PROPERTY, PRIVACY, AND PERSONAL DATA

*Paul M. Schwartz**

Modern computing technologies and the Internet have generated the capacity to gather, manipulate, and share massive quantities of data; this capacity, in turn, has spawned a booming trade in personal information. Even as it promises new avenues for the creation of wealth, this controversial new market also raises significant concerns for individual privacy — consumers and citizens are often unaware of, or unable to evaluate, the increasingly sophisticated methods devised to collect information about them. This Article develops a model of propertized personal information that responds to these serious concerns about privacy. It begins this task with a description and an analysis of several emerging technologies that illustrate both the promise and peril of the commodification of personal data. This Article also evaluates the arguments for and against a market in personal data, and concludes that while free alienability arguments are insufficient to justify unregulated trade in personal information, concerns about market failure and the public's interest in a protected "privacy commons" are equally insufficient to justify a ban on the trade. This Article develops the five critical elements of a model for propertized personal information that would help fashion a market that would respect individual privacy and help maintain a democratic order. These five elements are: limitations on an individual's right to alienate personal information; default rules that force disclosure of the terms of trade; a right of exit for participants in the market; the establishment of damages to deter market abuses; and institutions to police the personal information market and punish privacy violations. Finally, this Article returns to examples of technologies already employed in data trade and discusses how this proposed model would apply to them.

INTRODUCTION

Personal information is an important currency in the new millennium. The monetary value of personal data is large and still growing, and corporate America is moving quickly to profit from this trend.[1] Companies view this information as a corporate asset and have invested heavily in software that facilitates the collection of con-

---

* Professor of Law, Brooklyn Law School. For their helpful comments on this Article, I would like to thank Ian Ayres, Johann Bizer, Chris Hoofnagle, Ted Janger, Beryl Jones, Jerry Kang, Lance Liebman, Michael Madow, William McGeveran, Dana Brakman Reiser, Spiros Simitis, Daniel Solove, and Bill Treanor. A grant from the Dean's Scholarship Fund of Brooklyn Law School supported this work. I am grateful to Dean Joan Wexler for this support and her interest in this project. While working on this Article, I also benefitted from the sponsorship of the American Academy in Berlin (Fall 2002) and the German Marshall Fund and its Transatlantic Center in Brussels (Spring 2003). My thanks to Gary Smith of the American Academy and Bill Antholis and William Drodziak of the German Marshall Fund for providing stimulating and collegial environments for scholarship.

[1] As a single indication of the value of these data, one CEO has estimated that consumer marketers digest $75 billion of personal information each year. Jennifer Sullivan & Christopher Jones, *How Much Is Your Playlist Worth?*, WIRED NEWS (Nov. 3, 1999), *at* http://www.wired.com/news/technology/0,1282,32258,00.html.

sumer information.[2] Moreover, a strong conception of personal data as a commodity is emerging in the United States, and individual Americans are already participating in the commodification of their personal data.[3]

Once personal data become a commodity, questions arise regarding the necessity, if any, of legal limits on data trade. Legal scholars interested in protecting information privacy, however, have been suspicious of treating personal data as a form of property and have generally advocated imposing a ban on data trade, rather than restrictions on transferability.[4] In contrast, other legal scholars have advocated propertization of personal information, albeit generally without sufficient sensitivity to privacy concerns. As a result, such scholars usually see no need for legal limits on data trade[5] — that is, no need for "inalienabilities," which, in Susan Rose-Ackerman's succinct definition, are

---

[2] For a general discussion of the importance to corporations of customer information in the information economy, see CARL SHAPIRO & HAL R. VARIAN, INFORMATION RULES: A STRATEGIC GUIDE TO THE NETWORK ECONOMY 33–37 (1999). Regarding corporations' belief in their ownership of consumer data, see Bob Tedeschi, *E-Commerce Report*, N.Y. TIMES, Nov. 8, 1999, at C16. In contrast, two consultants to interactive media companies have argued that companies will be better served, in light of the privacy concerns of consumers, "to acknowledge that users themselves are the rightful owners of their own usage and transaction information." JOHN HAGEL III & ARTHUR G. ARMSTRONG, NET GAIN: EXPANDING MARKETS THROUGH VIRTUAL COMMUNITIES 106 (1997).

[3] *See, e.g.*, LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 142–63 (1999) (advocating the use of property rights to protect privacy on the Internet); Simon G. Davies, *Re-Engineering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity*, *in* TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE 143, 160–61 (Philip E. Agre & Marc Rotenberg eds., 1997) [hereinafter TECHNOLOGY & PRIVACY] (discussing processes by which personal information becomes a commodity). For a discussion of case studies involving different degrees of commodification of personal data, see *infra* section I.A.

[4] For a sampling of the views of those opposed to propertization of personal information, see Anita L. Allen, *Coercing Privacy*, 40 WM. & MARY L. REV. 723, 750–57 (1999); Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1423–28 (2000); Davies, *supra* note 3, at 160; Mark A. Lemley, *Private Property: A Comment on Professor Samuelson's Contribution*, 52 STAN. L. REV. 1545, 1551 (2000); Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)*, 2001 STAN. TECH. L. REV. 1, ¶¶ 92–97, http://stlr.stanford.edu/STLR/Articles/01_STLR_1/article_pdf.pdf; and Pamela Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L. REV. 1125, 1143 (2000).

[5] For a sampling of the views of advocates of propertization, see LESSIG, *supra* note 3, at 143–63; Patricia Mell, *Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness*, 11 BERKELEY TECH. L.J. 1, 26–41 (1996); Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 GEO. L.J. 2381, 2385 (1996); *Developments in the Law—The Law of Cyberspace*, 112 HARV. L. REV. 1574, 1634–49 (1999); and Kenneth C. Laudon, *Markets and Privacy*, COMMUNICATIONS OF THE ACM, Sept. 1996, at 92. For an op-ed adopting a market-based approach to privacy, see Thomas G. Donlan, *Freedom of Information: The Right to Privacy Must Be Maintained by Private Effort*, BARRON'S, June 21, 1999, at 62, 1999 WL-BARRONS 19353447.

For critical responses to Lessig's approach to propertization of personal information, see Rotenberg, *supra* note 4; and Paul M. Schwartz, *Beyond Lessig's* Code *for Internet Privacy: Cyberspace Filters, Privacy Control, and Fair Information Practices*, 2000 WIS. L. REV. 743, 744.

"any restriction[s] on the transferability, ownership or use of an entitlement."[6] This Article seeks to develop a model for propertization of personal data that will fully safeguard information privacy.

