally* Diane Leenheer Zimmerman, *Who Put the Right in the Right of Publicity?*, 9 DEPAUL-LCA J. ART & ENT. L. 35 (1998) (examining the history and recent expansion of the right of publicity).

51. *See generally* MELVIN SIMENSKY & THOMAS D. SELZ, ENTERTAINMENT LAW 572-603 (2d ed. 1997) (providing background on life story rights and agreements for their exploitation).

52. *See, e.g.*, Seale v. Gramercy Pictures, 964 F. Supp. 918, 929-31 (E.D. Pa. 1997) (dismissing Bobby Seale's right of publicity and false light claims arising from his portrayal in unauthorized docudrama).

rights can be wished into being, then why not wish for a property right in personal data?

To objections that individualized negotiations over disclosure and use of discrete facts would be unwieldy,[53] hopeful proponents of the privacy property model insist that, as computer technology develops, individuals will be able to delegate all of their dickering to intelligent software agents. Transaction costs for negotiation are or will soon be so low that individuals will be able to reach individualized bargains about the use and disclosure of their data.[54]

Whether or not it could be easily implemented, a privacy-as-property solution carries with it some serious disadvantages. Our society has a long-standing commitment to freedom of expression. Property rights in any sort of information raise significant policy and free speech issues.[55] Facts are basic building blocks: building blocks of expression; of self-government; and of knowledge itself. When we recognize property rights in facts, we endorse the idea that facts may be privately owned and that the owner of a fact is entitled to restrict the uses to which that fact may be put. That notion is radical. It is also inconsistent with much of our current First Amendment jurisprudence.[56] Thus, the idea of creating property rights in personal data

---

53. *See, e.g.*, Dreyfuss, *supra* note 19, ¶ 27.

54. *See, e.g.*, Lessig, *supra* note 19, at 17-18 (describing P3P, a standard for negotiating protocols on the Web that would quickly determine whether a Web site's privacy practices match the user's preferences); *Developments in the Law—The Law of Cyberspace*, *supra* note 19, at 1647-48 (same); *see also* notes 74-77 *infra* and accompanying text.

55. *See* BRANSCOMB, *supra* note 22, at 177-86 (discussing tension between society's interest in facilitating proprietary control over information and its interests in promoting free access to and use of information); Wendy J. Gordon, *On Owning Information: Intellectual Property and the Restitutionary Impulse*, 78 VA. L. REV. 149, 153-63, 267-81 (1992) (discussing free speech and information policy issues raised by ownership of information); J.H. Reichman & Pamela Samuelson, *Intellectual Property Rights in Data?*, 50 VAND. L. REV. 51, 56, 63-72 (1997) (analyzing free speech and information policy implications of broad intellectual property rights in information).

56. *See, e.g.*, Milkovich v. Lorain Journal Co., 497 U.S. 1, 19-21 (1990) (cataloging First Amendment limitations on defamation); Florida Star v. B.J.F., 491 U.S. 524 (1989) (elaborating First Amendment restrictions on the punishment of truthful disclosure); Gertz v. Robert Welch, Inc., 418 U.S. 323 (1974) (cataloging First Amendment limitations on defamation); Jessica Litman, *Reforming Information Law in Copyright's Image*, 22 U. DAYTON L. REV. 587, 600-10 (1997) (discussing First Amendment constraints on copyright protection). No current legal regime in the United States offers property protection to facts qua facts. Copyright law leaves facts unprotected. *See* Feist Publications, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340 (1991). Trade secrecy limits its protection to preventing disclosure of a trade secret by those who learn of it within a confidential relationship. *See* RESTATEMENT (THIRD) OF UNFAIR COMPETITION §§ 40-42 (1995) (defining trade secret appropriation). Even H.R. 354, the controversial database bill, doesn't purport to give property protection to individual facts. Instead, it casts its protection as defending the effort and expense of compiling valuable collections of data from commercial piracy. *See* Collections of Information Antipiracy Act, H.R. 354, 106th Cong. (1999); H.R. REP. NO. 106-349, at 9-12, 16-19, 25 (1999) (providing background on and purpose of proposed legislation). Nonetheless, the bill is widely, if not universally, criticized as unconstitutional. *See, e.g.*, Yochai Benkler, *Constitutional Bounds of Database Protection: The Role of Judicial Review in the Creation and Definition of Private Rights in Information*, 15 BERK. TECH. L.J. (forthcoming 2000) (concluding that H.R. 354 is

raises fundamental constitutional issues.[57] If it looked likely that a property rights model would prove to be an effective tool for protecting personal data privacy, it might be worthwhile to balance the privacy and free speech interests to see which one weighed more. As I argue in Part II, however, a property rights model would be ineffective in protecting data privacy. It would, in all likelihood, make the problem worse.

II

> Property interests are, in general, alienable. If a particular property interest is not alienable, this result must be due to some policy against the alienability of such an interest. The policy of the law has been, in general, in favor of a high degree of alienability of property interests. This policy arises from a belief that the social interest is promoted by the greater utilization of the subject matter of property resulting from the freedom of alienation of interests in it.
>
> —RESTATEMENT OF PROPERTY[58]

The raison d'être of property is alienability; the purpose of property laws is to prescribe the conditions for transfer. Property law gives owners control over an item and the ability to sell or license it. The control, denominated a "right to exclude" in property-speak, is akin to different sorts of control conferred by different branches of the law.[59] It would be unnecessary to treat an interest as property in order merely to protect it from invasion. Such protection is the traditional province of tort law. The law of battery protects the integrity of the body, even though people's bodies are no longer deemed property.[60] The law of defamation protects the integrity of the reputation, even though people's reputations are not property.[61] Anti-discrimination laws prohibit a wide range of discriminatory acts, even though the interest in freedom from invidious discrimination is not property.

---

unconstitutional under both the Copyright Clause and the First Amendment); Letter from Marci A. Hamilton, Director, Intellectual Property Law Program, Cardozo School of Law, to Rep. Howard Coble, Chair, Subcommittee on Courts and Intellectual Property (Feb. 9, 1998) <http://www.yu.edu/csl/law/hr2652.pdf>) (expressing the view that the Collections of Information Antipiracy Act, H.R. 2652, 105th Cong. (1998), is unconstitutional).

57. *See* ALDERMAN & KENNEDY, *supra* note 5, at 329 ("The idea that one can 'own' a name or other basic identifying information raises serious First Amendment concerns.").

58. RESTATEMENT OF PROPERTY § 489 cmt. a (1944).

59. *See* Wendy J. Gordon, *An Inquiry into the Merits of Copyright: The Challenges of Consistency, Consent, and Encouragement Theory*, 41 STAN. L. REV. 1343, 1354-61 (1989) (explaining "right to exclude").

60. When people were treated as property, of course, beating one was not deemed to be a battery but a trespass to chattels. *See, e.g.*, McRaeny v. Johnson, 2 Fla. 520, 524 (1849) (recognizing trespass to chattel action for injury to plaintiff's slave); Carmouche v. Bouis, 6 La. Ann. 95 (1851) (holding defendant liable to slaveholder for slave's value).

61. But see Ronald J. Krotoszynski, Jr., *Fundamental Property Rights*, 85 GEO. L.J. 555, 610-12 (1997), for the argument that reputation is a "fundamental property interest" that should therefore be constitutionally protected under a revived doctrine of substantive due process.

