Privacy As Intellectual Property?

by
Pamela Samuelson*

I. Introduction

Information privacy is a scarce commodity in cyberspace.[1] The technical infrastructure of cyberspace makes it remarkably easy and cheap to collect substantial amounts of information identifiable to particular individuals.[2] Once these data have been collected, information technologies make it very easy and cheap to process the data in any number of ways (for example, to make profiles of particular users' interests).[3] Although some privacy-enhancing technologies (PETs) are being developed and deployed, these technologies have thus far done little to make cyberspace more privacy-friendly.[4] The market incentives for firms to collect and process personal data are very high. Data about users is not only useful in assessing how a firm might improve its service for its customers,[5] but it also has become a key commercial asset which firms use both for internal marketing purposes and for licensing to third parties.[6] Although the Clinton Administration has worked very hard to persuade Internet economy firms to adopt privacy policies and practices to make users more comfortable about engaging in e-commerce transactions in cyberspace,[7] these efforts have done little to overcome the

* Professor of Information Management and of Law, University of California at Berkeley. I wish to thank Robert J. Glushko, Mark A. Lemley, Marc Rotenberg, Carol Rose, Jason Schultz, Leah Theriault, and Hal Varian for their insightful comments on earlier drafts of the article and Peter Huang, Jason Schultz, and Leah Theriault for excellent research assistance for the article. Research support for this article was provided by NSF Grant No. SES 9979852.

[1] See INFORMATION INFRASTRUCTURE TASK FORCE, PRIVACY AND THE NATIONAL INFORMATION INFRASTRUCTURE: PRINCIPLES FOR PROVIDING AND USING PERSONAL INFORMATION 1-3 (1995), available at http://www.iitf.nist.gov/ipc/ipc-pubs/niiprivacyprin_final.html (defining information privacy and discussing risks to information privacy in cyberspace).

[2] See, e.g., FRED M. CATE, PRIVACY IN THE INFORMATION AGE 14-15 (1997); Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 Stan. L. Rev. 1193, 1198-99 (1998).

[3] See, e.g., Joel Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 Iowa L. Rev. 497, 516-18 (1995) (discussing uses of personal data, including profiling).

[4] See, e.g., Herbert Burkert, *Privacy Enhancing Technologies: Typology, Critique, Vision*, in TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE (Philip E. Agre & Marc Rotenberg, eds. 1997) (book cited hereinafter as "TECHNOLOGY & PRIVACY").

[5] See, e.g., Rohan Samarajiva, *Interactivity As Though Privacy Mattered*, in TECHNOLOGY & PRIVACY, *supra* note 4, at 277-79 (mass customization of new economy requires more surveillance and knowledge about customers); John Hagel III & Jeffrey F. Rayport, *The Coming Battle for Customer Information*, Harv. Bus. Rev. 53, 53 (Jan.-Feb. 1997), available at http://www.hbsp.harvard.edu/graps/hbr/index.html (discussing reasons companies want to collect personal information).

[6] See, e.g., NATIONAL TELECOM. & INFO. ADMIN., U.S. DEPT OF COMMERCE, PRIVACY AND THE NII: SAFEGUARDING TELECOMMUNICATIONS-RELATED INFORMATION 15-16 (1995) (Appendix A on business of marketing profiles). See also Opening Remarks of FTC Chairman Robert Pitofsky, Public Workshop on Online Profiling, November 8, 1999, available at http://www.ftc.gov/opa/1999/9911/onlinepitofsky.htm.

[7] See, e.g., U.S. GOVERNMENT WORKING GROUP ON ELECTRONIC COMMERCE, FIRST ANNUAL REPORT 16-18 (Nov. 1998) (discussing the Administration's efforts to promote information privacy as part of its electronic commerce initiative).

inertia of the current technical and economic environment[8] that is generally hostile to privacy interests.[9] This symposium has been convened to consider whether the law should play a greater role in promoting greater information privacy in cyberspace.

A recent book succinctly stated the principal utilitarian argument for providing greater protection to personal data in cyberspace and elsewhere:

> Consider the incentives of a company that acquires private information. The company gains the full benefit of using the information in its own marketing efforts or in the fee it receives when it sells the information to third parties. The company does not, however, suffer losses from the disclosure of private information. Because customers often will not learn of the overdisclosure, they may not be able to discipline the company effectively. In economic terms, the company internalizes the gains from using the information but can externalize some of the losses and so has a systematic incentive to overuse it.
>
> This market failure is made worse by the costs of bargaining for the desired level of privacy. It can be daunting for an individual consumer to bargain with a distant Internet merchant… about a desired level of privacy. To be successful, bargaining might take time, effort and considerable expertise in privacy issues.[10]

To overcome this market failure, some American commentators have proposed that the law should grant individuals a property right in their personal data which would enable individuals to bargain over which personal data to reveal to which firms for what purposes.[11] Other American commentators have recommended a contractual approach to protecting personal data in cyberspace (or more generally).[12] Some suggest that the law should try to facilitate, and perhaps to approximate, the "privacy agreement the two sides would reach if they were both well informed and it was not expensive to reach an agreement."[13] American commentators generally prefer market-based solutions to

---

[8] Lawrence Lessig has emphasized that law is only one of four principal regulators of human behavior in cyberspace; norms, the market, and technology also have regulatory functions. See, e.g., LAWRENCE LESSIG, CODE AND OTHER FORMS OF LAW IN CYBERSPACE at [143-47] (forthcoming 1999). I wish in this footnote to acknowledge this influence on my perspective on information privacy issues.

[9] See, e.g., Joel R. Reidenberg, *Restoring Americans' Privacy in Electronic Commerce*, 14 Berkeley Tech. L.J. 771 (1999) (arguing that self-regulation has been a failure); Kang, *supra* note 2, at 1255-67 (explaining why the market is unlikely to provide a solution to information privacy problems in cyberspace).

[10] PETER P. SWIRE AND ROBERT E. LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE 8 (1998).

[11] See sources cited *infra* note 33.

[12] See, e.g., Steven A. Bibas, Note, *A Contractual Approach to Data Privacy*, 17 Harv. J. L. & Pub. Pol'y 591 (1994); Craig Martin, Comment, *Mailing Lists, Mailboxes, and the Invasion of Privacy: Finding A Contractual Solution To a Transnational Problem*, 35 Hous. L. Rev. 801 (1998); Scott Shorr, *Personal Information Contracts: How to Protect Privacy Without Violating the First Amendment*, 80 Cornell L. Rev. 1756 (1995). But see, e.g., Reidenberg, *supra* note 3, at 546-47 (discussing limits of contractual approaches to data protection).

[13] Swire & Litan, *supra* note 10, at 7.

personal data protection over the strict comprehensive regulatory regime adopted some years ago in Europe.[14]

While utilitarian considerations weigh heavily in the minds of many Americans who have written on information privacy issues, noneconomic considerations provide an equally or more compelling rationale for legal protection for personal data in cyberspace, according to other commentators. For those who conceive of personal data protection as a fundamental civil liberty interest, essential to individual autonomy, dignity, and freedom in a democratic civil society, information privacy legislation is often viewed as necessary to ensure protection of this interest.[15] Others regard cognitive limitations on the ability of individuals to comprehend and accurately assess the risks they run when revealing personal data to others as a reason for the law to provide corrective measures.[16] Still others argue for information privacy protection to guard against identity theft, harassment, and other wrongful uses of personal information.[17] Achieving consensus on the rationale for information privacy protection is, however, unnecessary given that both economic and noneconomic considerations favor greater protection for personal data in cyberspace.

Section II considers both the appeal and limitations of the property rights model for protecting personal data. A property rights model offers two principal benefits: First, it would establish a right in individuals to sell their personal data and thereby capture some of the value their data have in the marketplace. Second, a property rights model would force companies to internalize certain social costs now borne by others from the widespread collection and use of personal data. By internalizing these costs, firms may make better investment decisions about what data to collect and what uses to make of the data. However, a property rights model for protecting personal data nevertheless presents many problems. This approach to personal data protection would, in essence, establish a new form of intellectual property right in information. But it would be an intellectual property right of a very different sort than existing regimes provide. Deep differences in the purposes and mechanisms of traditional intellectual property rights regimes and the proposed property rights regime in personal data raise serious doubts about the viability

---

[14] See Directive 95/46/EC of the European Parliament and the Council, October 25, 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal of the European Community, L281 (November 23, 1995) (cited hereinafter as "EU Directive"). See, e.g., Swire & Litan, *supra* note 10, Chap. 2 for a discussion of the main features of the EU Directive. Although these authors agree with the EU Directive's underlying premise about the need for greater protection for personal data, they are among the Directive's strongest critics. See, e.g., *id.* at 8-21 (explaining why the EU Directive is unworkable and overbroad).

[15] See, e.g., Simon Davies, *Re-engineering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity*, in TECHNOLOGY & PRIVACY, *supra* note 5; Reidenberg, *supra* note 3, at 497-98; Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 Vand. L. Rev. (forthcoming 1999). See also Julie E. Cohen, *A Right To Read Anonymously: A Closer Look at Copyright Management in Cyberspace*, 28 Conn. L. Rev. 981 (1996). The EU Directive is based on a conception of personal data protection as a fundamental civil liberty interest. See EU Directive, *supra* note 14, Art. 1.1.

[16] See, e.g., Joseph Lasica, *Your Past is Your Future*, Wash. Post, Outlook, Oct. 11, 1998; William Safire, Nosy Parker Lives, N.Y. Times, Sept. 23, 1999, at A29.

[17] See, e.g., Kang, *supra* note 2, at 1212-17.

of a property rights approach and about its prospects of achieving information privacy goals.

Section III explores an alternative market-oriented legal regime for protecting personal information. Such a regime need not ground itself in property law. The law can establish a default rule providing individuals with certain rights to control the collection or processing of personal information about them while also providing individuals with the power to contract away this right (e.g., when they receive compensation for doing so). Because market imperfections may impede fair and effective licensing of personal data in cyberspace, the law can supply some default terms for the licensing of personal data. Certain trade secrecy licensing default rules may be adaptable to the licensing of personal data. Additional default rules for the licensing of personal data in cyberspace may be supplied by the Uniform Computer Information Transactions Act (UCITA).[17A] A market-based licensing approach to personal data protection could be facilitated through adoption of online privacy policies. When websites post notices saying personal data will not be collected, disclosed, or used except for named purposes, users who supply data in reliance on those restrictions may be able to enforce the restrictions. A market-based licensing approach may also arise if technology evolves to allow "negotiated" agreements on the collection, use, or disclosures of personal data.

Although this article endorses a licensing approach to the protection of personal data, it recognizes that the law alone cannot solve information privacy problems in cyberspace. Work must continue on evolving norms about appropriate and inappropriate uses of personal data, on persuading firms that the trust necessary for electronic commerce to flourish requires the interests of individuals in information privacy to be given appropriate deference, and on adapting the technological infrastructure of cyberspace so that information privacy becomes easier to achieve. The principal challenge of these multi-faceted endeavors is not to recreate in cyberspace some preexisting zone of privacy from the physical world,[18] but to articulate values inhering in information privacy that should constrain and structure social, economic, technological, and legal relations.[19]

II. The Appeal and Limitations of a Property Rights Approach To Protecting Personal Information

A. The Appeal of a Property Rights Approach

[17A] See UNIFORM COMPUTER INFORMATION TRANSACTIONS ACT (October 15, 1999 final draft recommended for enactment by state legislatures) available at <http://www.law.upenn.edu/bll/ulc/ucita/cita10st.htm> (cited hereinafter as "UCITA"). See *infra* notes 194 and accompanying text for a discussion of the implications of this law).

[18] See, e.g., Frederick Schauer, *Internet Privacy and the Public-Private Distinction*, 38 Jurimetrics J. 555, 560-61 (1998) (critical of this perspective)

[19] See, e.g., Lessig, *supra* note 8, at [4].

It may seem natural for individuals to assume that they do or should own data about themselves.[20] It is surely true that the law will enforce the expectations of individuals that certain private information (e.g., a diary or journal) should remain secret.[21] Because individuals generally have a legal right to exclude other people from access to their private data, they may have a sense that they have a property right in the data as well as a legal right to restrict access to it. Even when data about individuals are in the hands of others (such as banks, doctors, and insurance companies), individuals may perceive themselves to have a protectable interest in records of their financial transactions or medical histories.[22] Because the law will sometimes protect these and other types of data from unauthorized uses and disclosures,[23] this too may reinforce a sense of ownership in personal data.

Although the law often protects the interests of individuals against wrongful uses or disclosures of personal data,[24] the rationale for these legal protections has not historically been grounded on a perception that people have property rights in personal data as such.[25] Indeed, the traditional view in American law has been that information as such cannot be owned by any person.[26] The Fourth Amendment and real property law may provide protection against certain unauthorized intrusions into one's real or personal property for purposes of getting access to information that might be stashed there, and the

---

[20] "Why not," asks Kenneth Laudon, "let individuals own the information about themselves and decide how the information should be used?" Kenneth C. Laudon, *Markets and Privacy*, 39 Comm. ACM 92, 92 (Sept. 1996). See also Catherine M. Valerio Barrad, Comment, *Genetic Information and Property Theory*, 87 Nw. U. L. Rev. 1037, 1062-63 (1993) (discussing natural rights theory for recognizing property protection in genetic information)

[21] See, e.g., Samuel W. Warren and Louis D. Brandeis, *The Right of Privacy*, 4 Harv. L. Rev. 193, 198-99 (1890)

[22] See, e.g., U.S. v. Miller, 425 U.S. 435, 441-445 (1976) (considering arguments about the expectations of individuals as to bank records).

[23] See, e.g., Right to Financial Privacy Act, 29 U.S.C. sec. 3410 et seq.; Horne v. Patton, 291 Ala. 701, 287 So.2d 824 (1973) (doctor's disclosure of medical information to prospective employer was wrongful). But see, e.g., Paul M. Schwartz, *Privacy and the Economics of Personal Health Care Information*, 76 Texas L. Rev. 1, 3 (1997) (indicating that little legal protection is available for medical information).

[24] See, e.g., Fair Credit Reporting Act, U.S.C. sec. 601 et seq. See generally PAUL M. SCHWARTZ AND JOEL R. REIDENBERG, DATA PRIVACY LAW: A STUDY OF UNITED STATES DATA PROTECTION (1996) (providing an overview of state and federal information privacy laws).

[25] See, e.g., *id.*, Chap. 5 (explaining rationales of certain U.S. information privacy laws).

[26] See, e.g., Feist Pub., Inc. v. Rural Telephone Service Co., 499 U.S. 340 (1991) (copyright law does not confer exclusive rights in information in order to achieve constitutional purpose of promoting knowledge). Information can, however, sometimes be protected against unfair competition, including breaches of confidential relationships. See International News Service v. Associated Press, 248 U.S. 215 (1918). See also Yochai Benkler, *Constitutional Bounds of Database Protection: The Role of Judicial Review in the Creation and Definition of Private Rights in Information*, 15 Berkeley Tech. L.J. (forthcoming 2000); Yochai Benkler, *Free As The Air To Common Use: First Amendment Constraints On Enclosure Of The Public Domain*, 74 N.Y.U. L. Rev. 354 (1999); Jessica Litman, *The Public Domain*, 39 Emory L.J. 965 (1990); Malla Pollack, *The Right To Know?: Delimiting Database Protection At The Juncture Of The Commerce Clause, The Intellectual Property Clause And The First Amendment*, 17 Cardozo Arts & Ent L.J. 47 (1999); L. Ray Patterson & Stanley F. Birch, Jr., *Copyright and Free Speech Rights*, 4 J. Intell. Prop. L. 1 (1996); Pamela Samuelson, *Information As Property: Do* Ruckelshaus *and* Carpenter *Signal a Changing Direction in the Law?*, 38 Cath. U. L. Rev. 365 (1989); Diane Leenheer Zimmerman, *Information as Speech, Information as Goods: Some Thoughts On Marketplaces and the Bill of Rights*, 33 Wm & Mary L. Rev. 665 (1992).