Because this Article focuses on two notoriously slippery terms — property and information privacy — some basic definitions are in order. First, this Article defines property as any interest in an object, whether tangible or intangible, that is enforceable against the world.[7] From this perspective, property rights run with the object, and can be contrasted with contract rights, which bind only parties in privity.[8] Second, this Article conceives of information privacy as the result of legal restrictions and other conditions, such as social norms, that govern the use, transfer, and processing of personal data.[9] Information privacy can, therefore, be distinguished from "decisional privacy," which, for example, was at stake in the Supreme Court's decision in *Roe v. Wade*.[10] The focus of decisional privacy is on freedom from interference when one makes certain fundamental decisions, including those concerning reproduction and child-rearing.[11] In contrast, information privacy is concerned with the use, transfer, and processing of the personal data generated in daily life. Decisional and information privacy are not unrelated; the use, transfer, or processing of personal data by public and private sector organizations will affect the choices that we make. This link becomes explicit, for example, when courts in decisional privacy cases concerning access to abortions evaluate the impact on reproductive choice of state laws that require hospitals or

---

[6] Susan Rose-Ackerman, *Inalienability and the Theory of Property Rights*, 85 COLUM. L. REV. 931, 931 (1985).

[7] Henry Hansmann & Reinier Kraakman, *Property, Contract, and Verification: The* Numerus Clausus *Problem and the Divisibility of Rights*, 31 J. LEGAL STUD. S373, S374 (2002). For a contrasting definition of property that stresses the limited forms that property can take, see Thomas W. Merrill & Henry E. Smith, *Optimal Standardization in the Law of Property: The* Numerus Clausus *Principle*, 110 YALE L.J. 1 (2000).

[8] Hansmann & Kraakman, *supra* note 7, at S374.

[9] *See* Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609 (1999); *see also* Robert C. Post, *The Social Foundations of Privacy: Community and the Self in the Common Law Tort*, 77 CAL. L. REV. 957, 1009–10 (1989). For an overview of privacy law in the United States, see PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW 5–17 (1996); and DANIEL J. SOLOVE & MARC ROTENBERG, INFORMATION PRIVACY LAW (2003).

[10] 410 U.S. 113 (1973). Decisional privacy has also been the subject of numerous law review articles and books. *See, e.g.*, DAVID RICHARDS, TOLERATION AND THE CONSTITUTION 243–44 (1986); John Hart Ely, *The Wages of Crying Wolf: A Comment on* Roe v. Wade, 82 YALE L.J. 920 (1973); Jed Rubenfeld, *The Right of Privacy*, 102 HARV. L. REV. 737 (1989).

[11] One can also identify a third kind of privacy: physical privacy, or the ability to be undisturbed at home. This kind of privacy turns out to be a key concern for Ian Ayres and Matthew Funk in their proposal to regulate telemarking. *See* Ian Ayres & Matthew Funk, *Marketing Privacy*, 20 YALE J. ON REG. 77 (2003).

physicians to disclose certain data or keep certain records.[12] This Article explores the connection between the processing of personal information and decisionmaking; it examines how access to personal data affects both individual autonomy and the maintenance of a democratic order.[13]

In Part I, this Article examines four case studies involving the commodification of personal data: (1) the VeriChip, an implantable ID chip; (2) the wOzNet, a wearable ID chip; (3) networked computing, including spyware and adware; and (4) compensated telemarketing, as advocated in scholarship by Ian Ayres and Matthew Funk.[14] Each of these devices and systems represents an application of technology that commodifies personal data and thereby raises significant concerns about information privacy. Moreover, each has been supported by an argument regarding free alienability — that is, the notion that an individual has the right to do what she wants with her personal information.

Part II then explores three arguments that have been made in opposition to trade in personal data. The first of these points to privacy market failure, which is the idea that current conditions in the market for personal data are so problematic that the cost of any trading outweighs the potential gain. The second argument against data trade, which builds on the first, views privacy as a public good. From this perspective, privacy in personal information matters because of its social payoff, which is the creation and maintenance of a privacy commons. The danger is that trade in propertized personal data may fail to generate necessary privacy commons and destroy existing ones. Finally, a third critique views data trade as problematic because complete propertization of personal data prevents any imposition of restrictions on one's ability to trade personal data. This analysis concludes that none of these views provides a convincing basis for opposing propertization of personal data.

In section III.A, this Article develops the five critical elements of a model of propertized personal information. Rejecting the Blackstonian concept of property as "sole and despotic dominion" over a thing, this

---

[12] *See, e.g.*, Planned Parenthood of Southeastern Pa. v. Casey, 505 U.S. 833 (1992); Thornburg v. Am. Coll. of Obstetricians & Gynecologists, 476 U.S. 747 (1986). More recently, in February 2004, the Justice Department sought records from six hospitals to discover whether certain kinds of federally prohibited abortion procedures were being performed. Eric Lichtblau, *Defending '03 Law, Justice Dept. Seeks Abortion Records*, N.Y. TIMES, Feb. 12, 2004, at A1.

[13] *See infra* Part II.

[14] *See* Ayres & Funk, *supra* note 11; *see also* BARRY NALEBUFF & IAN AYRES, WHY NOT? (2003); Ian Ayres, *Dialing for Dollars*, N.Y. TIMES, Sept. 30, 2003, at A29; Ian Ayres & Barry Nalebuff, *If Telemarketers Paid for Your Time*, FORBES, Apr. 15, 2002, at 225, *available at* http://www.forbes.com/forbes/2002/0415/225.html; Ian Ayres & Barry Nalebuff, *Want To Call Me? Pay Me!*, WALL ST. J., Oct. 8, 2003, at A24.

Article views information property as a bundle of interests to be shaped through legal attention to five areas: inalienabilities, defaults, rights of exit, damages, and institutions. This Article's model of propertized personal data involves the development of a hybrid inalienability consisting of a use-transfer restriction plus an opt-in default. In other words, this hybrid inalienability regime will permit an initial transfer of personal data from the individual, but only if the concerned individual is granted an opportunity to block further transfers or uses by unaffiliated entities. Moreover, this ability to block will generally be set as an opt-in, which means that further use or transfer will not be allowed unless the individual affirmatively agrees to it. Finally, section III.B applies this hybrid alienability model to the four case studies considered earlier. Part IV concludes with a brief consideration of the need for regulation of data trading and an exploration of additional areas for application of the hybrid regime proposed here.

I. TRADING PERSONAL DATA

This Part first considers four methods for collecting and processing personal data. These methods involve an implantable chip, a wearable ID chip, distributed computing, and compensated telemarketing. This Part then explores how these systems and devices commodify personal information, thereby threatening individual privacy and raising the question whether free alienability of personal data is an inherent part of an entitlement to personal information.