We deem something property in order to facilitate its transfer. If we don't intend the item to be transferred, then we needn't treat it as property at all.[62] If we do intend to encourage its sale, a property model does the job admirably.[63] Thus, we have resorted to the property model for intangible interests when we want to make it easy to sell them.[64] Intellectual property is the paradigmatic example.

In United States copyright law, for instance, both statute and long tradition ensure that all parts of the copyright can be sold; almost nothing is inalienable.[65] The purchaser of a copyright steps into the author's shoes, and the author becomes a stranger to the rights in the copyright bundle. If she should then reproduce the work, or create a new one based on it, she may find herself in court facing a copyright infringement suit.[66] If an author sells her copyright, it is as nonsensical to assert that she has some continuing interest to use her work as it would be to insist that your landlord retains some implicit right to move in with you and your family, or that the seller of your home could continue to hang out on your front porch over your family's objections because she repaired and repainted it. In U.S. copyright law,

---

62. Indeed, the law of eminent domain enables us to *force* the owner of any item denominated as property to transfer the item to the government at the market price. If it isn't property, on the other hand, it isn't subject to condemnation. *See generally* 26 AM. JUR. 2D *Eminent Domain* § 99 (1996) ("[T]he right of eminent domain encompasses property of every kind and character, whether real or personal, tangible or intangible . . . .") (footnote omitted).

63. In 1886, for instance, frustrated because large expanses of resource-rich western land had been set aside for Indian reservations and were therefore unavailable for settlement and mining, Congress passed the General Allotment Act of 1887, ch. 119, 24 Stat. 388 (reversed by the Indian Reorganization Act, ch. 576, 48 Stat. 984 (1934) (codified as amended at 25 U.S.C. §§ 461-479 (1983))). The Allotment Act divided reservation land into parcels and allotted each parcel to an individual Indian. The parcels were held in trust for a term of years, after which each Indian succeeded to fee ownership of his parcel. In 1934, Congress repudiated the allotment program, but not before it had accomplished its purpose. After 48 years, 90 million acres of Indian land had passed into non-Indian ownership. *See* Blackfeet Tribe of Indians v. Montana, 729 F.2d 1192, 1195-98 (9th Cir. 1984), *aff'd*, 471 U.S. 759 (1985).

64. *See, e.g.*, Paige v. Banks, 80 U.S. (13 Wall.) 608, 614-15 (1871).

65. The sole exceptions are the rights to terminate transfers in 17 U.S.C. §§ 203, 304(c) (1994). Termination rights are hard to exercise and hedged with conditions and limitations, but they may not be assigned or waived in advance. Other reversionary features of the copyright, like the contingent future interest in the copyright renewal term, are freely assignable. *See* Fred Fisher Music Co. v. M. Witmark & Sons, 318 U.S. 643 (1943) (holding that an author may assign contingent renewal interest); Mills Music, Inc. v. Snyder, 469 U.S. 153 (1985) (holding that author could not recapture royalties payable to intermediate assignees). Free alienability of copyright interests is far from inherent. Many other countries treat copyright as more of a personal right than a property right, and restrict alienability accordingly. *See, e.g.*, Eugen Ulmer and Hans Hugo von Rauscher auf Weeg, *Germany (Federal Republic), in* STEPHEN M. STEWART, INTERNATIONAL COPYRIGHT AND NEIGHBORING RIGHTS 414, 426-33 (2d ed. 1989) (describing Germany's copyright regime).

66. *See, e.g.*, Fogerty v. Fantasy, Inc., 510 U.S. 517 (1994) (infringement action by holder of song copyright against original composer); Schiller & Schmidt, Inc., v. Nordisco Corp., 969 F.2d 410 (7th Cir. 1992) (infringement action by owner of mail order supply company against former employee for replicating catalogue design); Gross v. Seligman, 212 F. 930 (2d Cir. 1914) (action by holder of photograph copyright against photographer for using similar composition).

moreover, an individual who creates a work within the scope of her employment owns nothing at all—his employer is deemed the author for all purposes.[67] Should the employee depart for a different position, the law requires him to leave his creative output behind.[68]

The chief justification for so thoroughly commodifying rights in creative output is that it facilitates their transfer and exploitation.[69] In the copyright context, easy transfer allows the purchase of copyright rights by the entity best situated to exploit them, and easy exploitation persuades authors and distributors to invest their resources in the creation and dissemination of works of authorship, while encouraging the widest profitable distribution of copyrighted works.[70]

Casting copyright as a property right also allows the copyright owner to control the terms and conditions of its exploitation by others. If privacy is a property right, and individuals have an ownership interest in facts that describe them, then one can imagine that the property right would enable them to control the use of those facts, and people who cared about their own data privacy would have the means to secure it.[71]

That impression rests, however, on the unwarranted assumption that initial legal ownership of facts would enable individuals to restrain their downstream use by negotiating conditions of use before disclosing them. That assumption seems to be inspired by a fairy-tale picture of easy bargaining in cyberspace through the use of intelligent agents. Commentators have suggested that transaction costs for negotiation are, or will soon be, so low that individuals can reach individualized bargains about the use and disclosure of their data.[72] That's nonsense. Transaction costs are a trivial part of the

---

67. *See* 17 U.S.C. § 201(b) (1996).

68. *See, e.g.*, Miller v. CP Chems., Inc, 808 F. Supp. 1238 (D.S.C. 1992) (holding that employer owned all rights in programs written by discharged employee).

69. *See* 1 PAUL GOLDSTEIN, COPYRIGHT: PRINCIPLES, LAW AND PRACTICE 3-11 (1989) (describing purpose of U.S. copyright law).

70. *See, e.g.*, Stanley M. Besen & Leo J. Raskind, *An Introduction to the Law and Economics of Intellectual Property*, 5 J. ECON. PERSP. 3 (1991) (providing a basic introduction to the economics of intellectual property law).

71. *See* Samuelson, *supra* note 19, at 771.

72. The Platform for Privacy Preferences (P3P) is one proposed system of protocols through which Web site providers and Internet users can reach agreement on privacy preferences:

> A P3P regime will result in the optimal level of privacy protection because it permits individuals to value privacy according to their personal preferences. Individual users will configure their privacy preferences to protect privacy according to the value that they attach to it. In the resulting privacy market, those who value their personal information less will part with it more easily than those who value it more. This market will likely result in a de facto level of privacy protection, in which the interests of information collectors are balanced against the interests of individual users and site operators. Because this market features intense competition and very low transaction costs, the resulting de facto level of protection is likely to be the most allocatively efficient solution, reflecting the aggregate of individual preferences.

problem. Allowing consumers to communicate their privacy preferences cheaply, transparently, and automatically gains them little they don't already have. Customers could communicate their preferences now, exceedingly cheaply, when they applied for their credit cards, or even used them. Credit card companies could add a box to the standard form; checking that box would allow the cardholder to opt out of any data reuse or sharing related to that transaction. Customers could present their shopper advantage cards to the cashier and advise him that today's purchases (or even particular items in the shopping basket) are confidential; the cashier could enter some four-digit code to indicate this. Banks and supermarkets don't do that, however, not because it is expensive to allow a customer to express her preference, but because it would be expensive to honor it. The transaction costs involved in specifying one's personal privacy preferences are not a major reason why one is never given the opportunity to do so.[73] Rather, the cost of honoring such preferences makes it infeasible. Putting aside all of the money forgone if the merchant exempts the data from slicing, dicing, and renting, there is the bookkeeping nightmare of keeping data subject to a variety of different constraints. The intelligent agent model doesn't address that problem at all.