Fifth Amendment may provide protection against compulsion to reveal certain information about oneself. But these results are not grounded on a belief that people have property rights in information about themselves, but on the recognition of legally protectable interests of other sorts.[27] An individual, for example, may be able to obtain relief if a doctor releases details of her medical history to a prospective employer, but the individual's rights would arise under contract or privacy law, not from the existence of any property rights in this information.[28]

Many examples illustrate that the law does not generally recognize the legal right of an individual to control uses or disclosures of personal data.[29] Individuals, for example, have no legal right to stop firms from marketing their personal data to other firms based on information that the individuals disclosed on a product warranty card sent to manufacturers of that product.[30] Nor can they stop state governments from selling drivers' license data about themselves; indeed, the Supreme Court is about to decide whether even Congress has the power to stop this practice.[31] Thus, however intutitively powerful the notion of property rights in one's data may be, it is clear that in the U.S. the existence of some legally protectable interests in personal data in certain circumstances is not equivalent to a legal rule that a person has a property interest in her personal data.[32]

In recent years, a number of economists and legal commentators have argued that the law ought now to grant individuals property rights in their personal data.[33] Some favor propertizing personal data as a way to allow individuals to make appropriate deals for selling their personal data and to receive compensation for uses of their personal data so that markets in personal information will work more fairly.[34] Others favor propertizing personal data as a way of forcing companies to internalize more fully the

---

[27] See, e.g., Lessig, *supra* note 8, Chap. 8 (explaining Bill of Rights as a check on government power).
[28] See, e.g., Horne v. Patton, 291 Ala. 701, 287 So.2d 824 (1973).
[29] See, e.g., Moore v. Regents of the University of California, 51 Cal. 3d 120, 271 Cal. Rptr. 146, 793 P.2d 479 (1990), cert. denied, 499 U.S. 936 (1991) (rejecting individual's claim of property right in his genetic information); Polin v. Dun & Bradstreet, 768 F.2d 1204 (10th Cir. 1985) (rejecting privacy claim based on unauthorized release of credit report information).
[30] The European Directive, however, would generally prohibit use of personal data collected to enable the customer to qualify for warranty protection for marketing purposes. See EU Directive, *supra* note 14, Art. 6.1.
[31] See, e.g., Condon v. Reno, 155 F.3d 453 (4th Cir. 1998), cert. granted, 67 U.S.L.W. 3588 (1999).
[32] See, e.g., Randolph S. Sergent, *Note, A Fourth Amendment Model for Computer Networks and Computer Privacy*, 81 Va. L. Rev. 1181, 1200 (1995) ("one might conclude that an individual has no expectation of privacy in information kept by a third party").
[33] See, e.g., *Developments in the Law—The Law of Cyberspace*, 112 Harv. L. Rev. 1574 (1999) (cited hereinafter as "Harvard Developments"); Laudon, *supra* note 20; Lawrence Lessig, *The Architecture of Privacy*, 1 Vand. J. Ent. L. & Prac. 56 (1999); Lessig, *supra* note 8; Patricia Mell, *Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness*, 11 Berkeley Tech. L.J. 1 (1992); Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 Georgetown L.J. 2381 (1996); Carl Shapiro and Hal Varian, *US Government Information Policy*, May 28, 1997, posted at http://www.sims.berkeley.edu/~hal/Papers/policy.pdf.
[34] See, e.g., Laudon, *supra* note 20, at 92-100; Shapiro & Varian, *supra* note 33, at 29-30. Shapiro and Varian express concern that privacy protection legislation may not promote consumer welfare because it will be too strong and inflexible. *Id.* at 29.

costs associated with the collection and processing of personal data, in the hope that this will lead to greater privacy.[35]

There is at the moment a "lively market" in personal data, but it is a market in which individuals play at most a very small role.[36] Many firms collect and process personal data because it's valuable and because information technology makes it so much easier and cheaper to gather and use.[37] They also do so because they don't have to internalize the societal costs of private sector processing of personal data.[38] Because they may have invested time, money and energy in compiling, organizing, or processing the data, they may well think of themselves as owning the data they have gathered or otherwise acquired.[39] Perhaps firms would collect or process less personal data than they currently do if they had to pay individuals for rights to do so.[40] If so, this would simultaneously achieve information privacy goals and allow individuals who wish to sell their data to receive some benefits from this market. In addition, a property rights regime might enable firms to make fewer wasteful investments in personal data and to develop higher quality databases, since individuals would presumably agree to release personal data to firms from whom they would be willing to receive information, and would have less incentive to lie as a way to protect their privacy.[41]

---

[35] Email communication from Marc Rotenberg to Pamela Samuelson, Oct. 31, 1999 (cited hereinafter as "Rotenberg email").

[36] See Laudon, *supra* note 20, at 92.

[37] See, e.g., Kang, *supra* note 2, at 1199, 1220-30(discussing the technical infrastructure of cyberspace and how it enables collection of personal data).

[38] See, e.g., Laudon, *supra* note 20, at 98.

[39] See, e..g., Cate, *supra* note 2, at 74. The belief of data compilers in their ownership rights in personal data compilations will be strengthened if the U.S. Congress passes legislation to protect collections of data from "piracy," as has been proposed numerous times in recent years. See H.R. 354, 106th Cong., 1st Sess. (1999). Notwithstanding their investment-based claim of rights in data compilations, personal data compilers almost certainly recognize significant limitations on their ability to use these data. A firm claiming to "own" a list of ten thousand impotent men would surely recognize that publication of the names of those men in a widely circulated newsletter would be an invasion of privacy rights that these men would have in respect of this information. A firm possessing such a list may feel justified in licensing this information to the manufacturer of Viagra based on its belief that many men suffering from this condition would be interested in or might otherwise benefit from receiving information on this drug. Societal norms, then, already limit to some degree what firms do with personal data. See, e.g., Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 Calif. L. Rev. 957 (1989) (discussing normative concept of privacy). When norms alone do not suffice, the law sometimes imposes community norms on firms possessing personal data. Without resolving the question of whether traffickers in personal data have "property rights" in these data, it is easy to demonstrate that their rights (if any) in collections of personal data do not extend as far as the "property rights" label might suggest. This example illustrates that individuals have some residual legally protectable interests in personal data in the hands of data compilers.

[40] Rotenberg email, *supra* note 35.

[41] Laudon explains that "[t]he current situation costs corporations billions of dollars in waste as they pore money into privacy-invading marketing and authorization techniques." Laudon, *supra* note 20, at 104. See also Scott Killingsworth, *Minding Your Own Business: Privacy Policies in Principle and In Practice*, 3 J. Internet L. 1, 3-4 (Oct. 1999) (discussing data quality issues); and Mell, *supra* note 33, at 79-81 (suggesting the creation, by statute, of an agency relationship between an individual and an information holder, such that any subsequent use or disclosure of the information becomes subject to a warranty of authority to disclose and a warranty of accuracy). One consequence of the property rights regime which most commentators have not explored is the likelihood that individuals supplying false personal information

Governments clearly have power to create property rights when appropriate to cure or ameliorate market failure problems.[42] Creating property rights in informational assets is, in fact, remarkably common. Intellectual property law grants exclusive rights in information-based creations in order to promote develop of a thriving marketplace for them.[43] A number of commentators have observed that in an information economy, it seems almost inevitable that information will increasingly be commodified and new property rights will be created.[44] Granting individuals property rights in their data would seem to be consistent with this general trend and with the emergence of an "attention economy."[45]

A property rights approach to solving the information privacy problem may also be consistent with survey evidence suggesting that most Americans are willing to disclose personal data to businesses and allow them to use these data as long as the individuals obtain a discernible benefit from this disclosure and use (e.g., a discounted price for certain goods or services).[46] If what upsets Americans most about the loss of control over their personal data is that they are not receiving any benefits arising from private sector reuses of the data, a property rights approach would arguably provide individuals with a way to exercise meaningful control over the market in personal data which they do not currently enjoy. This would arguably cure a market failure, as well as overcome the unjust enrichment that compilers of personal information now enjoy.

A property rights approach may be especially useful to accommodate the varying preferences of individuals about private sector uses of personal data.[47] Although some individuals may value privacy so highly that they will choose not to engage in market transactions about their personal data, others may be quite willing to sell their personal data to firms A, B, and C (even if not to X, Y, or Z). Or they may be willing to sell personal data about their recreational interests, but about not the associations to which they belong. The market arguably provides an efficient device—namely the price

---

under the property model might themselves be subject to liability for the inaccuracy of their information: see, e.g., Mell, *supra* note 33 at 80. While such liability would help insure the accuracy of the information that individuals provide about themselves, it seems fair to say that most Internet users do not currently contemplate personal liability when they provide information online.

[42] See, e.g., Margaret Jane Radin, *Property Evolving in Cyberspace*, 15 J. L. & Comm. 509, 514-518 (1996) (discussing utilitarian criteria for creation of property rights).

[43] See, e.g., NATIONAL RESEARCH COUNCIL, THE DIGITAL DILEMMA (1999), at ES-1, portions of the text are available at <http://www.nap.edu/books/0309064996/html/>.

[44] See, e.g., Rochelle C. Dreyfuss, *Information Products: A Challenge to Intellectual Property Theory*, 20 N.Y.U. J. In't L. & Pol. 897 (1989); J.H. Reichman, *Legal Hybrids Between the Patent and Copyright Paradigms*, 94 Colum. L. Rev. 2432 (1994); Samuelson, *supra* note 26.

[45] See, e.g., Michael H. Goldhaber, *Attention Shoppers!*, WIRED, Dec. 1997, at 182-90; Radin, *supra* note 42, at 517.

[46] See, e.g., Newsday, *Web Privacy? Let's Make a Deal*, Palm Beach Post, Aug. 26, 1999, at 4E (survey by Opinion Research Corporation found that 86 per cent of web users would release personal information as long as they received a direct benefit, such as money or free products or services, for it). But see *Graphics, Visualization, & Usability (GVU) Center's 10th Annual Survey of Users* (1998), available at http://www.gvu.gatech.edu/user_surveys/survey-1998-10/ (reporting that between one-quarter and one-third of surveyed users would be willing to reveal demographic data to get some benefit).

[47] See, e.g., Shapiro & Varian, *supra* note 33, at 30-31.

mechanism—with which individuals can express their preferences about who should be able to use which of personal data and to what degree.[48] Private sector buyers would, of course, dicker on price and other terms, but economists generally assume that the market is a good way to achieve an efficient outcome that is satisfactory to both buyer and seller.[49] If the market works well in enabling transactions in other commodities, it would presumably work for transactions in personal data as well.

A property-rights approach to the information privacy problem would involve substantial transaction costs for individuals if they have to separately negotiate with each prospective buyer of their personal data.[50] To overcome such problems, some commentators have predicted the emergence of new businesses to serve as intermediaries on behalf of individuals to represent their interests and negotiate with buyers of these data ("infomediaries").[51] Others anticipate the development of electronic agents to perform negotiations and make deals to sell personal data in cyberspace.[52] Still others expect individuals to be able eventually to program their browser software to incorporate their privacy preferences.[53] Well-programmed browsers might then avoid websites that do not conform to their masters' preferences and only make automated deals with websites whose privacy terms are within an acceptable range.

A property-rights approach offers a further potential advantage over other legal approaches to protecting privacy in that it could protect personal data without requiring the establishment of a substantial government bureaucracy, as some nations have done to oversee regulation of personal data protection.[54] Americans generally disfavor the substantial costs associated with direct government oversight of industry practices. They also tend to bristle if the government requires firms to establish internal oversight procedures and structures, as the European Directive requires.[55] To the extent that a property rights approach would avoid such costs, this would seem to be another factor in its favor.

---

[48] See, e.g., id.
[49] See, e.g, *id.*; Laudon, *supra* note 20, at 102.
[50] See, e.g., *id.* at 101.
[51] See, e.g., Hagel & Rayport, *supra* note 5, at 54.
[52] See, e.g., Lorrie Cranor, *Internet Privacy*, 42 Comm. ACM 29, 30 (Feb. 1999).
[53] See, e.g., Harvard Developments, *supra* note 33 at 1646; Joseph Reagle & Lorrie Faith Cranor, *The Platform for Privacy Preferences*, http://www.w3c.org/TR/1998/NOTE-P3P-CACM.
[54] The European Directive requires all member states to establish "supervisory authorities" to ensure that the data protection regulations are enforced. See EU Directive, *supra* note 14, Art. 28. Many European countries already had established data protection authorities. See, e.g., COLIN J. BENNETT, REGULATING PRIVACY: DATA PROTECTION AND PUBLIC POLICY IN EUROPE AND THE UNITED STATES (1992). Americans tend to have reservations about the establishment of a privacy bureaucracy as such, although suggesting that privacy policy coordination be placed elsewhere in the government (e.g., in the electronic commerce group at the Commerce Department). See, e.g., Swire & Litan, *supra* note 10, at 17-18. See also Kang, *supra* note 2, at 1285 (indicating that privacy bureaucracy unlikely in U.S.); NATIONAL INFORMATION INFRASTRUCTURE, OPTIONS FOR PROMOTING PRIVACY ON THE INFORMATION SUPERHIGHWAY24-28 (April 1997) (discussing possible ways for the U.S. government to respond to challenges of information privacy, but expressing reservations on establishment of bureaucracy). There is clearly a need for the U.S. to have expert negotiators to participate in international discussions on information privacy issues. Swire & Litan, *supra* note 10, at 17-18.
[55] EU Directive, *supra* note 2, Arts. 17-18.

B. Limitations of a Property Rights Approach

Despite these appealing features, there are some reasons to doubt that a property rights approach to protecting personal data would actually achieve the desired effect of achieving more information privacy. A property rights approach may have some unintended consequences that proponents of this approach have not recognized.

To understand some possible disadvantages of the property rights approach, it is necessary to think beyond the initial creation of a property right in an individual's personal data. Proponents implicitly assume that the creation of the property right is the only significant act necessary to enable the growth of a functioning market in which individuals could engage in personal data transactions.[56] Kenneth Laudon is one of the few commentators to consider what infrastructure might be required to make a property rights system work.[57]

Laudon proposes the establishment of a regulated National Information Market (NIM) to allow "personal information to be bought and sold, conferring on the seller the right to determine how much information is divulged."[58] Individuals would first "establish information accounts and deposit their information assets and informational rights in a local information bank, which could be any local financial institution interested in moving into the information business."[59] The banks would then pool these information assets and sell "baskets" of them in a National Information Exchange.[60] Buyers would receive the right to make commercial uses of personal information in those baskets for stated periods of time, in exchange for compensation paid to the seller-banks. The banks would then equitably allocate this compensation among the individuals whose information was pooled in a particular basket (less a service fee).[61] Laudon foresees assigning every participant in the NIM a unique identifier and barcode symbol (to be known as a National Information Account number) which "would help individuals keep track of who is using their information by informing the account whenever the individual's name is sold as part of a basket of information."[62] Laudon proposes to make

---

[56] See, e.g., Harvard Developments, *supra* note 33; Lessig, *supra* note 33; Murphy, *supra* note 11. Other commentators expect a "long and drawn out period of confusion" before this market becomes stable, but expect standard contracts to solve the problem. See, e.g., Shapiro & Varian, *supra* note 33, at 31.

[57] See Laudon, *supra* note 20. See also Kenneth C. Laudon, *Extensions to the Theory of Markets and Privacy: Mechanics of Pricing Information*, in PRIVACY AND SELF-REGULATION IN THE INFORMATION AGE (1997).

[58] Laudon, *supra* note 20, at 92.

[59] *Id.*

[60] *Id.* at 100

[61] *Id.* Private placements of personal data might also occur through a National Information Accounts Clearinghouse which would be established by Congress to permit individuals to collect fees for uses of their information. *Id.*

[62] *Id.*

it a crime to use personal information without permission.[63] He also foresees a substantial role for government oversight of this market.[64]

One needn't agree with all of the particulars of Laudon's vision in order to agree with his basic insight that an institutional infrastructure would be needed to make a new property rights market in personal information work. Even if one "grandfathered" in private sector "rights" to continue using personal data collected before the effective date of the legislation establishing a property right in personal data, the new property system would introduce significant "friction" to a market that currently operates without it. This friction may be justifiable as a way to force data compilers to internalize certain costs they currently impose on others,[65] but it is fair to say that the costs of establishing new procedures and implementing them would be far from trivial for both companies and for individuals.[66] Collectors of personal data would presumably have to pay individuals for rights to process the data; this cost would unquestionably have to be passed on to others in the form of higher prices for the firms' own products or services, and establishing an enforcement system would also be costly. Property rights systems are not costless.[67] Too little thought has been given as yet about how to move from where we are today to a thriving market in personal data under a property rights regime in which individuals would have a right to control market transactions in data about themselves.

Achieving information privacy goals through a property rights system may be difficult for other reasons than market complexities. Chief among them is what to do about the alienability of personal information.[68] It is a common, even if not ubiquitous, characteristic of property rights systems that when the owner of a property right sells her interest to another person, that buyer freely can transfer to third parties whatever interest the buyer acquired from her initial seller.[69] Free alienability works very well in the market for automobiles and land, but it is far from clear that it will work well for information privacy. An individual may be willing to sell his data to company N for purpose S, but he may not wish to give N rights to sell these data to M or P, or even to let N use the data for purposes T or U. The individual may be able to make a reasonable

---

[63] *Id.* at 101.

[64] *Id.* at 103. Laudon recommends establishing a Federal Information Commission to oversee the NIM and related activities. *Id.*

[65] *Id.* at 98.

[66] *Id.*

[67] See, e.g., Radin, *supra* note 42, at 516-17 (indicating that the costs of enforcement must be included in the calculus of the costs and benefits of establishing property rights).

[68] Some commentators have recognized the need for limitations on resale rights. See, e.g., Hal R. Varian, *Economic Aspects of Personal Privacy*, http://www.sims.berkeley.edu/~hal/Papers/privacy/privacy.html at 5 (December 6, 1996) ("information about an individual could not be *resold*, or provided to third parties, without that person's explicit agreement").

[69] See, e.g., JOHN P. DWYER AND PETER S. MENELL, PROPERTY LAW AND POLICY: A COMPARATIVE INSTITUTIONAL PERSPECTIVE at 184-185 (1998) (discussing general hostility to restrictions on alienation in property law); MARGARET JANE RADIN, CONTESTED COMMODITIES 18 (1996) (concept of inalienability "negates a central element of property law"). See also RESTATEMENT OF PROPERTY § 406, comment a (1944), (referencing rationale for disfavoring restraints on alienation); and ROGER A. CUNNINGHAM, WILLIAM B. STOEBUCK and DALE A. WHITMAN, THE LAW OF PROPERTY § 2.2, at 35 (1984) (tracing public policy in favor of free alienability of lack back to Quia Emptores in 1290).

estimate of the value they should receive from N for a grant for S purpose, but may at the time of transacting with N be unable to assess what value he should receive for any transfer of the same data to M, P, or any other licensee of N. Collectors of data may prefer a default rule allowing them to freely transfer personal data to whomever they wish on whatever terms they can negotiate with their future buyers. However, individuals concerned with information privacy will generally want a default rule prohibiting retransfer of the data unless separate permission is negotiated. They will also want any future recipient to bind itself to the same constraints that the initial purchaser of the data may have agreed to as a condition of sale. Information privacy goals may not be achievable unless the default rule of the new property rights regime limits transferability.