A. Four Case Studies

1. The VeriChip: An Implantable Chip. — From a technological viewpoint, the VeriChip is simple. It stores six lines of text, which function as a personal ID number, and emits a 125-kilohertz radio signal to a special receiver that can read the text.[15] A physician implants the VeriChip by injecting it under the skin in an outpatient procedure that requires only local anesthesia.[16] A similar device has already been implanted in millions of pets and livestock to help their owners keep track of them.[17] Applied Digital Solutions, the maker of the VeriChip, plans an implantation cost of $200 and an annual service fee of forty dollars for maintaining the user's database.[18]

---

[15] Julia Scheeres, *They Want Their ID Chips Now*, WIRED NEWS (Feb. 6, 2002), *at* http://www.wired.com/news/privacy/0,1848,50187,00.html.

[16] *Id.*

[17] *Id.*

[18] Julia Scheeres, *Why, Hello, Mr. Chips*, WIRED NEWS (Apr. 4, 2002), *at* http://www.wired.com/news/technology/0,1282,51575,00.html. The Food and Drug Administration (FDA) has found that the VeriChip is not a "medical device" under the Food and Drug Act, and is therefore not subject to its regulation for security and identification purposes. Julia Scheeres, *ID*

Much of the attention toward the VeriChip has centered around the Jacobs, a Florida family whose members all chose to implant it. In an allusion to *The Jetsons*, a cartoon about a space-age family, the media dubbed this Florida family the "Chipsons."[19] Yet the motives that led to the Jacobs's decision to implant the VeriChip are more down-to-earth than space-age. For the father, Jeffrey Jacobs, the implantation decision was related to his severe disabilities. He thought that the device might help save his life one day by providing "instant, electronic access to his complicated medical history and long list of medications."[20] For the mother, Leslie, a similar underlying rationale was present: "[T]he VeriChip speaks for us, if we need it. . . . We can't lose it."[21] For the fourteen-year-old son, Derek, "[i]t's great technology and if you're the first person, it's pioneering."[22] News accounts identified Derek both as being technology-savvy and as having convinced his parents to implant the chip *en famille*.[23]

These comments highlight a number of reasons to choose a VeriChip. Once the ID number in a VeriChip is linked to medical databases, for example, it allows physicians rapid and complete access to medical histories. More prosaically, the VeriChip could identify someone who fell unconscious or for other reasons could not communicate her name.[24] The VeriChip could also be desirable for a different reason: It is the latest electronic gadget. Some consumers are "early adopters," who, in the definition of two economists, are those "electronics enthusiasts who derive utility from being the 'first on their block' to own a new technology."[25]

Additional justifications have been suggested in favor of implantable chips. For example, a chip might help reduce financial fraud as part of a system for withdrawing money from an ATM.[26] Similarly, some have suggested that the VeriChip might stop the growing na-

---

Chip's Controversial Approval, WIRED NEWS (Oct. 23, 2002), *at* http://www.wired.com/news/print/0,1294,55952,00.html.

[19] *See, e.g.*, Jim Goldman, *Family Gets Chipped*, TECHTV (May 10, 2002), *at* http://www.techtv.com/news/culture/story/0,24195,3384209,00.html; Lev Grossman, *Meet the Chipsons*, TIME, Mar. 11, 2002, at 56–57; Press Release, Applied Digital Solutions, VeriChip To Be Featured on ABC's Good Morning America (Feb. 13, 2002), http://www.adsx.com/news/2002/021202.html.

[20] Jim Goldman, *Florida Family To Get VeriChip*, TECHTV (Feb. 18, 2002), *at* http://www.techtv.com/news/culture/story/0,24195,3372523,00.html.

[21] *Id.*

[22] *Id.*

[23] *See, e.g., id.*; Scheeres, *supra* note 15.

[24] Goldman, *supra* note 20.

[25] David Dranove & Neil Gandal, *Network Effects, Standardization, and the Internet: What Have We Learned from the DVD vs. DIVX Battle?*, *in* THE COMMODIFICATION OF INFORMATION 461, 465 (Niva Elkin-Koren & Neil Weinstock Netanel eds., 2002).

[26] Applied Digital Solutions, VeriChip Corporation, *at* http://www.adsx.com/prodservpart/verichip.html (last visited Apr. 10, 2004).

tional crisis concerning identify theft.[27] Applied Digital Solutions has even discussed plans to market the chip in South America as a way "to identify kidnapping victims who are drugged, unconscious or dead."[28] More generally, scientists are now developing biosensors to manage long-term, time-controlled release of targeted medication.[29] Some of these chip-based "micro-electromechanical systems" (MEMS) are already undergoing testing in human subjects.[30] *Scientific American* points to these next-generation implantable chips as particularly important because of the kind of records that they can generate for healthcare personnel.[31]

The kinds of personal data involved in different applications of implantable chips can be extensive and the collection of such data continuous. Thus, a person with an implantable chip generates a data trail by moving about real space, whether in a nursing home, a retail store, or the outdoors. These personal data can be commodified and exchanged for additional services or special discounts. Conversely, the commodification of personal information can also have negative results for certain low-volume or otherwise undesirable customers. It might lead businesses to single out customers in order to discourage their patronage. The privacy consequences of implantable chips will be considerable, and no information privacy law at present regulates the terms of such data collection.

2. The wOzNet: A Wearable Chip. — Whereas the VeriChip involves an implantable identification device, the wOzNet involves a plan to commercialize a wearable identification device.[32] Stephen Wozniak, the famous cofounder of Apple Computer, is the creator of the wOzNet. A product of Wheels of Zeus, the wOzNet tracks a cluster of inexpensive electronic tags from a base station by using Global Positioning Satellite (GPS) information.[33] The broadcast of location information from the chip to the base station is done along the same

---

[27] *See* Julia Scheeres, *Implantable Chip, On Sale Now*, WIRED NEWS (Oct. 25, 2002), *at* http://www.wired.com/news/privacy/0,1848,55999,00.html. To the extent, however, that implantable chips can have their signals pirated or otherwise hacked, these devices will increase the risk of identity theft.

[28] Julia Scheeres, *Politician Wants To 'Get Chipped'*, WIRED NEWS (Feb. 15, 2002), *at* http://www.wired.com/news/technology/0,1282,50435,00.html; *see also* Julia Scheeres, *Tracking Junior with a Microchip*, WIRED NEWS (Oct. 10, 2003), *at* http://www.wired.com/news/technology/0,1282,60771,00.html.