The poster child for privacy protection through customized computer code is the Platform for Privacy Preferences (P3P), the privacy specification developed by the World Wide Web Consortium.[74] P3P is a protocol intended to be used with Internet browsing software to enable individuals to set customized privacy preferences. The P3P literature suggests that I might program my P3P agent to understand that I refuse to identify myself except to entities that promise that they will neither analyze the data generated by my transactions to bring me offers of new products that might interest me, nor sell or rent that data to any third parties, but will instead use the information I supply only for the purpose of completing the transactions for which I

Developments in the Law—The Law of Cyberspace, *supra* note 19, at 1647-48 (footnotes omitted); *see also* Lessig, *supra* note 19, at 17-18.

73. Anyone who is serious about preventing the deposit of cookies on her hard disk has long ago abandoned the strategy of refusing any cookies she doesn't want; websites that rely on cookies have adopted a variety of clever devices to ensure that that doesn't work. Some sites refuse access to browsers that don't accept cookies; others fire off dozens of successive cookie requests before loading webpages; all sites encode their cookies in indecipherable text so that one cannot tell whether any given cookie contains innocuous or sensitive information. There are other solutions, ranging from using software or proxy servers to cause your computer to seem to accept cookies when it does not, to using software tools to remove cookies after you've received them. My only point is that the cheapness of the click-through, "yes/no" transaction for accepting individual cookies has not generated a market permitting the selective rejection of cookies, because operators of websites have apparently concluded that they'd prefer not to facilitate such a market by informing individuals what information particular cookies contain and what purpose each cookie is intended to serve.

74. *See generally* World Wide Web Consortium, *Platform for Privacy Preferences (P3P) Project* (last modified Mar. 5, 2000) <http://www.w3.org/P3P/>.

supply it.[75] Whenever I visit a Web site that doesn't make such promises, P3P will inform me that I've hit a data privacy black hole, and offer me the option to change my mind about the conditions I impose. In theory, P3P could support multiple iterations of offer and counter-offer.[76] So, I can surf over to Bank One on the Web, and apply for a credit card.[77] P3P will advise Bank One that it can't find out who I am unless it promises not to reuse my data, and Bank One will advise P3P that it can respect that, but it won't give me a credit card. In theory, P3P could then suggest that I would be willing to accept a promise to reuse my data in-house so long as Bank One didn't sell it to anyone else. Bank One might tell P3P that that was all very well, but I still couldn't have a credit card. If I wanted to, though, Bank One would permit me to apply for the card under the standard circumstances, but would, in addition, allow me to advise Bank One that I did not want to receive unsolicited commercial come-ons; Bank One would be sure to pass this on to firms who care about such things. P3P would terminate the transaction and I would go visit some other bank-on-the-web, where an identical series of "negotiations" would ensue. At the end of the day, I would not yet have a credit card, but my bargaining costs would have been small. Of course, I can do all of that now, even more cheaply, by picking up the telephone and calling Bank One at 1-800-Bank-One. (I encourage you to try it to see how reliably it works.) In short, businesses that do not now protect data privacy are unlikely to be motivated to do so by the fact that it will be easy and cheap for their customers to request it.

Second, and more fundamentally, if a right is proprietary, it is normally fully alienable. The concept of alienable ownership rights in personal data is disturbing, because the opportunities to alienate are ubiquitous. Most obviously, there is the implicit information barter system that characterizes many consumer transactions, and is exemplified by commercial World Wide Web sites.[78] Information, goods, and services are free and freely available in return for a little volunteered demographic information, a dollop of attention, and the ability to record, slice, dice, correlate, and sell the clickstream data generated by your forays onto the Internet.[79] Because those data are valuable, data miners are already pressing claims to proprietary interests in the

---

75. *See* Lorrie Faith Cranor & Joseph Reagle Jr., *Designing a Social Protocol: Lessons Learned from the Platform for Privacy Preferences Project*, *in* TELEPHONY, THE INTERNET, AND THE MEDIA, ch. 12 (Jeffrey K. MacKie-Mason & David Waterman eds., 1998), *manuscript available at* <http://www.w3.org/TR/NOTE-TPRC-970930/> (made available by the World Wide Web Consortium for discussion only).

76. *See id.*; *see also* sources cited in note 72 *supra*.

77. *See* Bank One, *Bank One Home Page* <http://www.bankone.com>.

78. *See* Litman, *supra* note 56, at 615-17.

79. *See, e.g.*, Saul Hansell, *In Wired World, Much Is Free at Click of a Mouse*, N.Y. TIMES, Oct. 14, 1999, at A1 (describing how consumers exchange personal information for goods and services).

information they compile. Those claims rest on the effort and investment they have expended in amassing their collections.[80] If data miners could claim individual data as their property, though, the value of each datum would increase because the proprietor would be entitled to control it exclusively. This, in turn, would greatly enhance the incentives to collect as much data as possible, which would induce ever more rapacious collection of personal information. (This is, after all, precisely how the property rights model is supposed to work.[81])

Imagine the commercial world wide web in a world that treats personal data as alienable personal property. If personal data are alienable, then by ordering that free computer, downloading that free MP3 recording of a hit song, downloading and installing that software, you will surely have consummated the transfer. We could make a rule that the terms of such a transfer must be disclosed as part of the inevitable click-through license, and just as surely, they would be, and everyone would click "I accept" without even reading them. Indeed, arguably, for any website for which access requires clicking an "I accept" box, the fact that you, for instance, read the *New York Times* on the Web at a considerable savings over the newsstand rate will support the claim of transfer.

It's no better out here in meatspace. Imagine that a person, and let's for the sake of convenience and brevity call her "I," has initial ownership of information about herself, that is, me. I sign up for a check cashing card at the supermarket, or a shopper's club discount card, and, in return for the convenience of paying by check or a steady stream of small discounts on products I may or may not buy, I waive, forfeit, or assign any ownership rights I might have in whatever information resides in an ongoing record of my purchases.

The store, meanwhile, has its own proprietary interest in the compiled purchasing records of each and all of its customers, and will rely on that interest to sell facts about me to whomever. Whomever, of course, has a prop-

---

80. *See, e.g.*, *Information Anti-Piracy Bill: Hearing on H.R. 354 Before the Subcomm. on Courts and Intellectual Property of the House Comm. on the Judiciary*, 106th Cong. (1999) (statements of Marybeth Peters, Register of Copyrights; Terrence M. McDermott, Executive Vice President, Nat'l Assoc. of Realtors; Dan Duncan, Vice President, Government Affairs, Software & Info. Indus. Assoc.; and Michael Kirk, Executive Director, Am. Intellectual Property Law Assoc.) <http://www.house.gov/judiciary/106-ct18.htm>; *Copyright Protection of Information on the Internet: Hearing on H.R. 1858 Before the Subcomm. on Telecomm., Trade & Consumer Protection of the House Comm. on Commerce*, 106th Cong. (1999) (statement of Henry Horbaczewski, Senior Vice President and General Counsel, Reed Elsevier, Inc., on behalf of the Coalition Against Database Piracy) <http://com-notes.house.gov/cchear/hearings106.nsf/768df0faa6d9ddab852564f1004886c0/c5d12be951ffc45a8525679000583a95?OpenDocument> (supporting federal database protection legislation).