Consider also that the most common justification for granting property rights—to enable market allocations of scarce resources—does not seem to apply to personal data.[70] What's scarce is information privacy, not personal data. If anything, personal data are being too plentifully distributed in the marketplace right now. Indeed, a reason many people argue in favor of granting individuals property rights in these data is, in essence, to make the distribution of them scarcer. While there are other instances in which property rights have been created in order to make a too plentiful a resource more scarce—for example, the creation of property rights to allow emissions of pollutants up to certain levels as a way to achieve environmental goals[71]—such a property rights system works because of the free transferability of the property rights. The right to pollute to a certain level is, by virtue of the property right grant, made into a scarce resource that the market can then allocate efficiently.[72] The alienability of this property right is an essential part of what enables the property regime to accomplish its objective of controlling pollution levels. Yet, as noted above, the free alienability of property rights in personal data may prove to be troublesome.

---

[70] See, e.g., Radin, *supra* note 42, at 514-16 (discussing scarcity rationale for establishing property rights).

[71] See, e.g., 1990 Amendments to the Clean Air Act, 42 U.S.C. secs. 7401, 7651-7651o; Carol M. Rose, *The Several Futures of Property: Of Cyberspace and Folk Tales, Emission Trades and Ecosystems*, 83 Minn. L. Rev. 129, 164-80 (1998) (discussing regulatory property rights regimes).

[72] See, e.g., Rose, *supra* note 71, at 164-65. A further goal of this sort of property rights regime is to ensure that firms will have incentives to redirect its investments toward non-polluting or pollution-reducing equipment or otherwise to reduce production of the undesired substance. *Id.* at 166. Rose also emphasizes the critical importance of having the technological means to set, monitor, and enforce emissions rights regimes. *Id.* at 167. Of course, there are other differences between the right to pollute and the information privacy rights contemplated here. Chief among them is that one is a supplier's right and the other a buyer's right. In the environmental context, the purpose of the property right is to limit the amount of pollution any one *supplier* can distribute. In the personal data market, however, it appears that we aren't concerned with capping what *suppliers* want to do with their information or with creating a property right to inhibit such supplying. Instead, we want to cap what *buyers* do with the information they purchase. By giving a property right to the suppliers, we make it harder for the buyers to gather all the information they want. The Clean Air Act, on the other hand, creates a market among producers of pollution to trade among themselves, not a market between producers of pollution and buyers of pollution. To achieve the goals of information privacy using a Clear Air Act system for buyers, we would have to put a cap on the amount of information any one company could own and then give companies limited rights in the ability to own information, allowing them to trade those rights with other information collectors in order to create a market in information collection that reflected the value of amassing information.

Consider also differences between the rationale for the proposed property rights in personal information and the rationale for existing property rights regimes that regulate markets for information-based products, namely, intellectual property law.[73] The economic rationale for intellectual property law arises from a public goods problem with information products that this law strives to overcome.[74] In the absence of intellectual property rights, there may be too little incentive to induce an optimal level of private investments in the production and dissemination of intellectual products. Everyone benefits if such investments are made, regardless of whether they are in technological, artistic or literary fields.[75] However, without a legal protection system, creators will find it difficult to exclude free-riders from appropriating the fruits of their labor and selling identical or very similar products in the marketplace at a cheaper price.[76] The prospect of being unable to recoup research and development costs may deter such investments from being made in the first place.[77] A limited grant of property rights in intellectual productions gives creators assurance that they can control the commercialization of their work and enjoy some fruits of their labor, assuming the market finds the product attractive.[78]

The standard rationale for granting property rights in personal data is, of course, quite different.[79] The personal data most likely to become the subject matter of such a property right, for the most part, already exist. Property rights are not needed to bring them into being, nor to achieve widespread distribution of them. There are, in addition, no research and development costs to recoup. It is, of course, possible that people might invest more time, money and energy in the creation of additional personal data about themselves (e.g., hobbies the person would like to have or famous people the person would want to meet) if they could assert property rights in this new data, but there is some reason to think that people may be willing to do this even without a grant of property rights in the data.[80]

A further cause for concern about a property rights approach to protecting personal data is the potential that such grant of intangible rights in intangible information will lead

---

[73] See, e.g., Rochelle C. Dreyfuss, *Warren & Brandeis Redux: Finding (More) Privacy Protection* at 5 and 8, Virtual Symposium on Privacy and Computer-Mediated Surveillance, available at http://stlr.stanford.edu/STLR/Symposia/Privacy/index.htm (contrasting incentives rationale for intellectual property protection with rationale for privacy protection; concluding that "the fit between what intellectual property provides and what privacy advocates want is imperfect, more apparent than real and possibly evanescent").

[74] See, e.g., ROBERT P. MERGES, PETER S. MENELL, MARK A. LEMLEY, & THOMAS M. JORDE, INTELLECTUAL PROPERTY IN THE NEW TECHNOLOGICAL AGE 12-18 (1997).

[75] *Id.*

[76] *Id.*

[77] *Id.* The ability to recoup research and development expenses has become increasingly difficult because so many of today's most commercially valuable information products bear the knowhow required to make them on or near the surface of the product. See generally J.H. Reichman, *Computer Programs As Applied Scientific Know-How: Implications of Copyright Protection for Commercialized University Research*, 42 Vand. L. Rev. 639 (1989).

[78] As with the other property rights considered thus far, alienability of rights is a common feature of intellectual property rights systems. See, e.g., 17 U.S.C. sec. 201(d) (transfer of ownership rules).

[79] See *supra* notes 5-10 and accompanying text.

[80] See, e.g., Dreyfuss, *supra* note 73, at 1 (bemoaning the willingness of people to give away information about themselves).

to greater incoherency in intellectual property law. A fundamental principle for Congressional grants of intellectual property rights is that such legislation should "promote progress of science and [the] useful arts."[81] It is difficult enough these days for Congress to adhere to this principle: expanding intellectual property law to protect personal data would only strain the coherence of this body of law further.[82] This constitutional principle does apply to personal data. The creation and dissemination of personal data does not generally promote "science" in the constitutional sense (i.e., knowledge),[83] nor does it promote technological innovation.[84] Indeed, the purpose of the proposed new personal data property right is almost the inverse of traditional intellectual property law, for it would grant a property right in order to restrict the flow of personal data to achieve privacy goals.[85]

It is also far from clear what constitutional authority Congress would have to enact legislation creating a property right in personal data. Given the mismatch between the purposes of personal data protection and of traditional intellectual property rules, it would be difficult to justify such legislation under the enabling clause for copyright and patent legislation.[86] Because of the interstate character of the Internet and web, it might be possible to justify Congressional legislation granting property rights to personal data in cyberspace under the Commerce Clause.[87] However, a more general grant of property rights in personal data might be constitutionally troublesome.[88] Grants of property rights

---

[81] U.S. Constitution, Art. I, sec. 8, cl. 8. Some, of course, have considered alternative rationales for grants of intellectual property rights. See, e.g., Wendy J. Gordon, *On Owning Information: Intellectual Property and the Restitutionary Impulse*, 78 Va. L. Rev. 149 (1992) (discussing restitution-based rationales for intellectual property law). This, of course, is closer to the mark for information privacy concerns.

[82] See, e.g., Peter A Jaszi, *Goodbye To All That: A Reluctant (And Perhaps Premature) Adieu To A Constitutionally-Grounded Discourse Of Public Interest in Copyright Law*, 29 Vand. J. Trans'l L. 595 (1996) (explaining pressures emanating from major copyright industry organizations on Congress to deviate from constitutional and utilitarian purposes).

[83] See, e.g., REPORT OF THE REGISTER OF COPYRIGHTS ON THE GENERAL REVISION OF THE U.S. COPYRIGHT LAWS 3-6 (1961) (discussing constitutional purposes of copyright law). See also L. Ray Patterson, *Free Speech, Copyright, and Fair Use*, 40 Vand. L. Rev. 1 (1987).

[84] The U.S. Constitution speaks of promoting "science" and the "useful arts" as the purposes for which Congress is empowered to enact intellectual property legislation. U.S. Const., Art. I, sec. 8, cl. 8. See Merges et al., *supra* note 74, at 12-15 (discussing constitutional purposes).

[85] See, e.g., Rosemont Enters. v. Random House, Inc., 366 F. 2d 303 (2d Cir. 1966) (attempt by copyright owner to exercise copyright in order to keep suppress biography of Howard Hughes weighed against infringement). Of course, if an author has chosen not to publish her work (or not to publish it yet), copyright law will protect the work from unauthorized publication. See, e.g., Harper & Row Pubs. v. Nation Enters., 471 U.S. 539 (1985) (preemptive publication of excerpts from unpublished book was not fair use).

[86] U.S. Const., Art. I, sec. 8, cl. 8. The Supreme Court repeatedly emphasized constitutional limitations on the power of Congress to enact legislation in explaining why copyright protection could not be extended to unoriginal data compilations in Feist Pub., Inc. v. Rural Telephone Service Co., 499 U.S. 340 (1991).

[87] See, e.g., Kang, *supra* note 2, at 1267.

[88] Of course, it might be possible to assert that Congress has constitutional power to enact such legislation under Section 5 of the Fourteenth Amendment. The Solicitor General relied on this constitutional provision in arguing that Congress had power to enact the Drivers Privacy Protection Act, 18 U.S.C. sec. 2721 et seq. The Fourth Circuit Court of Appeals rejected this argument in Condon v. Reno, 155 F.3d 453 (4th Cir. 1998) on the ground that "neither the Supreme Court nor this Court has ever found a constitutional right of privacy with respect to the sort of information to which individuals do not have a reasonable expectation of privacy." *Id.* at 464. This decision is under review by the U.S. Supreme Court. If the Court

are generally the province of state law.[89] Indeed, the state law doctrine out of which a property right regime in personal data would seem the most natural extension is right of publicity law which gives individuals some rights to control commercial exploitation of their names, likenesses, and other indicia of the commercial value of their person.[90] Although the right of publicity has often been characterized as a property interest,[91] it is an interest that law has allowed celebrities, not ordinary folk.[92]

Creating a property right in personal data may, moreover, be objectionable to those who consider information privacy to be a fundamental civil right.[93] While the civil right conception of personal data protection is predominant in Europe,[94] sometimes this conception is evident in U.S. decisions on privacy, [95] even in cases involving uses or disclosures of personal data.[96] Other cases have been less deferential to information privacy as a protectable civil liberty interest,[97] but this conception of information privacy

---

decides there is a constitutional right of privacy in personal data, this would strengthen the argument that Congress has power to protect information privacy interests more generally, although whether granting individuals property rights in their data would be a proper exercise of this authority is an intriguing question. Legislation to create property rights in personal data might also, unless narrowly drafted, run afoul of the First Amendment. See, e.g., Hicks v. Casablanca Records, 464 F. Supp. 426 (S.D.N.Y. 1978) (rejecting a right of publicity claim for commercial use of information about Agatha Christie in a motion picture in part because of First Amendment considerations).

[89] See, e.g., Board of Regents of State Colleges v. Roth, 408 U.S. 564, 577 (1972) (property interests not created by U.S. Constitution, but by state law); Pruneyard Shopping Center v. Robins, 447 U.S. 74, 84 (1980) (questioning the residual authority of the federal government to create property rights).

[90] A number of states have enacted right of publicity statutes to protect such these interests. See, e.g., Calif. Civil Code sec. 3344. Other states have recognized publicity rights through common law process. See, e.g., Zacchini v. Scripps-Howard Broadcasting Co., 433 U.S. 562 (1977) (surreptitious taping of human cannonball act at county fair violated common law right of publicity).

[91] See, e.g., Midler v. Ford Motor Co., 849 F.2d 460, 463 (9th Cir. 1988) (describing publicity rights as property rights).

[92] See, e.g., Sheldon W. Halpern, *The Right of Publicity: Commercial Exploitation of the Associative Value of Personality*, 39 Vand. L. Rev. 1199, 1200 n. 3 (1986) (characterizing publicity rights as "peculiarly celebrity-based, arising only in the case of an individual who has attained some degree of notoriety or fame"). See also Pesina v. Midway Mfg. Co., 948 F. Supp. 40 (N.D. Ill. 1996) (granting summary judgment to video game maker on publicity claim by martial artist on theory that before the video game, his name and likeness had no commercial value); Hicks v. Casablanca Records, 464 F. Supp. 426 (S.D.N.Y. 1978) (questioning whether Agatha Christie had publicity rights given the paucity of evidence she'd made investments to promote the commercial value of her persona as such). But see Dreyfuss, *supra* note 73, at 5 (suggesting that there is no convincing basis for confining publicity rights to celebrities).

[93] See generally Radin, *supra* note 69, at 16-29 (1996) (discussing rationales for making certain rights inalienable).

[94] See, e.g., EU Directive, *supra* note 14, Recital 10 (referencing European Convention for the Protection of Human Rights and Fundamental Freedoms as well as general principles of European Community Law as recognizing data protection as a fundamental civil liberty interest). See also *id.*, Art. 1.1 ("Member states shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.").

[95] See, e.g., Roe v. Wade, 410 U.S. 113, 153 (1973) (finding right of privacy to be "founded in the Fourteenth Amendment's concept of personal liberty and restrictions on state action").

[96] See, e.g., Whalen v. Roe, 429 U.S. 589, 599 (1977) (recognizing constitutionally protected interest in information privacy interests extended to personal data in prescription drug records).

[97] See, e.g., American Fed. Of Gov't Employees, AFL-CIO v. Dept. of HUD, 118 F.3d 786, 791 (D.C. Cir. 1997) (expressing "grave doubts as to the existence of a constitutional right of privacy in the nondisclosure of personal information"); U.S. West, Inc. v. FCC, 182 F.3d 1224 (10th Cir. 1999) (striking down FCC rule

unquestionably has adherents in the U.S.[98] From a civil liberties perspective, propertizing personal information as a way of achieving information privacy goals may seem an anathema.[99] Not only might it be viewed as an unnecessary and possibly dangerous way to achieve information privacy goals, it might be considered morally obnoxious. If information privacy is a civil liberty, it may make no more sense to propertize personal data than to commodify voting rights.[100]

Europeans have more of a civil libertarian perspective on personal data protection in part because of certain historical experiences they have had.[101] One factor that enabled the Nazis to efficiently round up, transport, and seize assets of Jews (and others they viewed as "undesirables") was the extensive repositories of personal data available not only from public sector but also from private sector sources.[102] Europeans may realize more than most Americans the abusive potential for reuses of personal data that may initially have provided to a particular entity for a specific, limited purpose. If more Americans had an appreciation of the negative consequences that might arise from commercial distributions of their personal data, they might perceive personal data protection differently.[103]

---

aimed at protecting information privacy interests of telephone subscribers on First Amendment grounds). The FCC, joined by amici, has sought rehearing of this decision. See, e.g., http://www.epic.org/#hot (visited November 17, 1999).

[98] See, e.g., Congressional Findings and Statement of Purpose, sec. (a)(4), Privacy Act of 1974, Pub. L. No. 93-579, reproduced in THE PRIVACY LAW SOURCEBOOK 1999 (Marc Rotenberg, ed. 1999) at 38 ("the right to privacy is a personal and fundamental right protected by the Constitution of the United States"); "The Supreme Court on Privacy," editorial, N.Y. Times, Nov. 14, 1999 (endorsing the concept of information privacy as a fundamental civil liberty interest). See also Schwartz & Reidenberg, *supra* note 24, Chap. 4 (discussing constitutional roots of privacy rights).

[99] See, e.g., Davies, *supra* note 15, at 159-60 ("The process of commodification [of personal data] is inimical to privacy.")

[100] See generally Pamela S. Karlan, *Not By Money But By Virtue Won? Vote Trafficking and the Voting Rights System*, 80 VA. L. REV. 1455, 1455 (1994) (explaining rationale for public policies against vote trafficking).

[101] See, e.g., Laura Lee Mall, *The Right to Privacy in Great Britain: Will Anti-Media Sentiment Compel Great Britain To Create a Right to Be Let Alone?*, ILSA J. Int'l and Compar. L. 785, 805 (Spring 1998); Nora M. Rubin, *A Convergence of 1996 and 1997 Global Efforts To Curb Corruption and Bribery in International Business Transactions: The Legal Implications of the OECD Recommendations and Convention for the United States, Germany, and Switzerland*, 14 Am. U. Int'l L. Rev 257, 298 (1998) (discussing historical context of privacy protection in Europe).