[29] *See* Robert Langer, *Where a Pill Won't Reach*, SCI. AM., Apr. 2003, at 50, 57.

[30] *See id.*; Alexandra Robbins, *My Bio Buddy*, PC MAG., May 6, 2003, at 26.

[31] Langer, *supra* note 29, at 57. This capacity may include tracking the physical location of nursing home residents. *See* Robbins, *supra* note 30, at 26.

[32] Wheels of Zeus, *Overview*, *at* http://www.woz.com/about.html (last visited Apr. 10, 2004).

[33] John Markoff, *Apple Co-Founder Creates Electronic ID Tags*, N.Y. TIMES, July 21, 2003, at C3.

900-megahertz radio spectrum used by portable phones.[34] This portion of the spectrum is largely unregulated; the wOzNet will not be obligated to purchase spectrum rights like a cell phone company. A wOzNet product package, including the chip and the base station, is expected to sell for $200 to $250.[35]

Numerous uses of the wOzNet's tracking capacity have already been proposed. Once a user sets parameters for notification, the wOzNet can generate alerts, by phone or by e-mail, that let the owner know "when a child arrives at school . . . or a car leaves the parking lot."[36] The wOzNet can also help one track pets or personal belongings such as keys or golf clubs.[37] The company has remained vague, however, regarding all the services that it plans to offer; it has stated merely that its system will "help people take better care of what's important to them."[38]

The wOzNet wireless data network also has the potential to track objects far beyond the reach of any individual's base station. As the *New York Times* reports:

> Because the tags can report their location whether they are close to their home-base station or a neighbor's, the company is hoping to seed Silicon Valley and other large suburban counties with enough base stations to make it possible to easily track objects, even when they move outside the range of the owner's station.[39]

Thus, as with other information-age inventions, the wOzNet carries the potential for network externalities once it becomes widely adopted. A network externality is the change in benefit derived from a good as more people consume that good.[40] Once a critical mass of consumers purchase such a device, any user will be able to employ a wearable chip, for no additional charge, to track people and objects far beyond the reach of her base station. It might also be possible for the wOzNet to plant a large number of base stations in an area and capitalize these costs as an infrastructure expense.

Another tracking chip, using a different combination of technologies, has even overcome the need to draw on positive externalities from

---

[34] Benny Evangelista, *Wireless Networks Could Get Personal*, S.F. CHRON., July 21, 2003, at E1, LEXIS, San Francisco Chronicle File.

[35] Associated Press, *Apple Co-Founder To Form Locator Network*, ABCNEWS.COM (July 21, 2003), *at* http://abcnews.go.com/wire/Business/ap20030721_1823.html.

[36] Markoff, *supra* note 33.

[37] *See* Jon Fortt, *Wozniak's Latest Project; GPS Locator Tags for Everything*, SAN JOSE MERCURY NEWS, July 21, 2003, http://www.siliconvalley.com/mld/siliconvalley/news/6349353.htm?template=contentModules/printstory.jsp.

[38] Wheels of Zeus, *Products*, *at* http://www.woz.com/products.html (last visited Apr. 10, 2004).

[39] Markoff, *supra* note 33.

[40] For a general introduction, see S.J. Liebowitz & Stephen Margolis, *Network Effects and Externalities*, *in* 2 THE NEW PALGRAVE DICTIONARY OF ECONOMICS AND THE LAW 671 (Peter Newman ed., 1998).

others' base stations. This competing device, the Wherify GPS Personal Locator, combines GPS tracking with a Personal Communications Service (PCS) device.[41] Rather than send GPS coordinates to a base station, the Wherify Locator uses the PCS transmitter to transmit this information over the PCS wireless network to a Wherify service center. Because of this arrangement, Wherify will be obliged to buy spectrum rights to be able to transmit this information.

Like implantable chips, wearable chips permit extensive and continuous collection of personal data. As discussed later in this Article, both devices associate a unique ID — a kind of personal barcode — with the individual who bears or wears the respective device. This ID can track a person's position, link her movements to existing databanks, and generate new data collections. The privacy implications of this development are considerable and are yet unregulated by law.

3. Networked Computing: Spyware and Adware. — Through networked computing, computer programs can link thousands or even millions of PCs through the Internet. One of the applications of networking is distributed computing, a "form of information processing in which work is performed by separate computers linked through a communications network."[42] Distributed computing links computers to distribute their workload to solve processing-intensive problems.[43] In an uncontroversial application of this technology, Stanford University, the University of California at Berkeley, and other universities have used donated PC system resources for scientific research.[44] These donated resources allow creation of ad hoc supercomputers with massive system resources; the result is dramatically lower computing costs for large-scale research projects.[45]

---

[41] For the company's website devoted to this product, see Wherify Wireless, *GPS Locator for Children*, *at* http://www.wherifywireless.com/prod_watches.htm (last visited Apr. 10, 2004). For a largely negative review of the device, see *Parents & Technology: The Wherify GPS Personal Locator Offers Help but Fails To Protect*, SMART COMPUTING, Feb. 2004, at 35.

[42] MICROSOFT CORP., MICROSOFT COMPUTER DICTIONARY 147 (5th ed. 2002).

[43] Leon Erlanger, *Distributed Computing: An Introduction*, EXTREMETECH (Apr. 4, 2002), *at* http://www.extremetech.com/print_article/0,3998,a=25002,00.asp.

[44] The University of California at Berkeley uses distributed computing for an experiment termed "SETI@home" (The Search for Extraterrestrial Intelligence). *See* Ron Hipschman, *The Problem — Mountains of Data*, *at* http://setiathome.ssl.berkeley.edu/about_seti/about_seti_at_home_1.html (last visited Apr. 10, 2004). SETI@home allows anyone connected to the Internet to use her computer to analyze radio signals from outer space in the search for signs of intelligent life around the universe. *Id.* Volunteer users download SETI@home's software and, using available processing capability, the volunteers' computers process radio signals and report results to a central website. *Id.* It is estimated that roughly 500,000 users are voluntarily sharing their computing power for the SETI@home project alone. *See Screensavers of the World, Unite!*, SCI. DAILY (Dec. 14, 2000), *at* http://www.sciencedaily.com/releases/2000/12/001214082350.htm.