81. *See, e.g.*, Jane C. Ginsburg, *Creation and Commercial Value: Copyright Protection of Works of Information*, 90 COLUM. L. REV. 1865, 1907-12 (1990) (discussing incentive rationale for copyright).

erty interest in those facts because it paid for them, and will be able to combine them with facts about other people and more facts about me from other sources. Whomever may use that collection of data to make up a list of people who are ripe for Discover Card® solicitations, or who might be interested in a mail order catalog for folks suffering from depression, or who, based on recent medical and pharmaceutical purchases, might be eager to purchase some no-questions-asked life insurance.

What makes the whole situation worse is that privacy is one of those things that many people don't believe they really need until they find themselves with something to keep secret. If easy assignment is the rule, they may no longer have the power to preserve their secrecy; even if they could, the exceptional nature of their asserting a privacy claim will tip off those from whom this is a secret that there is an interesting secret there. So, if someone who is deemed to have waived any property rights in the information supplied to businesses in return for product discounts should suddenly find himself diagnosed with hemorrhoids, or herpes, or HIV, he may have no practical way to recapture his secrecy.

Now, imagine the world we have made. We each owned our own personal data initially, but we've assigned them for value to some business, which has sold them to some other business, which combines them with other data to generate a profile of each of us, and sells or rents that profile out. Nor is it unrealistic to imagine those businesses asserting their property interest in their collections of data: There is a lot of that going around.[82] In October, the *New York Times* reported that the NIH Recombinant DNA Advisory Committee had been stymied in its efforts to require more complete disclosure of the safety problems encountered in gene therapy by pharmaceutical companies' insistence that that information is proprietary.[83]

The market in personal data is the *problem*. Market solutions based on a property rights model won't cure it; they'll only legitimize it.[84]

III

> The truth of the matter is that we will never succeed in preventing powerful institutions or individuals from collecting as much information about others as they can. Nor will we stop folks from constantly sifting, correlating, and drawing conclusions about their neighbors—even things that are "none of their

82. *See, e.g.*, U.S. West, Inc. v. FCC, 182 F.3d 1224, 1247-48 (10th Cir. 1999) (Briscoe, J., dissenting) (describing Takings Clause argument against FCC regulations); *see also* note 80 *supra*.

83. *See* Sheryl Gay Stolberg, *U.S. Panel Moves to Force Disclosure in Gene Testing*, N.Y. TIMES, Oct. 30, 1999, at A10.

84. *See* Davies, *supra* note 10, at 160 ("Privacy's journey from the political realm to the consumer realm invokes a new set of relationships and values. Placing privacy in the 'free market' environment along with such choices as color, durability, and size creates an environment in which privacy becomes a costly 'add-on.'").

> business." That is because the underlying impulse goes beyond issues of power or profit. It is deeply rooted in human nature.
>
> —David Brin[85]

So, what's to be done? The property model has been sponsored by supporters of privacy who have concluded that other solutions are unlikely. If it offers only illusory protections, though, are there any potential solutions left? If no solution is practical, why not come out in favor of one's favorite of the impractical approaches? There's a certain emotional satisfaction to endorsing a plan that, while no more realistic than any of the others, offers the greatest moral or aesthetic virtue of the bunch. Science fiction author David Brin's answer, for instance, is a state of being that he calls "reciprocal transparency," in which ubiquitous electronic surveillance devices make all details about every citizen freely available to every other citizen.[86] Others dream that the United States will adopt laws modeled on the EU directive.[87] One of my favorites has always been the opposite of the personal-data-as-property model. Under this model, personal information could not be property, and it would be illegal to buy it or sell it.[88] One might still lawfully gather it and even charge for the service of gathering, and one might certainly give it away gratis, but nobody would own it because personal data could not be owned. If the people who believe that intellectual property incentives encourage behavior to generate property are right, this could have

---

85. DAVID BRIN, THE TRANSPARENT SOCIETY: WILL TECHNOLOGY FORCE US TO CHOOSE BETWEEN PRIVACY AND FREEDOM? 244 (1998).

86. *See id.* at 80-84.

87. *See, e.g.*, *Issues in U.S.-European Union Trade: European Privacy Legislation and Biotechnology/Food Safety Policy, Hearing Before the House Comm. on Int'l Relations*, 105th Cong. (1998) (statement of Marc Rotenberg, Executive Director, Electronic Privacy Information Center) <http://commdocs.house.gov/committees/intlrel/hfa50549.000/hfa50549_0f.htm.>; Transatlantic Consumer Dialogue, *Recommendations on Electronic Commerce* (last modified Oct. 4, 1999) <http://www.tacd.org/meeting2/electronic.html> (Doc Ecom-8-99: Safe Harbor Proposal and International Convention on Privacy Protection; Doc Ecom 11-99: Comments on the US Department of Commerce "Safe Harbour Proposal"; Doc Ecom-18-00: TACD Resolution on Safe Harbor Negotiations).

88. This isn't as un-American as it might seem at first. There are lots of things in U.S. law that are currently legally impossible to own: people, constitutional rights, navigable waterways, airways. They can't be owned because the law treats them as items not susceptible of private ownership, notwithstanding that they surely could be treated as property, and in other cultures and other historical eras of our culture were so treated.

What about trade secrets? Customer lists and the like? I've got the same glib answer to that question I had several years ago, and I still believe it would work. Trade secrecy is a blend of property and confidentiality and often covers things that by definition can't be property, like the details of an unpatentable process, which are protected from misappropriation because of the value the law attaches to confidentiality and loyalty. Here, one could protect a customer list or other collection of personal data so long as it remained secret and no longer, by adopting a rule that one can keep and use the information one collects but cannot sell it. The same rule would apply to a hospital and a credit card company (both of which have duties of confidentiality to the customers and patients whose data they collect) and to a credit agency (which may not). *See* Jessica Litman, *After Feist*, 17 U. DAYTON L. REV. 607, 615-16 (1992).

the salutary effect of reducing the irksome behavior of compiling, correlating, and packaging personal data and transactional information. If the believers in incentives are wrong, no harm would have been done, and we would have struck a symbolic blow for the principle that facts cannot be owned. Collecting and selling this stuff is, after all, a behavior that most of us deplore, although many seem unwilling to regulate it into demise. But a social statement that "this is not a good thing" is valuable in the same way that a social statement that selling drugs, or sex, or embryos, or infants is not a good thing is valuable, even if it does little to undermine the profit market in the thing.[89] It says that we value privacy enough to find the collection and sale of personal information to be unacceptable. What Brin's reciprocal transparency proposal and my anti-property proposal have in common is that they are even less plausible than the ones that have so far failed of adoption.

Do we really have a wrong with no credible remedy? Certainly, there are plenty of those out there. (The reader is invited to make her own list.) Is the data privacy problem necessarily one of them? Is it possible instead that we've been trying to find the remedy in the wrong closet? If the wrong doesn't fit the models we've been trying to cram it into, then the fact that industry, Congress, and the courts haven't seemed to take those models seriously may not mean that there is no workable solution.

The appeal of the property model derives chiefly from the fact that property rights can be recognized as a matter of state common law without invoking the federal regulatory machinery, which seems too helpless, pernicious, or corrupt (depending on your political persuasion) to offer any meaningful solutions. The weaknesses of the property model are, first, that it encourages transactions in data that most of us would prefer be discouraged and, second, that its reliance on alienability and easy waiver tend to vest control over personal data in the data miner rather than the data's subject.[90] Before succumbing to despair, then, it is worth considering whether there's an approach that might take advantage of some of the strengths without incorporating the features that I have argued are pernicious.