[102] See, e.g., DAVID H. FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES 306, 373-74 (1989): "European data protection laws include the hidden agenda of discouraging a recurrence of the Nazi and Gestapo efforts to control the population, and so seek to prevent the reappearance of an oppressive bureaucracy that might use existing data for nefarious purposes. This concern is such a vital foundation of current legislation that it is rarely expressed in formal discussions. This helps to explain the general European preference for strict licensing systems of data protection. . . .Thus European legislators have reflected a real fear of Big Brother based on common experience of the potential destructiveness of surveillance through record keeping. None wish to repeat the experiences endured under the Nazis during the Second World War." See also Peter Swire, *Financial Privacy and the Theory of High-Tech Government Surveillance*, 77 Wash. U. L. Quarterly 461, 495 (1999).

[103] See, e.g., PRIVACY RIGHTS CLEARINGHOUSE, SECOND ANNUAL REPORT 21 (1995) ("[Our] major finding…is that consumers suffer from a serious lack of knowledge about privacy issues. Many consumers are unaware of personal information collection and marketing practices. They are misinformed about the scope of existing privacy law, and generally believe that there are far more safeguards than

Congress has sometimes legislated information privacy protections out of concern about cognitive difficulties in appreciating the risks of supplying personal data to private sector firms, for example, in respect of gathering information from children under the age of thirteen.[104] On occasion, Congress has also recognized that adults too may not appreciate certain risks in supplying personal data to private sector firms and has decided that in those instances even the adults should be protected. When renting certain video cassettes from a corner rental store, Robert Bork, for example, surely did not anticipate that he was running the risk that the owner of the video store might disclose his rental choices to the press while he was a nominee to the U.S. Supreme Court.[105] The disclosure of his viewing choices was not, under then existing law, illegal. It is illegal now. And the Video Privacy Protection Act is far from the only law of this kind.[106] Congress has also acted to protect individuals against public sector commercialization of drivers' license data in part because of the involuntary nature of this particular kind of data collection and in part because of negative consequences arising from the widespread market availability of such data.[107]

As difficult as it may be for the average person to judge the risks of personal data misuse as a general matter, it may be even more difficult for the average person to judge the risks of selling her property rights in personal data.[108] Data collectors may well insist on broad transfers of all of a person's right, title and interest in her personal data.[109]

---

actually exist.") as cited in Kang, *supra* note 2 at n. 255; Pitofsky Remarks, *supra* note 6, at 1 (indicating that consumers have "little, if any, knowledge" about online profiling currently being done). See also Bibas, *supra* note 11, at 597-98; Harvard Developments, *supra* note 33, at 1644; R. Craig Tolliver, *Filling the Black Hole In Cyberspace: Legal Protections for Online Privacy*, 1 Vand. J. Ent. L. & Prac. 66, 70 (1999) (noting consumer ignorance of private sector data collection and processing practices). Often consumers do not know that firms are collecting data about them. See Pitofsky Remarks, *supra* note 6, at 1; Tolliver, *supra*, at 67-68.

[104] See Children's Online Privacy Protection Act of 1998, Pub. L. No. 105-277, 112 Stat. 2681-728 (1998) (requiring parental consent before websites targeting children can collect personal data from children under the age of 13). The FTC had recommended legislation of this sort in part because of "[c]hildren generally lack the developmental capacity and judge to give meaningful consent to the release of personal information to a third party." See FEDERAL TRADE COMMISSION, PRIVACY ONLINE: A REPORT TO CONGRESS at 5 (1998), available at http://www.ftc.gov/reports/privacy3/toc.htm, (cited hereinafter as "FTC Report")

[105] See Video Privacy Protection Act, 18 U.S.C. sec. 2710. See Schwartz & Reidenberg, *supra* note 24, at 10 (discussing the circumstances leading up to adoption of the "Bork Bill").

[106] See, e.g., Cable Communications Policy Act, 47 U.S.C. sec. 551; Electronic Communications Privacy Act of 1986, 18 U.S.C. sec. 2701 et seq. See generally Schwartz & Reidenberg, *supra* note 24 for examples of U.S. information privacy laws.

[107] See Drivers' Privacy Protection Act of 1994, 18 U.S.C. sec. 2721. See Protecting Driver Privacy: Hearings Before the Subcomm. On Civil and Constitutional Rights of the House Comm. Of the Judiciary, 103d Cong., 2d Sess (Feb. 4, 1994) (explaining rationale for this legislation). The constitutionality of this legislation is currently under review by the U.S. Supreme Court. See *supra* note 31 and accompanying text.

[108] Consider also that if someone loses her car, she can always get a new one, but when she loses her privacy, it may well be gone forever.

[109] Data compilers would likely prefer broad transfers because this might mean fewer contractual restrictions to negotiate and keep track of. Yet, if the goal of legal protection is to achieve information privacy, these concerns of compilers of personal data should not be paramount.

While such a broad transfer works very well in a sale of a used car or a house, it may be troublesome in the context of personal data. As a result of such a transfer, an individual could potentially be foreclosed from any control over these data in the hands of the transferee or in the hands of other firms to whom the data might have been transferred. The individual could even be precluded from engaging in further transactions to sell the same data to other firms because her rights in the data now belong to a personal data aggregator. Other firms wanting to get access to or use these data would have no choice but to go to the data aggregator and license the data from that firm- on terms that would likely reflect the interests of the aggregator rather than those of the individual whose data has been licensed.

This cluster of problems could be mitigated if the individual makes a more limited grant of rights to a data aggregator,[110] but this may suggest that a different approach to protecting information privacy may be more satisfactory than a property rights approach. It is unusual for a property rights regime to establish a rule or strong presumption against alienability.[111] A property approach may also thwart information privacy goals unless the law makes it clear that a person does not abandon property rights in personal data when visiting websites that collect personal data.[112] The rhetoric of property law may also be unsuited to further elucidation of normative understandings about acceptable and unacceptable uses of personal data that is sorely needed in this era of rapid technological, economic, and social change.

C. A Moral Right in Personal Data?

As vigorously as this subsection has argued against a property rights model for protecting personal data, it has done so because the standard models of property rights seem unsuitable to achieving information privacy goals. There is, however, one rather unusual class of property right that protects personhood interests of individuals, melding economic, reputational, and autonomy interests at its core. In the spirit of providing

---

[110] See, e.g., Varian, *supra* note 68, at 5 (on advisability of restrictions on transfer of rights in personal data).

[111] See, e.g., RESTATEMENT OF PROPERTY § 409 (1944), comment a; and ROGER A. CUNNINGHAM, WILLIAM B. STOEBUCK and DALE A. WHITMAN, THE LAW OF PROPERTY (1993) at § 2.15 (prohibitions against restraints on alienation are relaxed in the case of life estates, primarily because life estates are not that marketable to begin with; however, even so, certain conditions must be met for the restraint to be valid.) See also Radin, *supra* note 69, at 16-29 (discussing general policy favoring alienability of property rights and arguments against making property rights inalienable in the market). In the United States, however, there is a statutory scheme specifically designed to *prevent* the alienation of certain types of information: 42 U.S.C.A. § 2274 makes it a criminal act to communicated 'restricted data' when it is known that communication of such data might injure the U.S. or benefit a foreign nation. Although there are procedures for determining when information is 'classified', 42 U.S.C.A. § 2162, some information is considered by the U.S. government to be 'born classified'. See, e.g., Peter Swan, *A Road Map to Understanding Export Controls: National Security in a Changing Global Environment*, 30 Am. Bus. L.J. 607 (1993) at footnote 37; and Harold P. Green, *Constitutional Implications of Federal Restrictions on Scientific Research and Communication*, 60 UMKC L. Rev. 619, 630 (1992).

[112] Another issue with which a property rights regime would have to contend is whether an individual could assert property rights against a party who obtained her data from public records (e.g., publicly accessible drivers license data). See Varian, *supra* note 68, at 7-9 (discussing public policies favoring access to and reuse of personal data).

exemplars from the existing tool kit of property law, it may be worth mentioning "moral rights" of authors as a model for a nontraditional property right that might be adaptable to protecting personal data.[113]

In Europe and many other nations, authors have "moral rights" in the works they have created.[114] These rights are distinct from the purely economic rights that European law, like American copyright law, grants to authors. The moral rights regime derives from a conception of artistic and literary creations as emanations of the author's personality in which he can and should retain an interest even after copies of the work have entered the stream of commerce.[115] Among the commonly recognized moral rights are the rights of attribution (i.e., the right to be identified as the author of the work) and of integrity (i.e., the right to protect the work from alterations that would be harmful to the authors' reputation).[116] In some jurisdictions, authors also have moral rights of "divulgation" (i.e., the right to decide when and under what circumstances to divulge the work) and sometimes even of withdrawal (i.e., the right to withdraw all published copies of the work if the work no longer represents the author's views or otherwise would be detrimental to the author's reputation).[117]

Moral rights are generally waivable by contract, although some countries—notably France—regard such rights as sufficiently important and vulnerable to unfair contractual overrides that they have made rights inalienable.[118] An advantage of moral rights is that

---

[113] The term "moral right" is a rather rough translation of the French term, "droit moral." At least one commentator has suggested the use of a more exact terminology, namely that of the German term, "Urheberpersonlichkeitsrecht," meaning "author's rights of personality,": see, 1 S. LADAS, THE INTERNATIONAL PROTECTION OF ARTISTIC AND LITERARY PROPERTY § 272 (1938).

[114] There are many countries that protect moral rights, but the two most commonly discussed are France and Germany. See, respectively, Loi du 11 mars 1957 Sur la Propriete Litteraire et Artistique, 1957 J.O. 2733, 1957 D.L. 102 (Fr.) [hereinafter French Act] (translated in UNESCO, 1 COPYRIGHT LAWS AND TREATIES OF THE WORLD (1987)); and Gesetz uber Urheberrecht und verwandte Schutz rechte, 1965 Bundesgesetzblatt [BGB1.] I art. II (F.R.G.) [hereinafter German Act] (translated in UNESCO, 2 COPYRIGHT LAWS AND TREATIES OF THE WORLD art. II (1987)).

[115] See, e.g., the discussion in Neil W. Netanel, *Alienability Restrictions And The Enhancement Of Author Autonomy In United States And Continental Copyright Law*, 12 Cardozo Arts & Ent. L.J. 1, 7 (1992): "Although a work may be commercially exploited, it is not simply a commodity--and many commentators would say that it is not a commodity at all. Instead, the work is seen, partially or wholly, as an extension of the author's personality, the means by which he seeks to communicate to the public. 'When an artist creates, ... he does more than bring into the world a unique object having only exploitive possibilities; he projects into the world part of his personality and subjects it to the ravages of public use,'" quoting from Martin A. Roeder, *The Doctrine of Moral Right: A Study in the Law of Artists, Authors and Creators*, 53 HARV.L.REV. 554, 557 (1940). See also Radin, *supra* note 69, at 20 (noting that some interests are incompletely commodified).

[116] The right of attribution is codified in Article 6 of the French Act, *supra* note 114; and in Article 13 of the German Act, *supra* note 114. The right of integrity is codified in Article 6 of the French Act, *supra* note 114; and in Article 14 of the German Act, *supra* note 114.

[117] The right of divulgation is codified in Article 19 of the French Act, *supra* note 114; and in Article 12 of the German Act, *supra* note 114. The right of withdrawal is codified in Article 32 of the French Act, *supra* note 114.

[118] Continental authors may choose not to enforce their moral right out of fear of reprisals from producers and publishers in a tightly knit creative community, but this does not mean that they could not legally do so if they chose. See, e.g., Judgment of Dec. 12, 1988 (Delorme v. Catena-France), Cour d'appel, P.I.B.D. III, No. 454, 231, cited in Netanel *supra* note 115, at footnote 123 (even a copyright assignment "for all

these rights can be exercised long after the author has sold copies of her work to the public and can be exercised against remote purchasers. If the owner of a sculpture, for example, alters it in a way that the sculptor deems detrimental to his interests (for example, by tying red ribbons around its neck), the sculptor can assert his moral right of integrity in the work and can obtain injunctive relief requiring restoration of the original.[119] While moral rights generally focus on the personal, reputational interests of authors, an economic consideration may partly underlie moral rights. "Mutilation" of an author's work can tarnish the author's reputation in ways that may be difficult to measure, akin to the harm to goodwill when trademarks are disparaged or tarnished.[120]

A moral right-like approach might be worth considering as to personal data. As with the moral right of authors, the granting of a moral right to individuals in their personal data might protect personality-based interests that individuals have in their own data. The admixture of personal and economic interests could be reflected in the right. The integrity and divulgation interests may be the closest analogous moral rights that might be adaptable to protect personal data. An individual has an integrity interest in the accuracy and other qualitative aspects of personal data, even when the data are in the hands of third parties.[121] An individual also has an interest in deciding what information to divulge, to whom and under what circumstances.[122] An advantage of a moral rights-

---

purposes" requires the author's permission to modify the work). For a general discussion of the actual inalienability of the Continental right, see Netanel, *supra* note 115, at notes 254-305 and accompanying text (core of moral rights are properly considered to be inalienable under Continental law).

[119] See Snow v. Eaton Centre, 70 C.P.R.2d 105 (Ont. H.C.J. 1982).

[120] See, e.g., Soc. Le Chant du Monde v. Soc. Fox Europe, Jan. 13, 1953, Cours d'appel, Paris, Dallez, Jurisprudence, [D. Jur.] 16, 80, where the court held that Russian composers could prevent their music from being used in a film that had an anti-soviet theme, because of the 'moral damage' that would result. This case is discussed in Roberta R. Kwall, *Copyright And The Moral Right: Is An American Marriage Possible?,* 38 Vand. L. Rev. 1, 27-28 (1985). Section 43(a) of the Lanham Act can sometimes be used to protect an artist's reputation in a manner similar to protection available under moral rights law. See, e.g., Gilliam v. American Broadcasting Companies, 538 F.2d 14 (2d Cir. 1976) (Lanham Act invoked to prevent the television broadcast of a modified version of a Monty Python movie).

[121] See, e.g, Rose Aguilar, *Research Service Raises Privacy Fears*, Cnet News.com, (June 10, 1996) available at <http://news.cnet.com/news/0-1005-200-311506.html?tag=>. After gathering personal data (such as social security numbers, addresses, names and aliases) from various sources, Lexis-Nexis offers a centralized searching service to government or anyone else seeking such information. There is no oversight on who actually uses the service or how they use it. The service is also targeted to individuals, journalists, etc., who might want to find spouses that have missed support payments or engaged in criminal behavior. The range of harms that could result from such a collection of data appears obvious: think of a journalist working on a story about husbands who skip their support payments, or investigators who pursue an individual based on inaccurate information. Because the risk of data inaccuracy increases with the number of times data changes hands, this type of service, which involves at least four transfers, seems particularly prone to inaccuracy. See the range of products offered at: <http://www.lexisnexis.com/lncc/government/>.

[122] This interest was strikingly illustrated in the case of McVeigh v. Cohen, 983 F.Supp. 215 (D.D.C. 1998). Like many users of America OnLine, McVeigh took advantage of the opportunity to adopt a pseudonymous identity for interacting with other people on AOL and create for this identity an online profile which other users of AOL could see which included a reference to his being "gay." U.S. Navy officials, after becoming suspicious that this profile might be about McVeigh, sought confirmation from AOL, and after receiving this confirmation, the Navy sought to expel him from service. Although this case involved 'public' information, McVeigh did not use his real name in the profile, thus attempting to keep his identity undisclosed.

like approach is that this right can be asserted against persons beyond those with whom one has contracted. Contract law, in general, provides relief for breach as between the parties to a contract, not rights against third parties.[123] Firms that collect and process personal data are often not in privity with the individual whose data is being used.[124]

A moral right-like approach would overcome a second important limitation of a purely contractual approach which generally aims to compensate the non-breaching party through an award of damages, not by granting injunctive relief.[125] Property law, in contrast, generally allows the owner of the right to exclude other people from engaging in certain activities, and injunctive relief is consequently generally available.[126] A person who has licensed a particular use of her personal data, but not another use, would almost certainly want injunctive relief upon learning that her licensee is using the data for more

[123] The requirement of privity is a foundational principle of contract law (being an the inevitable consequence of bargain theory). In some cases a third party is allowed to 'step into the shoes' of one of the actual parties to the contract. See, e.g., E. ALLAN FARNSWORTH AND WILLIAM F. YOUNG, CONTRACTS: CASES AND MATERIALS (fifth edition) at 863-870. Generally, this substitution is allowed when the contract has been signed by A, but for the benefit of a third party, B. In American jurisprudence such contracts are known as 'third party beneficiary contracts, and one of the most common examples of this are insurance contracts. For a straightforward application of the privity doctrine, see, e.g.: Hanback v. Dutch Baker Boy, 70 App.D.C. 398, 107 F.2d 203 (App.D.C. 1939) (No suit in contract under the theory of implied warranty after a child gets food poisoning from a chocolate éclair because child was not in privity with the seller. Her mother bought the éclair, and so was the only person in privity with the seller.). The harshness of the privity requirement has been recognized and relaxed in the case of implied product warranties (which are imposed on contracts involving the sale of goods): see, e.g., Henningsen v. Bloomfield Motors, Inc., 32 N.J. 358, 161 A.2d 69, 75 A.L.R.2d 1 (N.J., 1960) (strict privity not required in cases involving implied warranty of merchantability).

[124] This situation arises because companies who collect data from individuals with whom they have a business relationship often sell this data to third parties. These third parties are not in any contractual relationship with the individual who originally supplied the data. This practice is especially common in industries which generate 'transactional data' such as the banking industry. See, e.g., Julie Tripp, *A Cause For the Masses: Banks Selling Personal Data*, The Oregonian, (June 27, 1999) available at <http://www.oregonlive.com/business/99/06/bz062706.html>.