[45] *See, e.g.*, Stanford University, *What is Genome@home?*, *at* http://www.stanford.edu/group/pandegroup/genome/using.html (last visited Apr. 10, 2004). A Stanford University research team launched this distributed computing project in 2000. Its partner project, Folding@home, uses

In contrast, spyware and adware are controversial applications of networked computing. *Smart Computing Magazine* defines spyware as a program that "install[s] itself without your permission, run[s] without your permission, and use[s] your computer without your permission."[46] Spyware draws on computer resources to create a network that can be used for numerous purposes, including collecting personal and nonpersonal information from computers and delivering adware or targeted advertisements to individuals surfing the Web.[47] Adware is sometimes, but not always, delivered as part of spyware; the definitional line between the two depends on whether the computer user receives adequate notice of the program's installation.

Companies such as Gator and Xupiter are industry leaders in the commercial application of distributed computing.[48] For example, the Gator eWallet helps complete online forms by learning usernames, passwords, credit card numbers, and addresses.[49] Gator also bundles its adware with Grokster, a music swapping program, and Weatherscope, a program that provides local weather information.[50] At present, Gator software runs on an estimated 35 million computers in the United States.[51] As a spokesperson for Gator has observed: "Our consumers save billions of dollars per year on software that they'd have to spend $20 to $30 on if they weren't ad supported."[52] But there is a

---

computers to calculate how proteins achieve their three-dimensional shape — that is, how they self-assemble in the human body. *See* Stanford University, *Folding@home Distributed Computing*, *at* http://www.stanford.edu/group/pandegroup/folding (last visited Apr. 10, 2004). Volunteers download Stanford's software onto their machines, and all computers running the software join the project. This use of distributed computing has enabled Stanford researchers "to simulate timescales thousands to millions of times longer than previously achieved" and has allowed the simulation of folding for the first time. *Id.*

[46] Tracy Baker, *Here's Looking at You, Kid: How To Avoid Spyware*, SMART COMPUTING, Sept. 2003, at 68. In the definition of a recent bill, introduced by Representative Mary Bono, a "spyware program" is defined as "any computer program or software that can be used to transmit from a computer . . . by means of the Internet and without any action on the part of the user of the computer to initiate such transmission, information regarding the user of the computer, regarding the use of the computer, or that is stored on the computer." Safeguard Against Privacy Invasions Act, H.R. 2929, 108th Cong. § 4(3) (2003) [hereinafter Bono Bill].

[47] *See* Baker, *supra* note 46, at 68; Cade Metz, *Spyware — It's Lurking on Your Machine*, PC MAG., Apr. 22, 2003, at M7, LEXIS, PC Magazine File.

[48] Gator has recently changed its name to Claria. *See* Claria Corp., *Corporate Overview*, *at* http://www.claria.com (last visited Apr. 10, 2004). This Article nevertheless refers to this company according to its previous, better-known name. In part, it does so because the company continues to call its best-known product the "Gator eWallet." Claria Corp., *Overview: Claria Products and Services*, *at* http://www.claria.com/products (last visited Apr. 10, 2004).

[49] James R. Hagerty & Dennis K. Berman, *New Battleground over Web Privacy: Ads That Snoop*, WALL ST. J., Aug. 27, 2003, at A1.

[50] *See* Metz, *supra* note 47; *see also* Hagerty & Berman, *supra* note 49.

[51] Hagerty & Berman, *supra* note 49.

[52] Declan McCullagh, *Harvard Study Wrestles with Gator*, CNETNEWS.COM (May 22, 2003), *at* http://news.com.com/2100-1032-1008954.html. For an analysis of the Gator Technology by a researcher at Harvard Law School's Berkman Center, see Benjamin Edelman, *Documentation of*

less desirable and less visible aspect of this business model; as *PC Magazine* notes, this program also "sends information about you, your computer, and your online behavior to Gator's website."[53]

The precise nature of the data collection done by these different applications requires some explanation. Gator has stated that its data collection does not include records of consumer identities, by which it means both the first and last names of individuals.[54] In an article focusing on Gator, however, the *Wall Street Journal* noted that this software gathers "a huge amount of information, including many of the sites visited, how much time is spent at them, whether anything is purchased and in some cases the first name, country and five-digit ZIP code of the user."[55] Additionally, Gator assigns a unique number to each computer that downloads its software.[56] As a consequence, it can easily tie a computer to a consumer identity. Moreover, no law prevents this linkage from being made, and other spyware and adware companies are already collecting such personal data.[57] As one computer magazine has stated, "[d]ata gathered by spyware . . . [are] a commodity likely to be sold time and again among third parties such as manufacturers, retailers, and market research firms."[58]

4. Compensated Telemarketing: Listening for Dollars. — As a final example of the commercialization of personal information, consider a recent proposal by Ayres and Funk to allow compensation for listening to telemarketing calls.[59] At present, state and federal "do not call" lists permit consumers only to refuse to receive telemarketing calls, but not to agree to receive these calls for a stated price.[60] This approach is

---

Gator Advertisements and Targeting, *at* http://cyber.law.harvard.edu/people/edelman/ads/gator (last updated June 7, 2003).

53 Metz, *supra* note 47.

54 *See* Hagerty & Berman, *supra* note 49.

55 *Id.*

56 *Id.*

57 On the absence of information privacy law on the Internet, see Schwartz, *supra* note 9, at 1632–40.

58 Brian Hodge, *Ever Get the Feeling You're Being Watched?*, SMART COMPUTING, Nov. 2003, at 60, 61.

59 Ayres & Funk, *supra* note 11, at 96.

60 *See, e.g.*, Telemarketing and Consumer Fraud and Abuse Prevention Act, 15 U.S.C. §§ 6101–6108 (1994) (authorizing the Federal Trade Commission to promulgate rules prohibiting "deceptive or abusive telemarketing practices"); Telemarketing Sales Rules, 16 C.F.R. § 310.4(b) (2003) (creating and establishing a federal "do not call" list); N.Y. GEN. BUS. LAW § 399-z (McKinney Supp. 2004); TEX. BUS. & COM. CODE ANN. §§ 44.101–44.104 (Vernon Supp. 2004); WIS. STAT. ANN. § 100.52 (West Supp. 2003). Although a district court recently held that the FTC's amendments to the Telemarketing Sales Rules violated the First Amendment, the Tenth Circuit recently reversed this holding, *see* Mainstream Mktg. Servs. v. FTC, 283 F. Supp. 2d 1151, 1168 (D. Colo. 2003), *rev'd*, 358 F.3d 1228 (10th Cir. 2004). For a discussion of how the process of getting on the federal "do not call" list will work, and why it is unlikely to stop all telemarketing calls, see Ryan J. Foley, *The Bad News: Telemarketers Will Still Call*, WALL ST. J., Oct. 9, 2003, at D1.