In 1976, a man named John Moore sought treatment for hairy cell leukemia from one David Golde, M.D. Dr. Golde removed Moore's spleen for therapeutic reasons, and then used tissue from the spleen in his own research. On Dr. Golde's instructions, Moore returned periodically to allow Golde to obtain additional blood and tissue samples, believing these tests to be necessary for the treatment of his condition. Golde ultimately succeeded in estab-

---

89. *See* Jessica Litman, *Copyright Noncompliance (Or Why We Can't "Just Say Yes" to Licensing)*, 29 N.Y.U. J. INT'L L. & POL. 237, 240 (1997) (discussing the symbolic power of laws).

90. *See, e.g.*, Dreyfuss, *supra* note 19, at ¶30.

lishing a cell line from Moore's tissue, patented the cell line, and entered into lucrative agreements for its commercial development.[91]

Moore sued Golde for conversion of his spleen cells, claiming that Golde's commercial exploitation of his cells invaded Moore's property interest in the parts of his own body. The California Supreme Court rejected Moore's claim to a continuing ownership interest in the tissue.[92] It nonetheless upheld his complaint against Dr. Golde on the ground that Golde had breached his fiduciary duty to his patient by failing to disclose his intention to use Moore's cells in his own research, and to obtain Moore's informed consent to treatment procedures by fully apprising Moore of his dual purpose in performing them.[93]

Moore's property claim failed; the court, however, found Dr. Golde's conduct actionable in tort. Tort law, like property law, derives from common law and is traditionally the province of the states. Tort law, even more than property law, is still largely a common-law preserve. More importantly, tort law's main line of work is protecting interests from invasion, whether or not those interests are property-like. A tort law solution to the problem of personal data privacy would carry some of the appeal of the property model without the most prominent drawbacks. Unfortunately, as the literature has made very clear, the invasion of privacy tort is too narrowly defined to serve.[94] A tort law solution would need to be found somewhere other than in the common law of privacy.

IV

> To the Editor:
>
> When my husband worked for a company that made baby formula, I asked a colleague how the marketing staff got the names of pregnant women . . . . Was I shocked! The staff bought the names from doctors' offices. He told me that most offices thought that they were doing their patients a favor by releasing the information.
>
> —Letter in the *New York Times*[95]

---

91. *See* Moore v. Regents of the Univ. of Cal., 793 P.2d 479, 480-82 (Cal. 1990). Cell lines make it possible to use cells in biomedical research; those created from unusual cells can generate millions of dollars. *See id.* at 482.

92. *See id.* at 487-97.

93. *See id.* at 485-86. It's worth emphasizing that Moore had signed a standard consent form prior to having blood and tissue samples taken after the surgery, and that that form included the usual boilerplate about medical research. *See* Moore v. Regents of the Univ. of Cal., 249 Cal. Rptr. 494, 510 (Cal. Ct. App. 1988), *aff'd in part, rev'd in part*, 793 P.2d 479 (1990).

94. *See, e.g.*, Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1634 (1999) (arguing that common law limitations make state tort less than useful); Gellman, *supra* note 36, at 209-12 (arguing that tort remedies are not responsive to privacy concerns raised in the computer era).

95. Jillayne Arena, Letter to the Editor, N.Y. TIMES, Nov. 25, 1999, at G5.

In 1987, the Senate failed to confirm Judge Robert Bork's nomination to the Supreme Court. In the course of Judge Bork's confirmation hearings, Washington's weekly *City Paper* published a profile of the judge based on his family's video tape rental records.[96] Public dismay inspired federal and state legislators to introduce laws prohibiting video rental stores from revealing customers' rentals, and Congress quickly passed one of the few federal laws protecting consumers' data privacy.[97]

In July of 1997, newspapers reported that America Online had contracted to sell the telephone numbers of its 8.5 million subscribers to telemarketers.[98] AOL had posted a notice a month earlier advising subscribers of its upcoming policy change, but had apparently not located the notice anywhere that most subscribers would encounter it. Dismayed subscribers flooded the company with angry telephone calls and email messages. AOL announced the following day that it was abandoning its plans.[99]

In February of 1998, *The Washington Post* reported that the CVS pharmacy chain was sending confidential prescription information to Elensys, a Massachusetts computer database marketing company that tracked patients who failed to refill their prescriptions and sent them letters on pharmacy letterhead, sometimes sponsored by drug companies. The letters reminded the customers to refill their prescriptions, or recommended new products appropriate for their apparent conditions.[100] Consumers were outraged; the story was a public relations disaster. Initially, CVS defended the arrangement as beneficial to its customers.[101] Four days later, it terminated the program.[102]

---

96. *See* Editorial, *Invasion of Video Privacy*, WASH. POST, Sept. 30, 1987, at A18; Michael deCourcy Hinds, *Personal but Not Confidential: A New Debate over Privacy*, N.Y. TIMES, Feb. 27, 1988, Consumer's World at 56.

97. *See* Video Privacy Protection Act of 1988 § 2(a)(2), 18 U.S.C. § 2710 (1994). Note that the statute prohibits video rental stores from revealing personal information, rather than regulating what some third party might do with such information if it were improperly revealed.

98. *See, e.g.*, Rajiv Chandrasekaran, *AOL Will Share Users' Numbers for Telemarketing*, WASH. POST, July 24, 1997, at E1.

99. *See* Editorial, *Direct Democracy, Net-Style*, WASH. POST, Aug. 2, 1997, at A18 (describing public's negative reaction); Rajiv Chandrasekaran, *AOL Cancels Plan for Telemarketing*, WASH. POST, July 25, 1997, at G1. That doesn't mean that AOL has stopped trying to exploit the personal information it collects from its subscribers. A little over a year after AOL rolled out an elaborate subscriber opt-out policy, it informed subscribers who had exercised the opt-out option that their preferences were due to expire, and if they wanted to protect their subscriber information from rental or sale, they would need to go through the whole opt-out procedure again, every year. *See* Doug Brown, *AOL to Users: Opt Out Again*, INTER@CTIVE WEEK, Nov. 29, 1999 <http://www.zdnet.com/intweek/stories/news/0,4164,2400502,00.html>; Jim Hu, *AOL Users Must Reiterate No-Spam Preferences*, CNET NEWS.COM, Nov. 23, 1999 <http://news.cnet.com/news/0-1005-200-1462616.html>.

100. *See* Robert O'Harrow Jr., *Prescription Sales, Privacy Fears: CVS, Giant Share Customer Records with Drug Marketing Firm*, WASH. POST, Feb. 15, 1998, at A1.