[125] The general unavailability of injunctions is witnessed by the fact that we generally do not speak of injunctions *per se* in contracts, but instead speak of awarding specific performance of the contract. Of course, in some cases, specific performance requires that certain activities be enjoined. A common example of this is the situation of non-competition agreements, in which the courts will enjoin a former employee from competing with the employer for a 'reasonable' length of time, as long as the non-compete agreement does not unreasonably prejudice the former employee's ability to earn a livelihood: Comprehensive Technologies Intl. v. Software Artisans, Inc., 3 F.3d 730 (4th Cir. 1993). For a general discussion of when specific performance will be ordered in a contract see, e.g.: First Nat. State Bank of New Jersey v. Commonwealth Federal Sav. and Loan Ass'n of Norristown, Pa., 455 F.Supp. 464 (D.N.J., 1978) (specific performance is only ordered when damages are otherwise inadequate, or where they cannot be calculated accurately). Also see RESTATEMENT (SECOND) OF CONTRACTS, § 357 "Availability of Specific Performance and Injunction".

[126] See, e.g., *Panduit Corp. v. Stahlin Bros. Fibre Works, Inc.*, 575 F.2d 1152, 1158 n.5, 197 U.S.P.Q. (BNA) 726 (6th Cir. 1978) (Markey, J., by designation) as cited in ROBERT P. MERGES, PATENT LAW AND POLICY (1997) at 973: "Patents must by law be given 'the attributes of personal property.' 35 U.S.C. § 261. The right to exclude others is the essence of the human right called 'property'. The right to exclude others from free use of an invention protected by a valid patent does not differ from the right to exclude others from free use of one's automobile, crops, or other items of personal property." (discussing rationale for the default rule of injunctive relief in patent law).

than the authorized purpose.[127] A property right in her personal data could provide grounds for injunctive remedy.

However, the idea of creating a moral right-like interest in personal data presents many difficulties. For one thing, U.S. law has generally been inhospitable to the idea of moral rights of authors,[128] even though it has ratified a treaty that requires such protection.[129] This augurs poorly for adaptation of the concept to protection of personal data. It is also unclear what constitutional authority Congress would have for enacting legislation of this sort. Moreover, even the Europeans might balk at the idea of generalizing the moral right concept for personal data because it undermines the special status of authorship that provides the theoretical justification for existing moral rights law.[130]

Two state law doctrines out of which a moral right-like interest might emerge are right of publicity law and the appropriation branch of privacy law. Right of publicity law, like moral rights law, has generally protected the interests of special status individuals (in the case of publicity rights, the interests of "celebrities"),[131] and like intellectual property laws, publicity law largely concerns itself with providing an appropriate incentives to induce investments in creative efforts, not to protect personality-based interests.[132] The appropriation tort could be extended to provide individuals with a protectable interest in personal data.[133] Even though the right created would not be a "property right,"[134] it could still allow individuals to contract about allowable uses of personal data[135] and to police third party uses of personal data insofar as these uses were objectively unreasonable in a normative sense.[136] This tort protects dignity, integrity, and

---

[127] It is unlikely that McVeigh or the impotent men discussed *supra* note 39 would license the use of certain personal information for purposes that they would not, *ex ante*, have approved. An injunction to prevent the use would therefore appear to be the desired remedy in many cases involving personal data.

[128] See, e.g., the discussions in Netanel, *supra* note 115 at footnote 12 (Discussing the vehement opposition to moral rights by Congress and American legal scholars.); and Kwall, *supra* note 120 at 57-72 (American copyright law has several entrenched doctrines which prevent the wholesale adoption of Continental-style moral rights.).

[129] On March 1, 1989, the U.S. acceded to the BERNE CONVENTION FOR THE PROTECTION OF LITERARY AND ARTISTIC PROPERTY, Sept. 9, 1886, 123 L.N.T.S. 233, last revised in Paris on July 24, 1971 (cited hereinafter the Berne Convention). Article 6bis of the Berne Convention requires signatories to protect the moral rights of authors.

[130] See, e.g., Netanel, *supra* note 115.

[131] See *supra* note 92 and accompanying text.

[132] The publicity right arises under the "commercial advantage" prong of the invasion of privacy tort: Restatement (2d) Torts § 652C. It therefore protects economic, rather than personality, interests. See, e.g., the discussion in the majority's opinion in White v. Samsung Electronics America, Inc. 989 F.2d 1512 (9th Cir. 1993).

[133] See, e.g., Jonathan Kahn, *Bringing Dignity Back to Light: Publicity Rights and the Eclipse of the Tort of Appropriation of Identity*, 17 Cardozo Arts & Ent. L.J. 213 (1999).

[134] *Id*. at 213. See also Robert C. Post, *Rereading Warren & Brandeis: Privacy, Property, and Appropriation*, 41 Case West. Res. L. Rev. 647 (1991) (distinguishing between the right of publicity and the appropriation tort).

[135] See, e.g., N.Y. Civil Rights Law, secs. 50-51 (proscribing use of a person's name or likeness unless written consent has been obtained from that person).

[136] See, e.g., Kahn, *supra* note 133, at 215.

autonomy based interests of individuals by setting bounds on acceptable behavior.[137] However, the appropriation privacy tort seems an unsuitable way to establish a market-based system for enabling transactions in personal data in which the individual participates, even though this is what many Americans seem quite willing to do with personal data.[138] The next section will explain why a licensing system built on modified trade secrecy default principles might offer a useful model for licensing of personal data, and will offer some suggestions about how such a system might be implemented to facilitate greater protection for personal data in cyberspace.

III. Modified Trade Secrecy Default Rules for Promoting Information Privacy

The law can grant individuals a protectable interest in their personal data without grounding that interest in property law.[139] It can do so by setting a default rule forbidding certain activities with respect to these data, such as unauthorized collection or uses of them unless the individual has agreed to these activities.[140] Because market imperfections make it difficult to negotiate effectively about terms of use as to personal data, [141] it may make sense to establish some default terms for such agreements which the parties could override if they so chose. Although trade secrecy and information privacy laws obviously differ in many significant respects, these laws nonetheless have at least three important interests in common: (1) an interest in protecting the interest of the claimant to restrict access to and unauthorized uses of secret/private information; (2) an interest in giving firms/individuals control over commercial exploitations of secret/private information, and (3) an interest in setting and enforcing minimum standards of commercial morality. To achieve policy goals embodied in these interests, trade secrecy law has evolved a set of default licensing rules. Some of these default rules may be adaptable to the licensing of personal information.

A. Rationale for Adapting Trade Secrecy Default Rules to Licensing of Personal Data

Like the information privacy law contemplated in this article, trade secrecy law facilitates license transactions in information while at the same time providing default rules to govern uses and disclosures of protected information and setting minimum

---

[137] In addition to damages for mental anguish and injured feelings, injunctive relief can be awarded in appropriation privacy cases. See, e.g., Kahn, *supra* note 133, at 265-266; Post *supra* note 134 at 667 (on the issue of damages); STIG STRÖMHOLM, RIGHT OF PRIVACY AND RIGHTS OF PERSONALITY (Stockholm: P.A. Nordstedt, 1967) at 151-164 (on remedies generally).

[138] See *supra* note 16 and accompanying text.

[139] See, e.g., Federal Elections Campaign Law, 2 U.S.C. sec. 438 (a)(4) (limiting commercial reuses of lists of campaign contributors); Privacy Act, 5 U.S.C. sec. 552a(b); Video Privacy Protection Act, 18 U.S.C. sec. 2710 (prohibiting disclosures of video rental records except under stated circumstances).

[140] See, e.g., Kang, *supra* note 2, at 1265-67 (considering an inalienability rule for personal data, but concluding that "if a person wants to exercise [her right of] control by disclosing information for various reasons, including monetary compensation, then the state should hesitate to proscribe information flow on some paternalistic theory." *Id.* at 1266.) See also EU Directive, *supra* note 14, Art. 7(a) (collection and processing of personal data is lawful if collector/processor has consent of individual)

[141] See *supra* note 10 and accompanying text. It may be sensible to consider licensable personal data as "incompletely commodified," to borrow Professor Radin's useful phrase. See Radin, *supra* note 69, at 20.

standards of acceptable commercial practice. Information privacy rights, like trade secrecy rights, can be based on contractual agreements, on conduct between the parties from which it is reasonable to infer that information was disclosed in confidence and use and disclosure beyond those purposes is wrongful, on the use of improper means to get the information.[142]

Agreement-based trade secrecy typically occurs when A has nonpublic information to which B wants access. A agrees to give B access to the information in exchange for B's agreement to respect certain restrictions on use and abide by other terms and conditions (e.g., payment of a stated sum or royalty). Because of the exchange value of such information, trade secret information can be a highly valuable asset of the firm and provide it with a substantial revenue stream.[143] The information, however, does not become "public" simply because a number of firms possess it - as long as each is under an implicit or explicit pledge to maintain the nonpublic status of the information.[144]

Confidential relationship-based trade secrecy may arise when A reveals certain nonpublic information to B under circumstances in which B would have reason to understand the limited purpose of the disclosure, and that use and disclosure for other purposes would be wrongful.[145] For example, if a firm discloses certain nonpublic information about the firm's operations to a consultant, the consultant will understand that he is entitled to use this data only for purposes of analysis in order to advise the company about how to improve its operations. The revealed information may have a commercial value beyond its utility to aid the consultant in doing his job, but the consultant understands that it would be inappropriate to sell or release the information to another firm or to reveal it to stockbrokers so they could make better decisions on whether to trade in that firm's securities. Both the consultant and the firm would understand, even if they didn't specifically agree, that rights to control uses of the information reside in the firm, not the consultant.

For similar reasons, individuals often regard the data that they reveal to others—their accountants, doctors, banks, just to name a few examples—as having been provided to those firms for limited purposes. Uses and disclosures of the data, whether internally or to third parties, may be inappropriate unless undertaken for purposes consistent with the initial disclosure. Just as the consultant could not justify revealing information to a third party on a theory that this disclosure would enable the other firm to provide new or better service to the company, individuals may be skeptical of those who argue that

---

[142] See discussion *infra* notes 146-55 and accompanying text.

[143] See, e.g., Josh Lerner, *The Importance of Trade Secrecy: Evidence from Civil Litigation*, Harv. Bus. School Working Paper #95-043 (Dec. 1994); and JAMES POOLEY, TRADE SECRETS § 9.01 (1997) (trade secret theft estimated to cost the U.S. economy between 5 and 10 billion dollars annually).

[144] See, e.g., 1 JAY DRATLER, INTELLECTUAL PROPERTY LAW: COMMERCIAL, CREATIVE, AND INDUSTRIAL PROPERTY § 4.03[3][b] (1991). As Dratler points out, the whole purpose of the law of trade secrets is to promote licensing and exchange of non-patented know-how between businesses and employees. The requirement in trade secret law is therefore, not absolute secrecy, but rather 'relative' secrecy.

[145] See, e.g., Smith v. Dravo Corp., 203 F.2d 369 (7th Cir. 1953) (implied confidential relationship arose from disclosure of trade secret information to enable other firm to evaluate whether to negotiate a proposed business deal).

disclosure of their personal data to a third party is justifiable because it enables that firm to offer service to them.

In trade secrecy law, as in the information privacy law contemplated in this article, there is no need to say that a property right exists in the protected information. [146]

[146] It must be noted here that although trade secret law does not rely on property rights 'as such', there is an ongoing debate about the exact nature of the rights underlying this body of law. There are two main theories behind trade secret law, generally referred to as the 'property school' and the 'confidential relationship' school. See, e.g., the discussion in Pooley, *supra* note 143, at § 1.02[8]. The choice of characterization is more than semantic; it has a practical impact on the legal consequences that courts will impose on parties. While Pooley prefers to settle the debate by referring to the regime as 'hybrid', *id.* at § 1.02[8][d], Milgrim gives the property theory more weight, pointing to the fact that the owner of a trade secret can exclude the world from his secret, and the fact that a trade secret can be assigned in the manner of property, especially when a business is sold, etc.: see discussion in 1 ROGER M. MILGRIM, MILGRIM ON TRADE SECRETS § 2.01 at 2-4 (1967). However, this author thinks that the answer to the exclusion point is that the right is not 'good against the world', except in so far as the owner's power to control the behavior of those he stands in confidential relations to: i.e., the exclusionary power is actually just a by-product of the relational power that the owner has against those in certain types of relationships with him. That this is so, is manifested by the fact that the 'exclusionary power' can only be maintained if it accompanied by the efforts of the owner to maintain actual secrecy. So, what appears to be a right against the world is merely a functional product of actual secrecy supplemented by enforced behavior on certain people who can destroy that secrecy. Furthermore, the descendability of trade secrets does not really support a characterization of the rights as a 'property' regime, as the issue here is not that the 'owner' or the assignee can exclude the world. Instead, the issue is *who* can exclude those in a confidential relationship or those who would otherwise use improper means to obtain the trade secret. We should not be confused in our characterization of the regime by the fact that courts have adopted a legal fiction (i.e., that of calling a trade secret property) for specific pragmatic reasons, such as to make the right descendable. An even more convincing argument for the 'property' characterization of trade secrets is the development of the 'improper means' branch of misappropriation. Trade secrets were historically considered *not* to be property. Both the Supreme Court's unequivocal statement in *E.I. du Pont & Co. v. Masland*, 244 U.S. 100(1917), and the RESTATMENT OF TORTS § 757 (1939), make this abundantly clear. However, courts and jurists soon saw that the 'breach of confidential relationship' ground of trade secret misappropriation was insufficient to police commercial morality, and therefore interpreted the 'improper means' branch of trade secret misappropriation as completely separate from any relationship between the parties. So, there are two, completely separate grounds for misappropriation: 'breach of confidence' and 'improper means'. I think you can see how the 'improper means', because it applies to everyone, looks like a property right. You could even conceptualize the 'breach of confidence' as one branch of improper means – and this line of reasoning adds even more support to the property school. And yet, in the opinion of this author, even the 'improper means' ground of trade secret misappropriation does not transform the trade secret in to a property right. We must remember that the locus of the trade secret right is in the behavior of the non-owner B, rather than the trade secret of the owner A. A does *not* have the right to exclude B from the trade secret, he merely has the ability to prevent B from taking *certain actions* to obtain it. An analogy might be useful in drawing this distinction. If I drop my purse, I can still sue to get in back, even though the person who finds it can't be charged with 'theft'. 'Finders keepers' rules are exceptional in the law, and usually are created for specific purposes, such as to promote salvage on the high seas via pecuniary reward. The fact that people don't sue people who find their purses because they don't know who found the purse is an evidentiary, rather than a legal, issue. On the other hand, if I 'drop' my trade secret while walking down the street, and my competitor discovers it, I cannot sue to get it back, even before he has disclosed it to anyone else. I also could not get an injunction preventing him from using or disclosing the trade secret, as he did not use improper means to obtain it. So, we can view the obligation of the trade secret owner to use reasonable efforts to maintain secrecy, as an implicit confirmation of the non-property status of trade secrets, because it is this obligation which effectively destroys the property character of the right. Of course, it should also be noted that the ALI has moved trade secrets closer to the status of a property right by providing a right of action against third parties who innocently discover the trade secret, once they

Although courts have sometimes loosely referred to trade secrets as the "property" of the firm that licensed them and have on occasion held trade secrets to be property for certain purposes, [147] the more appropriate way to characterize a firm's interest in a trade secret is to say that the law protects the firm against breaches of contracts and confidential understandings, [148] as well as against the use of improper means to obtain the secret. [149] Despite its frequent presence in texts of intellectual property law,[150] trade secrecy law remains firmly rooted in unfair competition law.[151] A true intellectual property right provides the owner with rights to exclude that are good against the world at large as to innovations that are generally widely distributed to the public.[152] Trade secrecy law, by contrast, remains a tort law that enforces minimum standards of commercial morality.[153] Going through trash bins outside a firm's office may, for example, be an acceptable way for the government to obtain information when investigating a crime,[154] but the law of trade secrecy regards this means of obtaining trade secrets to be improper and the trash searcher as a misappropriator of trade secret information.[155]

---

receive notice of the status of the trade secret: see discussion *infra* notes 165-67 and accompanying text. However, the author submits that this limited modification of the right seeks to prevent misappropriators from carelessly 'leaking ' the trade secret to 'innocent' third parties, who can then claim that they did not misappropriate the secret. Therefore, this rule is more about evidentiary issues involved in policing business behavior, than about transforming the trade secret into a property right. In the end, the overriding concern of the trade secret regime is with policing the behavior of business entities. In addition, the paucity of cases involving innocent third party 'misappropriators', see *infra* note 167, means that this modification to the right is more theoretical than real.

[147] See, e.g., Ruckelshaus v. Monsanto, 467 U.S. 986 (1984) (finding trade secret information to be "property" within the meaning of the Fifth Amendment for purposes of deciding whether the government's unauthorized use or disclosure of the information should be subject to eminent domain rules). See Samuelson, *supra* note 26, at 378-383 (critical of the property characterization for trade secrecy rights and of the Court's interpretation of Missouri law in *Ruckelshaus*).