flawed, according to Ayres and Funk, because it blocks exchanges by consumers who are willing to receive such calls for a price and telemarketers who are willing to pay for it. Ayres and Funk term this regime "government-imposed worthlessness" for consumers.[61] In response to this situation, they call for a "name your price" system in which consumers choose the price per minute they would accept for listening to telemarketing calls.[62] Further, Ayres and Funk propose that consumers should be able not only to name a price per minute for telemarketing calls, but also to express tailored preferences for receiving calls.[63] In other words, consumers should be able to sign up to receive compensated telemarketing calls about certain topics, such as Star Trek and running shoes, and refuse other calls, such as those about Time-Warner Cable or long-distance telephone service.[64]

If the Ayres-Funk price system were implemented, "the telephone might become a competitive outlet for polished advertisements (at least rivaling the radio)."[65] Moreover, this approach would allow for efficient use of one's time: "Have five minutes to spare waiting for your train? Why not turn on your cell phone and make some cool hard cash?"[66] Indeed, Ayres and Funk predict that their "name your price" approach would influence telemarketers to discontinue their current overinvestment in reaching consumers who do not wish to be solicited.[67] Ayres and Funk also argue that compensated telemarketing could be easily implemented within the current framework of federal and state "do not call" statutes by amending these laws to give "do not call" households the additional option to receive calls that meet their compensation requirements.[68]

Ayres and Funk propose that one alteration to existing technology as well as one new institution would be necessary to make compensated telemarketing possible. The alteration to existing technology would be the creation of a new kind of 1-900 number. Currently, 1-900 numbers permit consumers to call certain phone numbers for a per-minute charge.[69] For Ayres and Funk, these numbers are "ingoing" 1-900 numbers, and a related system, termed "outgoing" 1-900 numbers, should be established to permit telemarketers to transfer

---

[61] Ayres & Funk, *supra* note 11, at 133–34.

[62] *See id.* at 96.

[63] *See id.* at 110–11.

[64] For a discussion of how this aspect of the Ayres-Funk proposal would lead to the creation of finely grained metadata — or information about information — see *infra* pp. 2070–71.

[65] Ayres & Funk, *supra* note 11, at 101.

[66] *Id.* at 137.

[67] *See id.* at 85.

[68] *See id.* at 110.

[69] *See* 47 C.F.R. § 64.1501 (2002).

payments to consumers.[70] Ayres and Funk explain how a beautiful symmetry would exist under the outgoing 1-900 number: "Just as the resident pays a per-minute charge set by the recipient when she calls the psychic hotline, the psychic hotline would pay a per-minute charge chosen by the recipient if it chooses to drum up business by calling the resident."[71]

As for the new institution, "authorized intermediaries, most likely local phone companies, would have to serve as an interface between consumers and telemarketers."[72] According to Ayres and Funk, these intermediaries should: (1) maintain a list of how much compensation a specific consumer desires for listening to a minute of telemarketing; (2) permit telemarketers to make calls if they agree to pay this rate; (3) transfer the per-minute payment from the telemarketer to the consumer's phone bill; and (4) police telemarketers' compliance with consumer preferences by verifying payment of compensation.[73]

Compensated telemarketing would create massive new databases of personal data. Agreement to receive such calls would lead not only to solicitations, but also to databases that list consumer's likes and dislikes regarding Star Trek, running shoes, home renovation, or reality shows. The resulting databases would also include information about purchases related to the compensated calls. No law at present regulates how the personal information in such databases is collected, sold, or transferred.

To conclude this initial consideration of the four case studies, I wish to note that each of these methods and devices for data collection present a rich spectrum of issues relating to property, privacy, and personal data. One similarity of these systems is that their use will lead to the creation of finely grained collections of personal data. Moreover, these devices and methods all raise difficult issues regarding subsequent use of personal data, and they are at present largely unregulated by the law. Finally, initial collection of personal information is likely to be followed by further trade and even creation of new databases.

As for dissimilarities, some but not all of these systems raise issues concerning the secret collection of data. In particular, adware and spyware operate in an environment in which consumers generally lack any awareness that their computers are "phoning home" to the companies who are tracking their online behavior. In contrast, customers with implantable and wearable chips as well as those who agree to participate in compensated telemarketing will likely be aware at least of the initial collection of their personal information — if not of poten-

---

[70] Ayres & Funk, *supra* note 11, at 81.

[71] *Id.* at 111.

[72] *Id.* at 110.

[73] *Id.* at 110–13.

tial future uses of it. Another dissimilarity concerns the ability of customers to exit from a method of data collection by removing, uninstalling, or otherwise disposing of these different devices. A wearable chip can be unclipped, but an implantable chip must be removed in a medical procedure. Moreover, adware and spyware can be devilishly complicated to discover and uninstall.[74] The underlying software is sometimes written to resist detection through standard "uninstall" programs; indeed, the removal of adware and spyware can challenge even the most experienced of computer experts.[75] Hence, the costs of exiting from different systems vary considerably.

B. Commodification, Privacy, and Free Alienability

This section makes three observations regarding the VeriChip, the wOzNet, adware and spyware, and compensated telemarketing. First, these systems and devices demonstrate the extent to which technology is already commodifying personal information. Second, they raise significant privacy issues. Third, a centerpiece of debate about these systems and devices thus far has been the idea that free alienability of personal data is desirable and should be permitted.

1. Commodification. — The case studies show how technology is commodifying personal information. As Margaret Radin observes, commodities represent a certain kind of social construction,[76] something that is "capable of being reduced to money without changing in value, and completely interchangeable with every other commodity in terms of exchange value."[77] Thus, commodified personal data is a discrete package of personal information that can be exchanged for something else. There is a developing trade in personal information, which is following in the path of other controversial commodities discussed in Radin's book, *Contested Commodities*, such as body parts, babies, and services for sexual intercourse.[78]

Adware and spyware, as well as compensated telemarketing, provide good illustrations of the commodification of personal data. To be sure, these products also commodify other resources, including an individual's time, attention, and computing resources. These issues are relatively unproblematic, however, once the quality of notice is improved. When informed consent is obtained, one's donation of computer resources or attention to targeted advertisements does not raise especially complex or sensitive policy issues. After all, one can already

---

[74] *See* Cade Metz, *Spy Stoppers*, PC MAG., Mar. 2, 2004, at 79, 79–80.

[75] *Id.* at 80.

[76] MARGARET JANE RADIN, CONTESTED COMMODITIES 2–15 (1996).

[77] *Id.* at 3.

[78] *Id.* at 131–53.

donate other commodities to charity or watch advertisements on television.