101. *See id.*

In August of 1999, online bookseller Amazon.com announced a new fun feature it called "purchase circles," which allowed customers to find out what other customers in particular cities, schools, or corporations were reading. News reports focused on the privacy implications.[103] The following day, Amazon.com announced a new opt-out option, which allowed customers to keep other customers from finding out what they were reading.[104]

In November of 1999, a software company named RealNetworks found itself in a spot of trouble. RealNetworks distributed the leading audio and video streaming software over the Net as freeware, along with enhanced versions for purchase. The software allowed individuals to view and listen to video and audio content broadcast over the Internet. In 1999, RealNetworks had introduced a new product, called "RealJukebox," which allowed consumers to make digital recordings of music from their own CD collections, store those recordings and others downloaded from the Internet in a virtual jukebox format, and play all of the recordings through their computers using the RealJukebox player software. On November 1, the *New York Times* reported that the RealJukebox software surreptitiously collected information about the user's downloading, recording, and listening behavior, and transmitted that information to RealNetworks every time the user connected to the Internet.[105] Neither the RealJukebox license nor the posted RealNetworks privacy policy had deigned to mention this fact to the individuals who downloaded and installed the software, and the outrage was immediate.[106] By later that same day, RealNetworks had apologized profusely, issued a free software patch that it promised would disable the data gathering and transmission functions, and promised to omit them from all subsequent products.[107] Over the next several days, it appeared that similar undocumented features had been incorporated into the ubiquitous RealAudio, RealVideo,

---

102. *See* Rudolph A. Pyatt Jr., *Ultimately, a Healthy Decision at Giant and CVS Pharmacy*, WASH. POST, Feb. 23, 1998, at F4; Robert O'Harrow Jr., *CVS Also Cuts Ties to Marketing Service: Like Giant, Firm Cites Privacy on Prescriptions*, WASH. POST, Feb. 19, 1998, at E1.

103. *See* Declan McCullagh, *Big Brother, Big "Fun" at Amazon*, WIRED NEWS, Aug. 25, 1999 <http://www.wired.com/news/news/business/story/21417.html>.

104. *Amazon Alters Purchasing Data List Policy*, CNET NEWS.COM, Aug. 27, 1999 <http://news.cnet.com/news/0-1007-200-346529.html>.

105. *See* Sara Robinson, *CD Software Said to Gather Data on Users*, N.Y. TIMES, Nov. 1, 1999, at C1.

106. *See* Courtney Macavinta, *RealNetworks Changes Privacy Policy Under Scrutiny*, CNET NEWS.COM, Nov. 1, 1999 <http://news.cnet.com/news/0-1005-200-1426044.html>; Courtney Macavinta, *RealNetworks Faced with Second Privacy Suit*, CNET NEWS.COM, Nov. 10, 1999 <http://news.cnet.com/news/0-1005-200-1435099.html>.

107. *See* RealNetworks, Inc., *RealNetworks Issues Patch to Address Privacy Concerns of Users* (Nov. 1, 1999) <http://www.realnetworks.com/company/pressroom/pr/99/updateadvisory.html>; RealNetworks, Inc., *RealJukebox Update* <http://www.realnetworks.com/company/privacy/jukebox/privacyupdate.html>.

and RealPlayer freeware.[108] The following week, RealNetworks released a new free version of RealPlayer that it promised would solve the problem.[109] Nonetheless, within a matter of days, three different multi-million-dollar class action lawsuits had been filed against RealNetworks for its data gathering.[110]

None of the businesses caught misusing customer data responded by suggesting that nobody really expected her data to be private in today's world. None claimed that the fact that consumers had chosen to supply the information in the course of voluntary transactions entitled the businesses to do with the data what they wanted. None insisted that it was their ability to reuse the data they collected that enabled them to offer the products that consumers wanted at an attractive price. They apologized, and sheepishly promised not to do it again. They appreciated that when consumers had volunteered their names, addresses, phone numbers, credit card numbers, prescriptions, book choices, and musical preferences, they had done so expecting that the information would be used only to consummate the transaction, and that by reusing that information or sharing it with third parties, they had breached their customers' trust.

But why would consumers expect the merchants they patronize to respect their privacy? They do, of course. When consumers give cashiers personal checks imprinted with their home addresses and phone numbers, they don't expect that information to be extracted and used for any purpose beyond facilitating the payment. If they should discover that the store was routinely using that information to construct telemarketing lists, for example, they'd feel surprised and misused. Nor does that expectation depend on the sensitivity of the data. Should a shopper purchase a copy of Janet Dailey's *Notorious* in a bookstore and a pair of Queen-size control-top panty hose at the lingerie store, those facts are hardly private and only mildly embarrassing. On the other hand, imagine that the bookstore and the lingerie store got together and told each other what books and lingerie she had purchased, and then sold that information to the grocery store, which analyzed it and sent her a coupon for Snackwells® low-fat chocolate-flavored brownie cookie substitute. Isn't what's disturbing about that the fact that when the customer purchased, for example, the panty hose, she believed that she exchanged money for a package of knit nylon, and that she supplied identifying infor-

---

108. *See* Chris Oakes & Jennifer Sullivan, *Real Damage Control—Again*, WIRED NEWS, Nov. 6, 1999 <http://www.wired.com/news/technology/0,1282,32350,00.html>.

109. *See* RealNetworks, Inc., *RealNetworks Publishes Consumer Software Privacy Statement* (Nov. 8, 1999) <http://www.realnetworks.com/company/pressroom/pr/99/software_privacy.html>.

110. *See RealNetworks Is Target of Suit in California over Privacy Issue*, N.Y. TIMES, Nov. 9, 1999, at C16 <http://www.nytimes.com/library/tech/99/11/biztech/articles/09real.html>; *RealNetworks in Real Trouble*, WIRED NEWS, Nov. 10, 1999 <http://www.wired.com/news/politics/0,1283,32459,00.html>; *RealNetworks: Real Sued . . . Again*, USA TODAY (online), Nov. 23, 1999 <http://www.usatoday.com/life/cyber/tech/review/crg603.htm> .

mation for and only for the limited purpose of facilitating the merchant's collection of the money necessary for the exchange? The merchant's later use of that information for a completely different purpose feels like a violation precisely because she assumed at some level that her data would be used only for the purpose for which it was proffered. (Thus, when Independent Counsel Kenneth Starr sought to subpoena the list of book purchases made by Monica Lewinsky from a Washington bookstore, members of the public were outraged that he would even seek such a list or that the bookstore might consider providing it.[111])

Why do we expect the merchants, banks, and insurance companies we deal with to respect our privacy? Part of it, no doubt, derives from social mores left over from a pre-data-mining era. Another part, though, is that merchants, banks, insurance companies, and brokers encourage it.[112] It's profitable. Without that trust, we'd be reluctant to volunteer our credit card numbers; we'd think twice before making embarrassing purchases or watching certain pay-per-view movies. Adulterous spouses would pay for their trysts in cash, and would telephone each other from payphones rather than cellphones.

The reuse, correlation, and sale of consumer transaction data is a straightforward breach of trust—a trust cultivated by and profitable for the recipients of that data. Is it an actionable breach of trust? Under current law, probably not.

Physicians are routinely held to owe fiduciary duties to their patients, and thus unauthorized disclosure of patient information is actionable in tort.[113] Accountants and banks have been held liable for divulging information about their customers.[114] Employees who make unauthorized use of information they gained while on their employers' payrolls are misappropriating trade secrets.[115] The courts insist, however, that the obli-

---

111. *See* Doreen Carvajal, *Book Industry Vows to Fight 2 Subpoenas Issued by Starr*, N.Y. TIMES, Apr. 2, 1998, at A20. Apparently, it did not seem to occur to the journalists who covered the matter to ask what in the world the Kramerbooks store was doing with the data to generate a comprehensive list of purchases by a customer.