[148] The breach of confidential relationship and breach of contract grounds are often closely related in trade secret law, but they are conceptually distinct. Sometimes, a confidentiality agreement or other restrictive contract will help to establish a confidential relationship, but courts will often impose a confidential relationship without contractual restrictions on disclosure, particularly in the case of employees. See, e.g., Milgrim, *supra* note 146, at § 4.02[1][b] and cases discussed therein. Restrictive licensing agreements may also be used by the courts as evidence that sufficient efforts were made to maintain secrecy: Schalk v. State, 823 S.W.2d 633, 638-640 (Tex. Crim. App. 1991), cert denied, 118 L.Ed.2d 425 (1992).

[149] See, e.g., E.I. duPont deNemours & Co. v. Christopher, 431 F.2d 1012 (5th Cir. 1970), cert denied, 400 U.S. 1024 (1971), (Improper means is a separate branch of trade secret misappropriation, which neither requires a breach of a confidential relationship or illegal conduct. Industrial espionage, though not itself a criminal act, constitutes improper means when the trade secret owner was using reasonable efforts to maintain its secrecy.)

[150] See, e.g., Merges et al., *supra* note 74, Chap. 2.

[151] See, e.g., RESTATEMENT (THIRD) OF UNFAIR COMPETITION, §§ 39-45.

[152] See, e.g., 17 U.S.C. sec. 106 (setting forth exclusive rights of copyright law); 35 U.S.C. sec. 271 (setting forth exclusive rights of patentees).

[153] See, e.g, Kewanee Oil Co. v. Bicron, 416 U.S. 470, 497-498 (1974). Although there are other policies implicated in trade secret laws, maintaining commercial morality is a dominant interest. See 1 MELVIN JAGER, TRADE SECRETS LAW § 1.03, at 1-4 (1982). Some of the other policies are: the promotion of investment in research, exploitation of knowledge, privacy, mobility of labor and free competition. For a thorough discussion of these alternate policies, see Pooley, *supra* note 143, at § 1.02[3]-[7].

[154] See, e.g., California v. Greenwood, 486 U.S. 35, 40 (1988).

[155] See, e.g., Drill Parts & Service Co. v. Joy Manufacturing Co., 223 U.S.P.Q. 521, 526 (Ala. 1983); and discussion in Pooley, *supra* note 143, at § 6.02[2][e].

Trade secrecy law has a number of default rules that might be useful for information privacy protection. The general rule of trade secrecy licensing law is that if the licensor has provided data to another for a particular purpose, the data cannot be used for other purposes without obtaining permission for the new uses.[156] Licensing law generally accommodates the reasonable expectations of the parties.[157] If a licensor has failed to specify a limitation on use, the limitation may still be enforced so long as circumstances surrounding the agreement reasonably support an implicit understanding about limitations on use.[158] Moreover, licensing law generally permits revocation of the license for breach of material terms.[159] Contract law, far more than property law, takes into account cognitive difficulties individuals may have in assessing the risks of certain transactions and provides protections to overcome these cognitive problems.[160] Some of these doctrines may be adaptable to licensing of personal data, particularly in view of the cognitive difficulties people often have in assessing risks of permitting certain uses of personal data.[161]

One of the most significant advantages of the licensing regime is that it avoids the problems of a property rights approach deriving from its preference for free alienation. The general default rule of trade secret licensing law is that license rights are non-transferable unless the licensor grants a right to sublicense.[162] Sublicenses, if permitted,

---

[156] Although this principle is illustrative of a more general contractual rule of construing the actual agreement between the parties, this particular default rule finds strong expression in the context of trade secrets. See, e.g., Data General Corp. v. Grumman Sys. Support Corp., 36 F.3d 1147, 1165-1169, (1st Cir.), *partial summary judgment granted*, 32 U.S.P.Q.2d 1946 (D. Mass. 1994).

[157] This is a general principle of contract interpretation: CORBIN ON CONTRACTS § 1.1. (1993). See also, e.g., Darner Motor Sales, Inc. v. Universal Underwriters Ins. Co., 140 Ariz. 383, 682 P.2d 388 (1984) (unambiguous terms in standard-form contracts will not be given their effect if they do not meet the reasonable expectations of the parties).

[158] This is simply an application of the general contractual principle that a court will seek to protect and enforce the reasonable expectations of the parties. So, e.g., a court may refuse to interpret a term in a contract literally when the circumstances indicate that an alternate meaning was intended: Tartleff v. Truscelli, 110 A.D.2d 240 (2d Dept. 1985) discussed in Corbin, *supra* note 157, at § 1.1 (1993).

[159] See, e.g., Chameleon Dental Products Inc. v. Jackson, 18 U.S.P.Q.2d 1044 (7th Cir. 1991). The exact nature of what qualifies as 'material' does, however, differ between states and between judgments. See, e.g., Skil Corporation v. Lucerne Products Inc., 206 U.S.P.Q. 792 (Dist. Ct., N.D. OH 1980) (licensor entitled to terminate only if the licensee's behavior indicated abandonment of the contract or caused irreparable injury).

[160] Numerous contract doctrines seek to prevent a weaker party from making an improvident bargain. Whether this is conceived of as a cognitive dissonance sufficient to negate a meeting if the minds, or whether it is viewed as judicial 'undoing' of the contract to prevent harm to a weaker party, the result is the same. For a discussion of these doctrines, which include unconscionability, inequality of bargaining power, contracts of adhesion, see e.g., Melvin A. Eisenberg, *The Limits of Cognition and the Limits of Contract*, 47 Stan. L. Rev. 211 (1995); Anthony Kronman, *Paternalism and the Law of Contracts*, 92 Yale L.J. 763 (1983).

[161] This expected increase in cognitive difficulties is a result of the fact that transactions which transfer personal data most often involve, at least at the initial point of data collection, an interaction between an unsophisticated individual and a sophisticated business entity. See *supra* note 16 (citing sources pointing to cognitive difficulties in assessing information privacy risks).

[162] It should be noted that this is somewhat of a simplification. There are really two licensing issues which impact on alienability: sublicensing and assignment. Sublicensing is more damaging from a privacy perspective because it results in the creation of multiple right-holders. Assignment, on the other hand, merely allows one right-holder to be substituted for another (as when a business is sold, etc.) As a general

generally oblige the sublicensee to abide by the same terms as the license imposes on the now sublicensor.[163] Licenses are also nonexclusive unless expressly provided otherwise.[164]

Trade secrecy law also provides some rights against third party uses of protected information.[165] If a third party has obtained the protected information from one whom the party knows or has reason to know got the information by improper means or in breach of confidence, the trade secret can be enforced against the third party.[166] If the third party got the information innocently, the firm seeking to protect the information may nevertheless be able to stop unauthorized use of the information after giving notice to the third party about its rightful claim to control uses of the information.[167]

Adopting modified trade secrecy licensing default rules for protecting personal data may also be less likely to interfere with or contribute to confusion in the law in respect of intellectual property rights and the First Amendment because it would focus on enforcing agreements and confidential relationships and monitoring acceptable commercial practices.[168] In addition, such an approach makes it unnecessary to engage in a quasi-religious war to resolve whether the nature of a person's interest in her personal data is a fundamental civil liberty or commodity interest.[169] A licensing approach to protecting personal data is consistent with the widespread use of licenses in the digital

---

matter, sublicensing of non-exclusive licenses is not permitted unless such permission is express: see, e.g., NOEL BYRNE, LICENSING TECHNOLOGY 210-211 (1998). On the issue of assignment, which may or may not be permissible, depending on the circumstances, see, e.g., Terry B. McDaniel, *Shop Rights, Rights In Copyrights, Supersession Of Prior Agreements, Modification Of Agreement, Right Of Assignment And Other Contracts*, 14 AIPLA Q.J. 35, 45-47 (1986) (discussing problems that could arise with trade secret protection due to non-assignable employee confidentiality agreements). In general, contracts which do not involve federally granted intellectual property rights are assignable as a matter of state law, except when the contract relies on the honesty, reputation, skill, character or ability of one of the parties: 4 Corbin § 866 (1951 & Supp. 1971). See also Green v. Camlin, 92 S.E.2d 125, 127 (S.C. Sup. Ct., 1956): "Rights arising out of a contract cannot be transferred if they are coupled with liabilities, or if they involve a relationship of personal credit and confidence" (in the context of a franchise agreement). See also RESTATEMENT (SECOND) OF CONTRACTS, §§ 317(2), 318(2) and 319(2).

[163] See, e.g., Byrne, *supra* note 162, at 210.

[164] *Id.* at 23.

[165] See, e.g., Uniform Trade Secrets Act, § 1(2).

[166] See, e.g., *id.*, § 1(2)(ii)(B).

[167] See, e.g., *id.*, § 1(2)(ii)(C). However, if an innocent third party has made substantial investments based on an understanding of its entitlement to use the information, courts may withhold injunctive relief and provide the trade secret claimant with a damages only remedy. *Id.* See also Pooley, *supra* note 143 at § 2.03[3][a] at 2-19. There are very few cases involving innocent third parties who thereafter receive notice-the author could find only one: see Forest Laboratories, Inc. v. Pillsbury Co., 452 F.2d 621 (C.A. 7th Cir. 1971).

[168] See discussion *supra* notes 81-90 and accompanying text regarding the constitutional problems with granting 'intellectual property-like' rights in personal data. A licensing regime would be less likely to interfere with the First Amendment than a property regime would because, unlike property rights, contract rights are not "good against the world." See, e.g., Robert P. Merges, *The End of Friction? Property Rights and Contract in the "Newtonian" World of Online Commerce*, 12 Berkeley Tech. L.J. 115, 118-27(1997). See also Cohen v. Cowles Media Co., 501 U.S. 663 (1991) (no First Amendment right to breach negotiated agreement not to disclose identity of news source). See also Kang, *supra* note 2, at 1277-82 (concluding that default rule providing protection to personal data would not conflict with the First Amendment).

[169] See discussion *supra* notes 93-103 and accompanying text.

networked environment.[170] If software and Internet companies have devised licenses to cover virtually every Internet transaction between them and their customers, it may seem only fair for the customers to start insisting on contractual terms that serve their interests as well.

It is also noteworthy that virtually all of the advantages offered in support of the property rights approach for the legal protection of personal data would be achievable through a licensing regime.[171] A licensing model would allow a market to exist in personal information insofar as individuals wished to participate in that market. New infomediary businesses could also arise under a licensing regime. Licensing also avoids the need for a government bureaucracy to regulate information privacy practices. Like the property model, the licensing model assumes that the marketplace can generally achieve workable outcomes.

There are obviously significant differences between trade secrets and personal information which may require each law to have different rules.[172] However, borrowing trade secrecy licensing default rules makes sense insofar as a person and a firm have agreed that the person will reveal nonpublic information to the firm in exchange for a stated sum and a willingness to restrict uses of the information to stated purposes. It also makes sense when a person reveals information to a firm in circumstances in which it is fair to infer that the information has been disclosed in confidence and for limited purposes. Borrowing from trade secrecy law's default rules may even make sense if one can articulate some means of obtaining personal data that the law should be considered improper. Consider, for example, the impropriety in getting personal data by engaging in unauthorized surveillance, by fraud, trickery, misrepresentation, or by hacking into a cryptographic envelope in which the data are being stored.[173] The law of information privacy, like the law of trade secrecy, could monitor commercial morality, adapt to changing circumstances, and at the same time accommodate the interests of individuals who are quite willing to reveal or allow uses of their personal information as long as they derive a benefit from it.

B. Developments That Might Cause Licensing To Emerge As a Viable Solution to Cyberspace Information Privacy Problems

Societal consensus about appropriate and inappropriate uses of personal information in cyberspace is forming in the United States, shaped in part by news coverage about

---

[170] See, e.g., Digital Dilemma, *supra* note 43, at ES 5-6.

[171] See *supra* Section II-A.

[172] For example, trade secrecy law aims to provide lead-time protection to induce appropriate levels of investment in industrial innovations. See, e.g., Reichman, *supra* note 44, at 2446-47. As a consequence, remedies for trade secrecy protection will often be limited to those necessary to restore adequate lead-time to the firm whose secret was misappropriated. See, e.g., Lamb-Weston, Inc. v. McCain Foods, Ltd., 941 F.2d 970 (9th Cir. 1991) (upholding eight-month injunction "'to eliminate commercial advantage that otherwise would be derived from the misappropriation'").

[173] See also Joseph Elford, *Trafficking in Stolen Information: A "Hierarchy of Rights" Approach to the Private Facts Tort*, 105 Yale L.J. 727 (1995) (arguing that use of improper means to obtain personal information ought to be illegal).

information privacy issues. Several times a week, major news stories about information privacy issues appear. One day the story may be about legislation forbidding states to sell drivers' license data as a commercial product.[174] Another day someone will have discovered that widely used software is sending surreptitious messages back to the firm when a user is playing a sound recording.[175] Yet another day will bring news that proposed legislation to deregulate the financial services industry will enable subsidiaries to share information about customers (which the industry claims will promote better service to customers and which privacy advocates say will bring harmful consequences, e.g., the denial of a person's application for a mortgage on the ground that the insurance data about him suggests he won't live long).[176] In view of the negative publicity that occurs when information privacy is not respected, major websites now worry about whether the information sharing they do is, in fact, fair or unfair.[177] This publicity has caused firms to back down very publicly when they have acted in a privacy-unfriendly way.[178] Internet companies know that an installed base of millions of users can quickly evaporate if customers don't trust the provider.

While fears of negative publicity is one inducement to attend to information privacy concerns, companies have realized that the news can be favorable as well, as when it publicizes private sector initiatives to further information privacy goals. The Online Privacy Alliance has been particularly active in taking a proactive stance on information privacy policy issues and getting the word out about its initiatives.[179] Industry commentators also frequently point out that information privacy is a key to building trust among consumers and trust is essential for the promise of e-commerce to be realized.[180]

---

[174] See, e.g., Bill Swindell, *House carries on over photo sales*, The Post and Courier: Charleston.Net, (February 26, 1999) <http://www.charleston.net/news/imagedata/house0226.htm>. On April 15, 1999, e.g., H.R. 1450 was introduced into the house. The "Personal Information Privacy Act of 1999" would prevent state departments of motor vehicles from transferring drivers' photos without permission. Congress passed the Driver's Privacy Protection Act of 1994, 18 U.S.C. sec. 2721(a), but several states have objected to it as an intrusion on state prerogatives under the 10th Amendment. See, e.g., Condon v. Reno, *supra* note 31. A discussion of the case can be found at: Linda Greenhouse, *States' Rights Adherents on Top Court Appear to Be Given Pause*, New York Times, November 11, 1999, <http://www.nytimes.com/library/politics/scotus/articles/111199states-rights.html>.

[175] See, e.g., Sara Robinson, *CD Software Is Said to Monitor Users' Listening Habits*, New York Times, (November 1, 1999) <http://www.nytimes.com/library/tech/99/11/biztech/articles/01real.html>.

[176] See, e.g., Jeri Clausing, Revised Banking Legislation Raises Concerns About Privacy, New York Times, (October 25, 1999) <http://www.nytimes.com/library/tech/99/10/biztech/articles/25priv.html>.

[177] See, e.g., David F. Gallagher, *Amazon Tries to Ease Privacy Worries*, New York Times, (August 30, 1999) <http://www.nytimes.com/library/tech/99/08/biztech/articles/30amaz.html>.

[178] See, e.g., Ted Bridis, *RealNetworks apologizes, fixes software to block tracking technology*, The Nando Times, (November 2, 1999) <http://www.techserver.com/noframes/story/0,2294,500052471-500086156-500289976-0,00.html>.

[179] See, e.g., Steve Lohr, *Online Industry Seizes the Initiative on Privacy*, N.Y. Times, (October 11, 1999) <http://www.nytimes.com/library/tech/99/10/biztech/articles/11priv.html>.

[180] See, e.g., Denise Caruso, *Consumers' Desire for Information Privacy Ignored*, N.Y. Times, (August 30, 1999) <http://www.nytimes.com/library/tech/99/08/biztech/articles/30digi.html>. See also Thomas P. Novak, Donna L. Hoffman and Marcos Peralta, *Building Consumer Trust in Online Environments: The Case for Information Privacy*, Working Paper of Vanderbilt University Project 2000, (December 1998) working paper available at <http://ecommerce.vanderbilt.edu/papers/CACM.privacy98/CACM.privacy98.htm> (also published in

In addition, American firms with substantial international market presence are becoming more attentive to information privacy practices and policies because of the need to comply with data protection rules in other jurisdictions.[181]

1. From Self-Regulation Norms to Licensing

"For e-commerce Web sites, having a privacy policy is no longer optional. Federal legislation, Federal Trade Commission (FTC) enforcement, the European Union Privacy Directive, economic coercion and consumer demand have all recently converged to create a new environment in which implementing a privacy policy is a business necessity for most and a legally advisable for all."[182]

To give content to "self-regulation," the Clinton Administration has endorsed privacy principles that it strongly recommends private sector firms should adopt as part of a self-regulatory strategy.[183] The FTC announced the following five pairs of principles as critical components of a true self-regulatory regime.[184]

a. Notice/Awareness
b. Choice/Consent
c. Access/Participation
d. Integrity/Security
e. Enforcement/Redress

In 1998 the FTC conducted a survey of more than 1400 commercial websites on privacy policy practices. The agency reported to Congress that a high proportion of such sites (92%) collected personal information from visitors to their sites, although nearly as substantial a proportion (86%) provided no notice about their information privacy policies. A year later, the FTC reported a substantial increase in the proportion of commercial websites that provided some notice about the sites' privacy policies.[185] Based on this progress, the FTC indicated that self-regulation should be given additional time to succeed.[186]

Communications of the ACM 1999); and SETH GODIN, PERMISSION MARKETING 163-65 (1999) (discussing the importance of customer privacy and consent-based data sharing in the online environment).