In contrast, the commodification of personal information raises more complex questions. Commodification of personal data falls into four broad categories: (1) lists of those who are willing to commodify their personal data; (2) lists of those who wish to receive tailored ads and the particular interests of those persons; (3) lists of transactional activities, such as purchases, that follow the release of commodified personal data; and (4) privacy metadata, which comprise information about one's privacy preferences.[79]

The topic of privacy metadata deserves additional discussion at this point. Metadata are a relatively common phenomenon in the Information Age, and compensated telemarketing as well as the other systems and devices considered in the case studies are all capable of creating privacy metadata. Metadata are information about information; they are, for example, found in the popular text-processing software Microsoft Word, which permits association of rich metadata with documents.[80] Metadata in Word can include the author's name and initials; the names of previous document authors; the name of the author's company or organization; the name of one's computer; the name of the network server or hard disk where the document was saved; document revisions; hidden text or cells; and personalized editing comments.[81] All these metadata can be associated with a single text document.[82]

The personal data market will increasingly include privacy metadata. The systems and devices considered in the case studies above generate finely grained information about consumers' privacy preferences,[83] and privacy metadata will in turn be commodified and contribute to additional privacy invasions.[84] Already in the offline world,

---

[79] For an overview of privacy metadata, see Schwartz, *supra* note 5, at 768–71.

[80] *See* Microsoft Corp., *OFF: How To Minimize Metadata in Microsoft Office Documents* (Microsoft Knowledge Base Article No. 223,396), http://support.microsoft.com/default.aspx?scid=kb;en-us;223396 (last visited Apr. 10, 2004).

[81] *Id.* In some instances, embarrassing secrets have been revealed through Word metadata. *See* Michael J. McCarthy, *Beware, "Invisible Ink" Inside Computer Files May Reveal Your Secrets*, WALL ST. J., Oct. 20, 2000, at A1.

[82] Metadata are also discoverable under the Federal Rules of Civil Procedure. *See* Richard E. Donovan & Lauri A. Mazzuchetti, *Judicial Attention to Electronic Discovery Heats Up*, METROPOLITAN CORP. COUNS., Sept. 2003, at 54.

[83] On the Internet, moreover, software protocols, such as P3P, and increasingly XML, can lead to the creation of privacy metadata. *See* Schwartz, *supra* note 5, at 768–71. There are ways, however, to minimize most metadata when one uses P3P. *See* William McGeveran, *Programmed Privacy Promises: P3P and Web Privacy Law*, 76 N.Y.U. L. REV. 1812, 1826–33 (2001).

[84] For a battle over such privacy metadata in the context of traditional telephony, see *U.S. West, Inc. v. FCC*, 182 F.3d 1224, 1228 (10th Cir. 1999), *cert. denied sub nom.* Competition Policy Inst. v. U.S. West, Inc., 530 U.S. 1213 (2000) (mem.). For differing views on the merits of this decision, compare Fred H. Cate, *Principles of Internet Privacy*, 32 CONN. L. REV. 877, 893–95

and in no small irony, direct marketers generate and sell lists of people who have expressed interest in protecting their privacy.[85] Analogous to these marketing lists of those who wish to protect their privacy, privacy metadata can include information concerning an interest in not receiving certain kinds of solicitations or not receiving telemarketing calls at certain times. These metadata will be highly marketable.

As a specific example of the process of commodification, consider, for example, how the Gator eWallet commodifies personal information. Gator, as well as similar companies, provides something of value, usually software, in exchange for something from a consumer that is also of value, namely personal data. Indeed, many post-Napster file-sharing services, such as Grokster, come bundled with adware.[86] As *PC Magazine* observes, "[t]hat's how file sharing vendors make money while not charging for their products."[87] The Ayres-Funk proposal for compensated telemarketing also demonstrates the commodification of personal data. Once it is possible to agree to receive phone calls for a given price, a rich trove of personal data will be created.

As for implantable and wearable chips, their use will also lead to the creation and exchange of data lists in an information marketplace. VeriChip or wOzNet customers, such as the Jacobs family, can generate records by having their physical location continuously monitored, and the resulting personal data can be commodified and traded. This phenomenon may even lead the makers of the VeriChip and the wOzNet to adjust their business model, which one might term a "pay-and-go" approach, in order to permit data trade. Under the current "pay-and-go" approach, the VeriChip and the wOzNet are sold to consumers for a flat price. This one-size-fits-all approach fails to capture the value that might have been created by permitting individuals to pay for restrictions on dissemination of their personal data, or conversely, by giving potential customers a discount in exchange for the right to use their data.[88] Although the VeriChip and the wOzNet are not yet taking full commercial advantage of the personal data their systems generate, personal data trade is flourishing in other contexts. As one computer magazine observed of the

---

(2000), with Paul M. Schwartz, *Charting a Privacy Research Agenda: Responses, Agreements, and Reflections*, 32 CONN. L. REV. 929, 935–36 (2000).

[85] *See* SCHWARTZ & REIDENBERG, *supra* note 9, at 234.

[86] *Id.*

[87] Metz, *supra* note 47.

[88] One can imagine two additional versions of these products. A "data trade" version of these devices would permit a customer to exchange her personal data for a discounted or free VeriChip or wOzNet. On the other hand, a "privacy" version would permit VeriChip and wOzNet to extract additional value from customers who value their privacy more highly and are willing to pay extra for restrictions on the companies' use of their personal data.

adware offered by filesharing services: "In a sense, you are paying, but the coin is privacy, not money."[89]

2. Privacy. — These technologies also raise threats to privacy. In particular, the commodification of personal data is likely to impact information privacy by leading to an increase in data trade. For example, the unique ID number employed by the VeriChip and the wOzNet could track a person's position and link her movements to existing databanks.

Consider a hypothetical shopping expedition by Derek Jacobs, the fourteen-year-old early adopter of tracking technology.[90] As Derek arrives at a store with his implanted VeriChip or wearable wOzNet chip, he triggers the store's central computer, which makes his profile, based on previous purchases and commercially available marketing lists, available to sales clerks throughout the building. The store also tracks his overall path through its interior to see which departments and products are of interest to him. Should Derek linger at the table where digital cameras are displayed, a sales clerk can glance at his shopping profile. If this summary were to list him as a heavy spender on electronics or as a frequent customer of a particular company the sales clerk could suggest certain products to him, steer him away from others, and, in general, pay more attention to him than to an unidentified customer.[91]

Even if Derek makes no purchases, his presence in the store and interest in digital cameras can be added to his marketing profile and shared with other merchants for other purposes. The kinds of marketing directed to him, and even the prices for the products offered to him, can all be customized according to a constantly updated and expanding database of personal information. As a dystopian alternative to the scenario sketched thus far, one can also imagine that Derek may receive worse service as a result of this tracking. The store's database might reveal that Derek is not a heavy spender or that he is someone who purchases products exclusively online. In fact, some retail consultants are already recommending that stores create "not wanted" lists with the names of undesired customers.[92]

Thus, implantable and wearable chips enable the collection, storage, transfer, and tailored use of enormous amounts of personal data.