112. *See, e.g.*, CVS.com, *Privacy Matters* <http://www.cvs.com/aboutCVS/cvs_privacy.asp> (stating that CVS is a licensee of the TRUSTe Privacy Program and outlining its privacy policy).

113. *See, e.g.*, Horne v. Patton, 287 So.2d 824 (Ala. 1973) (recognizing physician's duty not to disclose information obtained in course of patient's treatment); Cannell v. Med. & Surgical Clinic, 315 N.E.2d 278 (Ill. App. Ct. 1974) (same); Doe v. Roe, 400 N.Y.S.2d 668 (N.Y. App. Div. 1977) (same); McCormick v. England, 494 S.E.2d 431 (S.C. Ct. App. 1997) (same).

114. *See, e.g.*, Rubenstein v. South Denver Nat'l Bank, 762 P.2d 755 (Colo. Ct. App. 1988) (recognizing duty not to reveal information concerning customer's financial affairs); Edward L. Raymond, Jr., Annotation, *Bank's Liability, Under State Law, for Disclosing Financial Information Concerning Depositor or Customer*, 81 A.L.R. 4th 377 (1990).

115. *See, e.g.*, Suncoast Tours, Inc. v. Lambert Group, Civ. Action No. 98-5627 (JEI), 1999 U.S. Dist. LEXIS 17635, at *18-*23 (D.N.J. Nov. 10, 1999); Norand Corp. v. Parkin, 785 F. Supp. 1353 (N.D. Iowa 1990) (granting injunction to prevent former employee from seeking employment with competitor); Integrated Cash Management Servs., Inc. v. Digital Transactions, Inc. 732 F.

gation to keep information confidential derives from the exceptional relationship between the subject and the recipient of the information.[116] Whatever one may say about the context in which merchants, banks, insurance companies, brokers, cable television operators, telephone companies, and Internet websites collect data about their customers, one cannot plausibly call the relationships exceptional.

If breach of confidence captures the essence of the outrage customers feel at the trafficking in their personal information, though, and it seems to, then there must be something in their perception of the relationship with the entities with whom they do business that explains their sense of transgression. The fact that businesses respond to consumer privacy complaints with defensive apologies rather than toughing it out suggests that that perception is one businesses are aware of, intentionally cultivate, and may even to some extent share. The fact, in other words, that every consumer enters into transactions with a large number of merchants, banks, insurance companies, brokers, cable television operators, telephone companies, travel agents, pharmacists, and subscription services doesn't itself negate the claim that the information disclosed within those relationships is disclosed subject to implicit constraints of confidentiality. The employer-employee relationship, after all, is itself hardly exceptional. Rather, there's something about the relationship that fosters the expectation that information learned by the employee in the employer's service will be kept in confidence, notwithstanding objective evidence to the contrary. The merchant-customer relationship generates similar expectations. People give merchants sensitive information—credit card numbers, checking account numbers, unlisted home telephone numbers, the contents of today's shopping basket—in order to consummate commercial transactions, believing the information will be used only for that purpose and then discarded.[117]

Supp. 370, 376-78 (S.D.N.Y. 1989); *see also* RESTATEMENT (THIRD) OF UNFAIR COMPETITION §§ 40-42 (1995).

116. *See, e.g.*, Smith v. Weinstein, 578 F. Supp. 1297, 1307 (S.D.N.Y. 1984), *aff'd*, 738 F.2d 419 (2d Cir. 1984) (asserting that a breach of confidence claim requires a relationship of trust between the parties); Alexander v. Culp, 705 N.E.2d 378 (Ohio Ct. App. 1997) (recognizing clergy's duty to maintain parishioner's confidentiality); Doe v. Roe, 400 N.Y.S.2d 668 (N.Y. App. Div. 1977) (recognizing the same duty between a psychoanalyst and patient); *see also* RESTATEMENT (SECOND) OF AGENCY §§ 395, 396 (1958) (defining agent's duty to maintain confidentiality); RESTATEMENT (SECOND) OF TORTS § 874 (reporter's notes) (1965) ("One breach of fiduciary duty that is more commonly regarded as giving rise to an action in tort is the disclosure of confidential information.").

117. *See Police Charge High-Tech Sleight of Hand*, N.Y. TIMES, Nov. 24, 1999, at B4. If you do any catalog shopping, you may have noticed an incongruity in what data your catalogue merchants keep handy. A number of them insist that although they have your name, address, home phone, and complete purchase history for the past several years at their fingertips, the company retains no record of your credit card number in their files. Presumably, they do this because they think it will make you feel better.

Consummating any given transaction may require that personal data be passed along. Securing payment from a credit card company requires sharing the relevant credit card number; arranging delivery of a package necessitates passing on the relevant address; persuading an insurance company to pay for medical tests probably involves advising an HMO of the reason the tests were ordered.[118] People anticipate that their information may be passed along when necessary, but not retained; they expect that their personal information will not be reused without their consent.

What counts or should count as effective consent has been one of the most contentious issues in the privacy debate. Civil liberties groups have insisted that meaningful consent requires that the default rules prohibit data sale and reuse; consumers should be required to affirmatively "opt-in" to a regime permitting their information to be reused, mined, or sold.[119] Proponents of industry self-regulation have been adamant that consumers wishing to prevent the reuse of their data should be required to "opt-out," by taking (sometimes onerous) affirmative steps to notify all merchants, etc., that they object to common uses of their personal and transactional information.[120] Here, too, tort law has an edge over its common law cousin, property, because tort law has a finely developed jurisprudence of consent.[121] The tort law version of consent doesn't depend on formalities like opt-in or opt-out.

---

118. People probably do not expect that their health insurance companies will get, or have any business demanding, the *results* of those tests except in connection with an authorization for further tests or treatment. *See* HEALTH PRIVACY PROJECT, EXPOSED: A HEALTH PRIVACY PRIMER FOR CONSUMERS 2, 6, 10-11 (1999) <http://www.healthprivacy.org/resources/exposed.pdf>.

119. *See, e.g.*, *Senate Privacy Hearing*, *supra* note 12 (statement of Marc Rotenberg, Electronic Privacy Information Center); *Financial Privacy: Hearing Before the Subcomm. on Fin. Insts. and Consumer Credit of the House Comm. on Banking*, 106th Cong. (1999) (statement of Edmund Mierzwinski, Consumer Program Director, U.S. Public Interest Research Group) <http://www.house.gov/banking/72099mie.htm> (asserting that Congress should enact legislation that "gives consumers the right to opt-in for all information sharing for secondary purposes"); Consumer.Net, *Consumer.Net's Privacy Policy* <http://privacy-policy.com/> ("Opt-In . . . Let the Consumer Decide.").

120. *See, e.g.*, Letter from Daniel L. Jaffe, Assoc. of Nat'l Advertisers, Inc. to Donald S. Clark, Secretary, FTC (Oct. 18, 1999) (available at <http://www.ftc.gov/bcp/profiling/comments/jaffe.htm>) (Online Profiling Project, Comment P994809, Docket No. 990811219-9219-01) (urging the FTC to adopt an opt-out approach).

In theory, consumers have opt-out options now. *See, e.g.*, DIRECT MARKETING ASS'N, PRIVACY PROMISE <http://www.the-dma.org/library/privacy/privacypromise.shtml>. The steps they must take to exercise them, though, are typically both inconvenient and ineffective. *See* Email from Jason Catlett, President, Junkbusters Corp., to Donald S. Clark, Secretary, FTC (Oct. 18, 1999) ¶12 (Online Profiling Project, Comment P994809, Docket No. 990811219-9219-01) (available at <http://www.ftc.gov/bcp/profiling/comments/catlett.htm>) (describing DoubleClick's current opt-out option). AOL, for example, requires subscribers who opt out to repeat the process annually. *See* Brown, *supra* note 99.