[181] See, e.g., Killingsworth, *supra* note 41, at 1. The need for private sector firms to adopt privacy policies and practices to comply with the EU Directive has also been recognized by the Clinton Administration which has been working on "safe harbor" guidelines. See Draft, International Safe Harbor Privacy Principles, Issued by the U.S. Department of Commerce, Nov. 15, 1999, available at http://www.ita.doc.gov/ecom/Principles 1199.htm.

[182] Killingsworth, *supra* note 41, at 1.

[183] See, e.g., IITF Principles, *supra* note 1.

[184] FTC Report, *supra* note 104, at 7- 14.

[185] Prepared Statement of the Federal Trade Commission Concerning "Self-Regulation and Privacy Online" Presented by Chairman Robert Pitofsky before the Subcommittee on Telecommunications, Trade, and Consumer Protection of the Committee on Commerce, United States House of Representatives, available at <http://www.ftc.gov/os/1999/9907/pt071399.htm>.

[186] *Id.* at 1-2.

While it is true that more online firms have privacy policies today, it is also true that if the FTC had judged the adequacy of privacy policies based on the criteria it set forth about what constitutes meaningful notice, the agency might have perceived less progress than it reported.[187] And if it judged progress based on private sector adherence to all five privacy principles, it might well have concluded that self-regulation had a very long ways to go. Nevertheless, there is some evidence that American-based commercial websites are providing more notice about privacy policies now than they did a year ago.[188] Some progress is also occurring in implementation of the other principles, in part because of well-publicized actions of major firms, such as IBM Corp., that have announced they will not place advertising with websites that do not meet certain privacy standards.[189]

Providing users with meaningful notice about what information a site is collecting about an individual and what the site intends to do with this data is definitely a step in the right direction. Notice alone, particularly one that is vague in content, may provide little basis for inferring that the site owner has bound itself to collect only these data and use the data only for stated purposes. However, misrepresentations in website privacy notices about the collection or use of personal data might be actionable.[190] In addition, the FTC has authority to monitor sites to ensure that they are not engaging in deceptive or other unfair trade practices with respect to personal data they collect.[191] And the FTC,

---

[187] See, e.g., *Hearing on S. 809: The Online Privacy Protection Act of 1999, Before the Subcommittee on Communications Committee on Commerce, Science and Transportation U.S. Senate* (July 27, 1999) (testimony of Marc Rotenberg, Director, Electronic Privacy Information Center) at 4-5, available at <http://www.epic.org/privacy/internet/EPIC_testimony_799.pdf>.

[188] See, e.g., *Georgetown Internet Privacy Policy Survey* ("GIPPS Report"), and the *Online Privacy Alliance Report on the Top 100 Web Sites*, both available at <http://www.msb.edu/faculty/culnanm/gippshome.html>.

[189] See, Jeri Clausing, *IBM Takes Stand for Consumer Privacy on Web*, New York Times, (April 1, 1999) <http://www.nytimes.com/library/tech/99/04/cyber/articles/01ibm-ad-column.html>.

[190] So, e.g., Real Networks had a privacy policy, but it didn't say that it was collecting data every time one used the software. See, e.g., *RealNetworks Is Target of Suit in California Over Privacy Issue*, New York Times, (November 9, 1999) <http://www.nytimes.com/library/tech/99/11/biztech/articles/09real.html>. There are several bills pending in Congress which would require web site owners to give consumers clear notice of the data being gathered and of the uses being made of that data: Online Privacy Protection Act of 1999, S. 809, 106th Cong. (requires notice); Internet Growth and Development Act of 1999, H.R. 1685, 106th Cong. § 301 (requires notice); and Consumer Internet Privacy Protection Act of 1999, H.R. 313, 106th Cong. (prohibits disclosure of personally identifiable information gathered online without consumer consent).

[191] See, e.g., In re Geocities, FTC Docket No. C-3489, Final Decision and Order (Feb. 12, 1999), available at http://www.ftc.gov/os/1999/9902/982015d&o.htm (finding deceptive practices in the collection of personal information from children deviating from stated privacy policy). The FTC power "to prevent persons ... from using unfair methods of competition ... and unfair or deceptive acts or practices in commerce." 15 U.S.C. § 45(a)(1). The legislative history of the FTC act reflects a disinclination to specify the unfair acts or practices because "there is no limit to human inventiveness in this field." H.R. REP. NO. 1142, 63d Cong., 2d Sess. 19 (1914). Before 1938, the FTC's jurisdiction was limited by the requirement that the FTC show specific injury to competitors. See, e.g., Federal Trade Comm'n v. Ralendam, 283 U.S. 643 (1931)), but Congress responded in 1938 with the Wheeler-Lea Amendment which added to the language of Section 5 a prohibition of "unfair or deceptive acts or practices." The announced purpose of the amendment was to overcome the limitation on jurisdiction imposed by the Supreme Court in the *Ralendam* decision, and to make the consumer injured by unfair trade practices of equal concern, under the law, with injured businesses. See Pep Boys--Manny, Moe & Jack, Inc. v. FTC, 122 F.2d 158, 161 (3d Cir. 1941)

among other agencies and groups, can be expected to press for greater adherence to the privacy principles over time.

As firms adhere more fully to the FTC privacy principles, it may enable the emergence of a contractual basis for holding firms to privacy representations. The more notice a website gives about what data will be collected and for what purposes, the more the site seek consent for collection and use of personal data, the greater the firm's representations about the integrity of its data and the security with which it maintains the data, and the more explicit a firm is about remedies available for failure to adhere to stated privacy policies, the more reasonable is an inference that firms have contracted with users about personal data practices. As one legal commentator has observed, "[a]s between the Web site owner and the user, a privacy policy bears all the earmarks of a contract, but perhaps one enforceable only by the user. It is no stretch to regard the policy as an offer to treat information in specified ways, inviting the user's acceptance by using the site or submitting the information. The Web site's promise is sufficient consideration to support a contractual obligation, as is the user's use of the site and submission of personal data."[192] The modified trade secrecy licensing default rule approach discussed above might supply some terms for such contracts.

The evolution of a licensing approach to personal data protection may be necessary because, unlike other fields in which self-regulation has been accepted,[193] there is no Internet e-commerce industry organization to serve as the overseer of self-regulatory practices to ensure that members of the organization are abiding by self-regulatory norms. Private sector firms are likely to prefer a licensing approach to having the government establish a new privacy bureaucracy. The more enlightened among private sector firms are coming to realize that fuller adherence to privacy principles will promote consumer trust which will, in turn, promote commerce. But providing consumer protection through implied or explicit licenses may ensure that self-regulation will work.

2. Promulgation of Uniform Computer Information Transactions Act

---

(stating that 1938 amendments intended to broaden FTC jurisdiction over business practices). Given this broad mandate, it would seem possible for the FTC to investigate and issue orders concerning commercial businesses that were practicing unfair or deceptive acts involving personal information dissemination. However, it is somewhat unclear if the FTC has power, for example, to order websites to post privacy policies. See, e.g., Tolliver, *supra* note 103, at 69 (discussing limits to the FTC's jurisdiction on information privacy issues).

[192] Killingsworth, *supra* note 41, at 12. This attorney recommended that Web site owners prepare explicit privacy licensing agreements, rather than allowing such agreements to be inferred from the existence of a privacy policy, so that the firm could include terms of choice, such as clauses requiring arbitration of disputes. *Id.* at 13.

[193] Securities dealers, for example, have formed nonprofit organizations to oversee and evolve self-regulatory activities in that business. Although some cyberspace privacy self-regulatory enforcement mechanisms do exist, such as the Truste privacy "seal" program, these have not proven particularly effective. See, e.g., Courtney Macavinta, *Truste Reports on RealNetworks as FTC Examines Net Privacy*, available at http://www.cnet.com/news.cnet.com/news/0-1005-200-1431844.html (reporting that Truste had taken no action against several firms that violated seal requirements).

A recent development that might have implications for the licensing of personal data is the promulgation of a model law, once known as Article 2B of the Uniform Commercial Code and now known as the Uniform Computer Information Transactions Act (UCITA).[194] The paradigmatic transaction of the Information Age is, in its view, that of licensing.[195] In July 1999, the National Conference of Commissioners of Uniform State Laws (NCCUSL) approved this model law for submission to state legislatures,[196] and it is already being considered for enactment by some states.[197] For a variety of reasons, this model law has been highly controversial.[198] UCITA could pave the way for a licensing regime for protecting personal information.[199]

In considering the possible implications of UCITA for personal data protection, it is appropriate to begin with the recognition that the personal data gathered in cyberspace falls within UCITA's rather open-ended definition of "computer information."[200] Interactive communications between and individual and a commercial website, moreover, would seem to constitute a "transaction."[201] Since the paradigmatic transaction of

---

[194] See the UNIFORM COMMERCIAL CODE Article 2B (February 1, 1999 proposed draft) available at <http://www.law.upenn.edu/bll/ulc/ucc2b/2b299.htm> (cited hereinafter as "UCC 2B"). The final version of UCITA, as passed at the 108th annual meeting of NCUSSL in Denver, Colorado, July 23-30, 1999 is available online at <http://www.law.upenn.edu/bll/ulc/ucita/cita10st.htm>. There were several reasons why why proposed this model law was removed from the UCC and promulgated as a stand-alone model law. For one thing, the licensing paradigm did not fit well with the sales of goods transactions covered by UCC Article 2, and the UCC is normally reserved for codification of well-established commercial practices - which practices have not developed in the area of information transactions. The American Law Institute (ALI) also had significant reservations about UCC 2B which might have made it difficult for this model law to become part of the U.C.C. See Joint Press Release by ALI and NCCUSL, *NCCUSL to Promulgate Freestanding Uniform Computer Information Transactions Act*, (April 7, 1999) stated only that: "it has become apparent that this area does not presently allow the sort of codification that is represented by the Uniform Commercial Code," available at <http://www.2bguide.com/docs/040799pr.html>.

[195] See, e.g., Raymond T. Nimmer, *Breaking Barriers: The Relation Between Contract and Intellectual Property Law*, 13 Berkeley Tech. L.J. 827, 829 (1998).

[196] See, e.g., Brenda Sandburg, *E-commerce Plan Faces Tough Fight*, Cal Law, (August 4, 1999) available at <http://www.callaw.com/stories/edt0804e.html>.

[197] The Joint Committee on Science and Technology (JCOTS) of the Virginia General Assembly is currently considering UCITA, but has not yet drafted a bill because of the 'controversial' nature of UCITA: see *Letter from John S. Jung, Staff Attorney, JCOTS, to Members of Advisory Committee #5*, (October 27, 1999) available at <http://legis.state.va.us/jcots/agendas/99-11-04_AC5-format.htm>. JCOTS will continue its consideration of UCITA at its meeting on December 7, 1999. Meeting schedules are available at <http://legis.state.va.us/jcots/meetings.htm>.

[198] See, e.g., Symposium, *Intellectual Property and Contract Law in the Information Age: The Impact of Article 2B of the Uniform Commercial Code on the Future of Transactions in Information and Electronic Commerce*, 13 BERKELEY TECH. L.J. 809 (1998) and 87 CALIF. L. REV. 1 (1999).

[199] See, e.g., Lorin Brennan, *The Public Policy of Information Licensing*, 36 Hous. L. Rev. 61, 111 (1999) (anticipating the use of UCITA in consumer licensing of personal data to private sector firms); Martin, *supra* note 11, at 849 n. 344. See also Pamela Samuelson, *A New Kind of Privacy? Regulating Uses of Personal Data In the Global Information Economy*, 87 Calif. L. Rev. 751, 776 (1999) (expressing doubts about suitability of UCITA for information privacy protection).

[200] UCITA § 102(a)(10): "'Computer information' means information in electronic form which is obtained from or through the use of a computer or which is in a form capable of being processed by a computer. The term includes a copy of the information and any documentation or packaging associated with the copy."

[201] UCITA § 102(a)(11): "'Computer information transaction' means an agreement or the performance of it to create, modify, transfer, or license computer information or informational rights in computer information. The term includes a support agreement under Section 612. The term does not include a

UCITA is a license, transactions between an individual and a commercial website may be among the transactions which UCITA could govern.[202]

For a license in computer information to be enforceable under UCITA, a prospective licensee of personal data (in this case, the website owner) must manifest assent, through conduct or otherwise, to the terms of a license after an opportunity to review the terms and conditions of the license.[203] A potential problem with using UCITA to protect personal information in cyberspace is that individuals today do not generally articulate terms and conditions to which the site must agree before the individuals will supply the site with personal data; nor do they present such a license to site owners for their review before using the site.[204] Site owners could conclude from the absence of proffered terms that whatever information individuals might provide to the site, wittingly or unwittingly, is being provided without license restrictions.[205]

However, it may be possible to establish restrictive licensing terms for personal data by looking to the prospective licensee's privacy policy as a statement of that party's willingness to restrict its uses of personal data. After all, UCITA does not require restrictive license terms to be set by the licensor; all it requires is a manifestation of assent to restrictive terms. If users assent to the licensee's privacy policy restrictions by supplying information to the site or using it otherwise in accordance with the site's terms, a license agreement subject to these restrictions might be formed.[206] This license might then be supplemented with the modified trade secrecy licensing default rules proposed

---

transaction merely because the parties' agreement provides that their communications about the transaction will be in the form of computer information."

[202] It is somewhat unclear under UCITA whether someone needs to have a legally protectable interest in information, in order to be entitled to license it. See UCITA § 102(a)(38): "'Informational rights' include all rights in information created under laws governing patents, copyrights, mask works, trade secrets, trademarks, publicity rights, or any other law that gives a person, independently of contract, a right to control or preclude another person's use of or access to the information on the basis of the rights holder's interest in the information." For a criticism about UCITA's failure to be clear on this issue, see, e.g., Jessica Litman, *The Tales that Article 2B Tells*, 13 BERKELEY TECH. L.J. 931 (1998), discussing the confusion in UCC 2B over the nature of the rights an information licensor might have in information other than those supplied by intellectual property law. If the law confers on individuals a legally protectable interest in personal data, these would seem to be "informational rights" that UCITA would cover. It is not, however, at all clear that under existing law, individuals can reasonably be said to have such rights in personal data. See *supra* notes 24-32 and accompanying text. But if they did, or if the law came to recognize that they did, such rights would seem to be licensable under UCITA.

[203] See UCITA § 112.

[204] But see *infra* notes 217-223 and accompanying text (discussing how the technological infrastructure might evolve to enable consumers to offer terms for use and disclosure of personal data).

[205] UCITA does, of course, provide an array of default rules to fill in missing terms. See, e.g., UCITA §§ 307 and 308. Some of these, such as its narrow implied right provision, might bode well for protecting personal data. See, e.g., UCITA, §§ 307(a) and (b). But see Jane C. Ginsburg, *Authors as "Licensors" of "Informational Rights" Under U.C.C. Article 2B*, 13 Berkeley Tech. L.J. 945, 954-965 (1998) (reporting that the narrow implied rights provision of Article 2B might be good news for writers, but anticipating that publishers would respond to this model law by developing elaborate contracts to protect their interests to which they'd insist authors agree).

[206] See *supra* notes 203-205 and accompanying text.

above to which site owners and the individuals would agree unless expressly agreed otherwise.[207]

Future developments may also aid in the development of restrictive personal data licenses for cyberspace transactions. Consumer protection organizations could, for example, draft standard form restrictive licensing agreements for individuals to use to protect their privacy interests when dealing with websites.[208] Given the current technical infrastructure of the web, individual users may not be in a position to present their standard form contracts to the site owner in a meaningful way. However, the technical infrastructure of the web may in time allow automated negotiations of privacy licenses that will restrict uses that can be made of personal data (a matter to be considered in the next subsection).[209]

While much more could be said about the pros and cons of utilizing UCITA for personal data protection, there is some reason to question whether UCITA will be useful in achieving information privacy goals. UCITA was, after all, drafted with very different kinds of licensing transactions in mind. From the outset, the core subject matter of the UCITA/Article 2B project has been computer programs.[210] Some years ago, the subject matter of this model law was expanded to cover virtually transactions in information.[211] After several major information industries objected to this scope for the law, in large part because the assumptions and default rules of UCITA/Article 2B did not match well with the licensing practices of those industries,[212] the drafters eventually contracted the scope of the model law to computer information.[213] Even with this contracted scope, major

---

[207] Consider also that websites set their own terms and conditions for use of their sites. Under UCITA, individual users could be said to have "assented" to such terms and conditions, either by clicking here "I agree" or by continuing to use the site after having an opportunity (which they will typically not take up) to examine the site's terms and conditions. Even a cursory review of the terms of service at commonly visited websites reveals how one-sided they typically are (e.g., disclaiming warranty and other responsibilities on the part of the site owner and imposing responsibilities on users). See, e.g., *Yahoo GeoCities Terms of Service*, available at <http://docs.yahoo.com/info/terms/geoterms.html>. Given this, it might be reasonable to expect that if UCITA becomes the law, site owners will add to existing terms of service a waiver of their responsibilities toward personal data that users reveal at the site or a broad release of informational rights. See UCITA § 208. If this occurs, it would constitute a step backwards for information privacy, not a step forward.