121. *See, e.g.*, Moore v. Regents of the Univ. of Cal., 793 P.2d 479, 483-85 (Cal. 1990); Biddle v. Warren Gen. Hosp., 715 N.E.2d 518, 525-29 (Ohio 1999); *In re* A.C., 573 A.2d 1235, 1243-44 (D.C. 1990) (en banc). *See generally* RESTATEMENT (SECOND) OF TORTS §§ 10A, 892, 892A-892D (1965) (defining consent and its limitations).

Rather it requires that the subject appreciate the act that she consents to and be in fact willing that it occur.[122] Apparent consent can be effective when it is reasonable to interpret the subject's behavior as a manifestation of actual willingness.[123] By the same token, consent can be limited in scope:

> If the consent given is restricted to acts within a particular time or a particular area or in other respects, it is effective only within the limits of the restriction. . . . Even when no restriction is specified the reasonable interpretation of the consent may limit it to acts at a reasonable time and place, or those reasonable in other respects. . . .
>
> One important form of restriction is the limitation of the consent to acts done for a particular purpose. When there is a restriction or it is implied from the terms of the consent or the circumstances, the consent may be regarded as conditioned upon the purpose, and it confers no privilege to do the same act for a different purpose.[124]

As the medical malpractice "informed consent" case law demonstrates, adjudication of consent allows the trier of fact to assess the context in which consent was given and the probable understanding of the person giving consent. [125] Data collectors could use whatever method they choose to secure consumers' consent to data collection, reuse, sale, resale, and so forth, subject to the understanding that courts might later evaluate that method to ascertain whether the consumers in fact appreciated and agreed to the data collectors' actions. Faced with that possibility, perhaps the data marketing industry would rethink its fair information practices.

Current tort law does not offer much protection for an individual's data privacy. The breach of trust approach to tort protection is plausible in the sense that one can draw a line that gets from here to there.[126] A relational approach to data privacy protection carries significant intuitive appeal. It seems comparatively innocuous, since its scope can easily be limited by confining the definition of a qualifying relationship. If the concept of breach of trust in fact captures the essence of the wrong, then perhaps courts could be persuaded to take that route to that destination.

---

122. *See* RESTATEMENT (SECOND) OF TORTS §§ 10A, 892 (1965).

123. *See id.* § 892(2).

124. *Id.* § 892A cmt. g.

125. *See, e.g.*, Canterbury v. Spence, 464 F.2d 772, 794 (D.C. Cir. 1972) ("The jury, not [the doctor, is] the final arbiter of whether nondisclosure was reasonable under the circumstances."); Miller v. Kennedy, 522 P.2d 852, 864 (Wash. Ct. App. 1974), *aff'd*, 530 P.2d 334 (Wash. 1975) (same).

126. One hurdle I have not discussed in text is the difficulty of defining the appropriate measure of damages for unauthorized disclosure or misuse of personal information, since without some demonstration of damage there can normally be no tort. Most tort causes of action permit recovery of damages for emotional distress as well as exemplary or punitive damages; this cause of action seems particularly suitable for the latter. Nonetheless the tort approach probably would be more effective in deterring misuse of data than in actually compensating victims for the loss of their data privacy.

V

> Now that intellectual production has become a key economic sector, people have finally begun to realize that information, like time, is money. When they consider the claims of law enforcers, creditors, insurers, direct marketers and other information-intensive industries, they are no longer weighing an amorphous "feel good" interest in privacy against efficiency, savings, jobs, and investment-backed expectations. Now there is hard cash on both sides of the equation and that alters the political calculus. The populace may, in fact, now be ready to press for a new order: It has growing concerns about a legal regime that assigns ownership interests in valuable private information to strangers (and only to strangers).
>
> —Rochelle Cooper Dreyfuss[127]

An approach based loosely on the tort doctrine of breach of confidence might appeal to the courts, especially if recent public response to news reports of data misuse reflect opinions that judges share. That raises the question whether, in the end analysis, it would be worthwhile to push against the edges of tort law to see whether one could stretch them to encompass this new cause of action. The effort involved would be substantial, and unfortunately the payoff ultimately modest.

A tort law breach of trust approach does have significant advantages over a privacy-as-property model. It avoids the trap of alienability and the perverse incentives that a market in alienable personal data would create. Because it forgoes the privacy-rights-management market[128] entirely, it is less likely to legitimize wholesale commercial exploitation of personal information. It would permit courts to give effect to subtle distinctions between consensual and invasive disclosure. Moreover, it has some symbolic value as a statement of societal expectations.

At the same time, a tort approach would be at least as easily achieved as a property-rights regime. Common law tort jurisprudence is still largely intuitive. If breach of trust embodies the essence of what upsets people about the commercial exploitation of their personal information, then it will be easier to persuade courts to endorse the theory. Moreover, the remedy lends itself to incremental adoption and gradual expansion, and may therefore persuade cautious judges that it can safely be deployed a little bit at a time.

The features that make the approach plausible, however, also make it weak. The flexibility of a tort law remedy permits courts to define its scope, by, for example, limiting it based on free speech or information policy issues. It also gives opponents of data privacy opportunities to limit its reach, by seeking narrow definitions of the relationships that it applies to and the sort of information that it covers. The attractiveness of incremental deployment

---

127. Dreyfuss, *supra* note 19, ¶ 3.

128. *See* text accompanying notes 71-77 *supra*.

is also a prescription for sloth. Common law lawmaking is ordinarily both gradual and slow. Although the rare judicial opinion can inspire widespread and rapid endorsement,[129] the litigation process is protracted and resource intensive, and typically yields only incremental change. Before a tort action could have any significant impact on information practices, it would need to be adopted in a critical mass of jurisdictions. If the constraints tort law imposed on data collection and marketing were modest, businesses might alter their approach to data privacy, but only if it seemed easy to do so. If tort law required substantial reforms, most business interests would simply direct their efforts into lobbying Congress to preempt the pesky state tort laws with a data privacy law they found more congenial. Ironically, the widespread adoption of tort law liability for data misuse is perhaps the most realistic scenario for generating some sort of federal law protecting information privacy.

If what data privacy really needs is federal statutory protection, tort litigation is actually a plausible route to enactment. The flaw in such a plan, of course, is the likely content of a law enacted with the support of the direct marketing industry. Viewed realistically, then, pursuing a tort law strategy for privacy protection would be better than a property rights approach not because it would be especially effective, but rather because it would be comparatively benign. Viewed realistically, anything so slow is likely to deliver too little, too late. As the process inches along, more and more data will be compiled into ever more intrusive dossiers. By then, citizens may have grown used to the idea that they no longer have any meaningful secrets.

---

129. *See, e.g.*, Tarasoff v. Regents of the Univ. of Cal., 551 P.2d 334 (Cal. 1976) (recognizing therapist's duty to warn); Hoffman v. Jones, 280 So. 2d 431 (Fla. 1973) (abrogating contributory negligence in favor of comparative negligence); Canterbury v. Spence, 464 F.2d 772 (D.C. Cir. 1972) (articulating elements of informed consent).