[208] Consumer Reports Online currently makes 'e-Ratings', which include an evaluation of online merchants' privacy and security policies, available to its subscribers <http://www.consumerreports.org/Special/Samples/Reports/9910etip.htm>. Such activities could be expanded to include drafting of model licensing agreements.

[209] See *infra* notes 217-228 and accompanying text.

[210] See, e.g., Robert Gomulkiewicz, *The License is the Product: Comments on the Promise of Article 2B for Software and Information Licensing*, 13 BERKELEY TECH. L.J. 891, 894 (1998).

[211] Compare, e.g., UNIFORM COMMERCIAL CODE Article 2B (December 1, 1995 proposed draft) with UNIFORM COMMERCIAL CODE Article 2B (February 2, 1996 proposed draft). Both are available at <http://www.2bguide.com/drafts.html>. A rationale for the expansion of scope can be found in: *Notes on the February 1, 1996 Draft* available at <http://www.lawlib.uh.edu/ucc2b/febnotes.html>.

[212] See, e.g., *Letter from MPAA, RIAA, NAA, NAB, NCTA and MPA to NCCUSL*, December 7, 1998 available at <http://www.2bguide.com/docs/1298mpaa.html> (voicing opposition to scope and enactment of UCC 2B).

[213] See the *Report on the November 13 - 15, 1998 Drafting Committee Meeting*, available at <http://www.2bguide.com/nov98rpt.html>.

information industries continue to oppose UCITA in part because of the "software-centric" nature of its rules.[214] If these industries are correct in thinking that UCITA is not suitable for the licensing of such computer information products as computer-processable motion pictures or newspapers, it seems likely that UCITA would be suitable for protecting personal data. After all, the commercial goals of the motion picture and news industries would seem to be much closer to those of the software industry than to the licensing of personal data. In view of this, it may be naïve to think UCITA would provide a workable framework for achieving information privacy goals.

Still, some believe that UCITA provides a licensing regime capable of providing individuals with somewhat greater protection in transactions involving their personal data than they might otherwise have.[215] To counteract concerns about potential disparities in bargaining power of commercial website owners and individuals about personal data matters, it might be worth considering an adaptation of proposals made by Reichman and Franklin for public-interest unconscionability default rules to achieve a better balance in non-negotiated UCITA transactions.[216] Although Reichman and Franklin may have had other public interests in mind, the concept of public interest unconscionability default rules for licensing of personal data may provide a way to achieve information privacy goals.

3. Privacy-Enhancing Technologies

A number of privacy-enhancing technologies (PETs) have been developed in recent years which are capable of masking personal identity in cyberspace in order to achieve information privacy goals.[217] There is substantial appeal in the idea of a technological solution to a problem that technology itself seems to have created, in part because such technologies are self-enforcing and appear to reduce the need for regulatory interventions.[218]

One commentator has differentiated among four types of PETs: (1) subject-oriented PETs (those aiming to limit the ability of others to discern the identity of a particular person, e.g., an anonymizing browser); (2) object-oriented PETs (those aiming to protect identity through the use of a particular technology, e.g., anonymous e-cash); (3) transaction-oriented PETs (those aiming to protect transactional data, e.g., automated systems for destroying transactional data); and (4) system-oriented PETs (those aiming to create "zones of interaction where the identity of the subjects is [] hidden, where the

[214] See, e.g., *Letter from MPAA, RIAA, NAA, NAB, NCTA and MPA to NCCUSL*, May 10, 1999 available at <http://www.2bguide.com/docs/coalit5.html> (voicing continued opposition to UCITA).
[215] See *supra* note 199.
[216] See J.H. Reichman & Jonathan A. Franklin, *Privately Legislated Intellectual Property Rights: Reconciling Freedom of Contract With Public Good Uses of Information*, 147 U. Penn. L. Rev. 875 (1999).
[217] See, e.g., Burkert, *supra* note 4, at 125-142. See also Ian Goldberg, David Wagner, & Eric Brewer, *Privacy-Enhancing Technologies for the Internet*, http://www.cs.berkeley.edu/~daw/privacy-compcon97-www/privacy-html.html.
[218] Philip Agre, Introduction, in TECHNOLOGY & PRIVACY, *supra* note 5, at 7.

objects bear no traces of those handling them, and where no record of the transaction is created or maintained," e.g., anonymous remailer systems).[219]

To these might be added a fifth category of PETs capable of being programmed to interact with websites about the privacy preferences of individuals potentially interested in visiting the sites. One well-publicized example is the Platform for Privacy Preferences (P3P) effort underway at the World Wide Web Consortium.[220] Some expect electronic agents to be programmed to negotiate privacy and other user-preferred terms of contracts in cyberspace.[221]

If P3P's designers achieve the project's objectives, P3P would enable individuals to program their browsers to identify classes of information that they are willing and unwilling to disclose (e.g., yes to zip code, but no to street address) to website owners.[222] Individuals would then not have to haggle over terms and conditions with every site they visit. Instead, their browsers could be set to avoid sites that do not comport with the individuals' privacy preferences.[223] The prospect of having fewer people visiting one's site if one's privacy policy does not comport with common user preferences may create significant commercial pressure for firms to offer more consumer-friendly privacy policies.

As promising as P3P and other PETs technologies may be,[224] it is fair to say that they have yet to prove their worth in achieving information privacy goals except in limited

---

[219] Burkert, *supra* note 4, at 125-128. An example of the latter is considered in Bernardo A. Huberman, Matt Franklin, and Tag Hogg, *Enhancing Privacy and Trust in Electronic Communication*, April 29, 1999 (on file with author) (aiming to "facilitate finding shared preferences, discovering communities with shared values, removing disincentives posed by liabilities, and negotiating on behalf of a group" by adapting cryptographic techniques).

[220] See, e.g., Reagle & Cranor, *supra* note 53.

[221] The prospects for electronic agent technology for engaging in electronic commerce are explored in, e.g., Pattie Maes, Robert H. Guttman, Alexandros G. Moukas, *Agents That Buy and Sell*, 42 Comm. ACM 81 (March 1999). See also Brennan, *supra* note 199, at 109-14 (discussing the use of electronic agents to contract in cyberspace on privacy terms); and *A Killer App for Computer Chat*, THE ECONOMIST, April 10, 1999 at 79, 80 (bots can be programmed to ask about a web sites' privacy policies). UCITA validates contracts made by electronic agents. See UCITA at §§ 107, 112 and 206. Some speak of P3P as though it will serve as an electronic agent negotiating privacy terms. See, e.g., Chris Oakes, *The Trouble With P3P*, Wired News, June 25, 1999, at 1.

[222] See Reagle & Cranor, *supra* note 53. See also Harvard Developments, *supra* note 33, at (expressing enthusiasm for P3P as a means to protect information privacy). Privacy advocate Marc Rotenberg is skeptical about how useful P3P will be in the protection of personal data. See, e.g., Testimony and Statement for the Record of Marc Rotenberg on Privacy in Electronic Communications, March 26, 1998, at 7 ("P3P…wont' by itself protect anybody's privacy. That's because the technology isn't really designed to prevent websites from gathering information about a Web user, but rather to convey personal information explicitly from the Web user to the Web site as long as the Web site promises to abide by certain privacy policies…P3P lacks both auditing and enforcement measures."). See also Oakes, *supra* note 221, at 2 (explaining difficulties for humans in adequately programming browsers with P3P instructions); and Karen Coyle, *P3P: Pretty Poor Privacy? A Social Analysis of the Platform for Privacy Preferences*, (June, 1999) available at <http://www.kcoyle.net/p3p.html> (P3P cannot adequately protect privacy because it is designed to facilitate the gathering of data by web sites).

[223] Reagle & Cranor, *supra* note 53.

[224] See, e.g., Harvard Developments, *supra* note 33, at 1645-46

circumstances.[225] Other presenters at this symposium are better able than I to assess the likelihood that such technologies will provide greater privacy protection over time.[226] However, it is unlikely that technology alone can solve the problem.

As Professor Burkert has observed, "the main task [of] social scientists, lawyers, regulators, and privacy practitioners [is] to accept the challenge of information and communication technologies as a challenge for social innovation."[227] Information privacy is a social goal, not a technological one. To achieve information privacy goals will require social innovations, including the formation of new norms and perhaps new legal rules to establish boundary lines between acceptable and unacceptable uses of personal data. It may be easier for information technologists to embody such norms and legal rules in code after society has configured what those rules should be, and they will surely have greater incentives to do so if the law requires it.[228]

III. Conclusion

Europeans have realized that it is not just an information infrastructure we are in the process of constructing, but an information society.[229] They have identified information privacy as a fundamental value that should be a keystone of the architecture for achieving an information society in which people will want to live.[230] In addition, they have demonstrated that political will can be found to utilize the law to ward off Scott McNealy's vision for the information society ("you've got zero privacy now—get over it"[231]). In these insights may lie some useful lessons for Americans who also value information privacy.[232]

---

[225] Some e-cash systems have been implemented with anonymizing features. However, not all e-cash systems have this feature: see, e.g., Bruno Giussani, *Feeding the Meter - With a Pocketful of Micropayments*, New York Times, August 19, 1997, available at <http://www.nytimes.com/library/cyber/euro/081997euro.html>. See generally A. Michael Froomkin, *Flood Control on the Information Ocean: Living With Anonymity, Digital Cash, and Distributed Databases*, 13 J. Law & Comm. (1994) (discussing technical and policy reasons for doubting technology will protect privacy).

[226] See, e.g., Philip E. Agre, [title of symposium paper]; A. Michael Froomkin, [title of symposium paper].

[227] Burkert, *supra* note 4, at 140.

[228] See, e.g., Rudiger Grimm, Nils Lohndorf, & Philip Scholz, *Data Protection in Teleservices (The DASIT Project)* (on file with the author) (describing research project on uses of technology to implement the EU Directive in telecommunications services); Ridiger Grim, *User Control Over Personal Web Data*, EEMA Teletrust: ISSE '99, Berlin, Oct. 1999 (forthcoming 1999)(discussing technical means of implementing German data protection rules).

[229] Compare THE NATIONAL INFORMATION INFRASTRUCTURE: AN AGENDA FOR ACTION, available at http://www.iitf.gov/ with EUROPE AND THE GLOBAL INFORMATION SOCIETY: RECOMMENDATIONS TO THE EUROPEAN COUNCIL, available at http://www2.echo.lu/eudocs/en/bangemann.html.

[230] See, e.g., EU Directive, *supra* note 14, Art. 1.1.

[231] This rather infamous quote has been reported in various places. See, e.g., Robert Lemos, *The dark side of the digital home*, ZDNet, (February 7, 1999) <http://www.zdnet.com/zdnn/stories/news/0,4586,2203898,00.html>.

[232] See, e.g., Kang, *supra* note 2, at 1196-97 (citing polls about privacy concerns).

Myriad reasons explain why the U.S. response to the challenges of information privacy for an information society has been so much slower, more erratic, and less comprehensive than in the E.U. [233] Among them are certainly considerable differences in the regulatory cultures of the U.S. and the E.U., as well as dissimilar attitudes toward the private sector and toward technology.[234] However, a serious impediment to a comprehensive approach in the U.S. is the lack of clarity in this country about the nature of the interest that individuals have in information about themselves (e.g., is it a commodity interest, a consumer protection interest, a personal dignity interest, a civil right interest, all of the above, or no interest at all?).[235] One of the strengths of the EU Directive is that the regulatory regime it embodies is consistent with its underlying conception of information privacy as a fundamental human right. Without a coherent conception about the nature of a person's interest in personal data, it is difficult to design a legal regime to protect this interest appropriately.

One of the virtues of the property rights approach to protecting personal data discussed in Section II is that it would seem to solve the nature-of-the-interest problem which, in turn, should simplify the task of constructing a legal regime to protect the interest. However, as Section II has shown, a serious mismatch exists between the traditional rationale for granting property protection to an information resource and the rationale for granting individuals property rights in personal data.[236] Also mismatched are traditional policies of property law favoring free alienability and information privacy policy preferences for restrictions on alienation.[237] If the goals and mechanisms of property law are misaligned with information privacy policy objectives, protecting privacy as intellectual property simply may not work.

Even though a one-dimensional conception of a person's interest in her information makes crafting a legal regime easier, in truth, individuals may not have just one interest in personal information, but many interests. Sometimes a person's interest in personal data is a civil liberties interest (e.g., not being forced to disclose whether I am a member of the NAACP[238]), and sometimes it's not (e.g., Amazon.com sending me email to let me know that an author whose books I've bought before has just released a new novel).

---

[233] One impediment to the development of American information privacy law has been its unduly heavy focus on "reasonable expectations of privacy." See, e.g., Schwartz & Reidenberg, *supra* note 24, at 60-73. This has two serious drawbacks. First, it largely excludes consideration of normative purposes for limiting the collection and use of personal data, thereby undermining society's ability to evolve norms and rules to regulate these matters because it tends to make the law concerned about places, not people. See, e.g., Olmstead v. United States, 277 U.S. 439 (1928). This case is discussed in: Lawrence Lessig, *Reading The Constitution In Cyberspace*, 45 EMORY L.J. 869, 872-875 (1996). Second, it is conducive to an ongoing erosion of privacy. The more intrusive surveillance technology becomes, the less reasonable is any expectation that individuals will have privacy, and as a consequence, the less privacy the law will recognize. Schwartz & Reidenberg, *supra* note 24, at 64.

[234] See, e.g., Swire & Litan, *supra* note 10, at 153-59.

[235] The lack of consensus about the nature of a person's interest in personal data may help to explain the wide range of solutions to the information privacy problem that legal commentators have proposed.

[236] See *supra* notes 70-80 and accompanying text.

[237] See *supra* notes 68-69 and accompanying text.

[238] See NAACP v. Alabama, 357 U.S. 449 (1958) (state interfered with First Amendment interests in requiring disclosure of membership).

Sometimes it is a commodity interest (e.g., I can get a discount if I disclose my zipcode) and sometimes it's not (e.g., I don't want software on my hard drive to surveill what other software I have installed there and report on this to its home base). Sometimes it's a dignity interest (e.g., whether I sweat profusely) and sometimes it's not (e.g., whether my eyes are blue).

The task of devising a workable legal framework for regulating private sector uses of personal data is obviously more difficult if one takes a multi-dimensional perspective on the nature of a person's interest in personal data. Yet it is an advance to recognize that a person has more than one kind of interest in personal information. It is also an advance to realize that the propriety of collecting or processing personal data depends in part on context.[239] For my doctor to send information about my medical condition to an insurance company so that it will cover the costs of treatment is appropriate, but for the doctor to give the same information to a prospective employer is inappropriate. It further advances understanding to realize that a major factor in a contextual analysis about uses of personal information is whether the person whose data is being collected or processed knows or has reason to know that the data are being collected and what uses will be made of them.[240] In addition, it may be important to realize that our concept of information privacy, and in particular, our understanding of what is appropriate and inappropriate to do with personal information, is evolving over time.[241]

One of the virtues of a contractual approach to protecting information privacy is that it can accommodate the multiple interests people have in personal information, the contextual nature of determinations about the appropriateness of collection or use of personal data, the significance of consent as a factor in determining appropriate uses, and the evolutionary nature of social understanding about information privacy. It is a flexible, adaptable, market-oriented way to allow individuals to control uses of personal data. Oddly enough, it may more easily be achieved in cyberspace than in meatspace because a website's privacy policy can become the basis of a contractual understanding between the user and the website.[242] Although individuals and website owners may sometimes reach express agreement on all relevant issues pertaining to allowable uses of personal data, a set of default licensing rules adapted from trade secrecy law might "fill in the gaps" of such agreement (e.g., restricting rights to sublicense the data to others if the privacy policy is silent on this issue). Despite obvious differences between trade secrecy and information privacy, there are some significant parallels in the objectives of trade secret law and the information privacy law envisioned in this article: protecting commodity and non-commodity interests of persons in restricting others' uses of certain information; protecting information disclosed in confidence; protecting information against the use of improper means to obtain it; facilitating commercial transactions

[239] See, e.g., Samarjiva, *supra* note 5, at 283 ("privacy is situational and relationship-specific").
[240] See, e.g., *id*. (emphasizing the importance of consent). For my doctor to test my blood to see if I have HIV when I have not agreed to this is, for example, inappropriate (unless, of course, the law has required the doctor to do so).
[241] See, e.g., Schauer, *supra* note 18, at 557 ("[T]he standard rhetoric of Internet privacy challenges ironically understates the Internet revolution because it does not acknowledge the way in which the Internet and related technologies have changed the concept of privacy itself.")
[242] See *supra* notes 190-192 and accompanying text.

allowing the holder of the interest to negotiate compensation for allowing uses of information; enforcing agreements about nondisclosure or limited use; and establishing minimum standards of commercial morality that can evolve over time.

Americans may want information privacy, but they also want a strong information economy. They appear to be willing to balance their interests in keeping certain information about themselves private with their interests in getting access to customized information and services that disclosure of their personal data may enable firms to provide.[243] If information privacy goals can be achieved without establishing a new government bureaucracy, as a modified licensing regime should allow, Americans objectives for an information society may more fully be realized.

[243] See *supra* note 46 and accompanying text.