---

[89] Metz, *supra* note 47.

[90] Jerry Kang has engaged in a similar discussion comparing a visit to a shopping mall and one to a "cyber-mall." *See* Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1198–99 (1998).

[91] This kind of attention is reminiscent of the idea of "one to one" marketing developed by Don Peppers and Martha Rogers. *See* DON PEPPERS & MARTHA ROGERS, THE ONE TO ONE FUTURE: BUILDING RELATIONSHIPS ONE CUSTOMER AT A TIME (1993).

[92] *See* LARRY SELDEN & GEOFFREY COLVIN, ANGEL CUSTOMERS & DEMON CUSTOMERS: DISCOVER WHICH IS WHICH AND TURBO-CHARGE YOUR STOCK (2003).

This possibility also raises significant privacy concerns, as do adware, spyware, and compensated telemarketing, which allow online behavior to be tracked and personal data collected. This software "configures itself to load each time your system boots, sitting quietly in the background and taking notes on your computing activities."[93] This tracking is a cyberspace analog to the attention that Derek Jacobs received on his hypothetical shopping expedition.

As for telemarketing, Ayres and Funk consider it an intrusion onto one's solitude. Their concern is with *physical* privacy, or what they term "the right to be left alone in one's home."[94] In contrast, the focus in this Article is on *information* privacy, an interest to which compensated telemarketing raises a different sort of threat. The critical point regarding information privacy is that an agreement to receive phone calls for a given price leads not only to the agreed telemarketing calls, but also, in the absence of effective legal rules, to the additional use of personal data.[95] Some of this information might be trivial, other data might be embarrassing, and some might even create potentially damaging labels or lead to other kinds of harmful results. Moreover, as section II.B argues, these databanks of personal information can have a profound impact on society in general.

In sum, the privacy implications of these devices, programs, and systems are troublesome.[96] Indeed, the example of the telescreen from George Orwell's dystopian masterpiece *Nineteen Eighty-Four* comes to mind. As Orwell wrote: "There was of course no way of knowing whether you were being watched at any given moment. . . . You had to live — did live, from habit that became instinct — in the assumption that every sound you made was overheard, and, except in darkness, every moment scrutinized."[97] Unlike Orwell's telescreen, however, the VeriChip and the wOzNet permit even movements made in darkness to be scrutinized. Another significant difference may exist: unlike Orwell's telescreen, access to these devices or systems can be restricted to persons who have *agreed* to have others observe them and collect their personal information. This distinction leads to a final observation, which concerns the alienability of personal data.

---

[93] Baker, *supra* note 46, at 68.

[94] Ayres & Funk, *supra* note 11, at 83.

[95] For a general discussion of secondary use of personal data, see Paul Schwartz, *Data Processing and Government Administration: The Failure of the American Legal Response to the Computer*, 43 HASTINGS L.J. 1321, 1339–41 (1992).

[96] Plans are even underway to develop a larger VeriChip device with a built-in Global Positioning Satellite receiver. *See* Scheeres, *supra* note 27.

[97] GEORGE ORWELL, NINETEEN EIGHTY-FOUR 6–7 (1949). For a pathbreaking discussion of metaphors of privacy in novels by George Orwell and Franz Kafka, see Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1413–30 (2001).

3. Free Alienability of Personal Data. — According to this Article's previous definition, an inalienability is any restriction on the transferability, ownership, or use of data. In the context of the case studies, inalienability relates to restrictions on the exchange of personal data, even restrictions contrary to an individual's wishes. In other words, even if someone wants to engage in data trade, society may wish to limit her ability to do so. A principle of free alienability for personal information would mean, in contrast, that an individual has a right to do what she wants with her data.

ADS, makers of the VeriChip, and wOz, developers of the wOzNet, respond to privacy questions regarding their products by declaring that it is all a matter of personal choice for their customers. The Chief Technology Officer of ADS states: "This is an elective technology. We live in the United States of America, it's a free world. You want the VeriChip, get the VeriChip. You don't want the VeriChip, don't get the VeriChip."[98] In a similar vein, ADS customer Leslie Jacobs observes: "People who need this should be able to elect to have it. . . . The VeriChip could help save lives."[99] Or, as the makers of the wOzNet stated, "because the network is voluntary, and will employ encryption that keeps unauthorized users from monitoring someone else's wOzNet activities, privacy and surveillance concerns are not relevant."[100] Thus, justifications for this data-gathering technology typically rest on the notion that an individual's self-ownership entails the right freely to share or dispose of personal information. Or, restated in more colloquial terms: "If you want to sell your personal information, do it. If you don't want to sell it, don't do it."

Alienability has yet to emerge as a policy issue for adware and spyware because the makers of these products generally offer inadequate notice of their data practices. It would be difficult for adware and spyware companies to make an argument for free choice to trade personal data in the absence of sufficient notice of data collection and processing practices. Informed consent to adware and spyware would require notice of such practices; without it, there is no free choice to trade data.[101] At present Congress is considering competing bills, in-

---

[98] Jim Goldman, *Family Gets Chipped*, TECHTV (May 10, 2002), *at* http://www.techtv.com/news/culture/story/0,24195,3384209,00.html (quoting Applied Digital Solutions CTO Keith Bolton) (internal quotation marks omitted).

[99] Scheeres, *ID Chip's Controversial Approval*, *supra* note 18.

[100] Markoff, *supra* note 33.

[101] The area of informed consent to medical decisionmaking provides possible analogies. *See* Joseph Goldstein, *For Harold Lasswell: Some Reflections on Human Dignity, Entrapment, Informed Consent, and the Plea Bargain*, 84 YALE L.J. 683, 691 (1975) (discussing how informed consent should be analyzed as "the process of informing [the citizen] for decision" (emphasis omitted)); Peter H. Schuck, *Rethinking Informed Consent*, 103 YALE L.J. 899, 942–48 (1994) (proposing a model of "cost-effective" informed consent).

troduced by Representative Mary Bono and Senator John Edwards, which would impose a notice requirement for companies who wish to install either spyware or adware.[102] The Bono Bill requires, for example, that software applications of distributed computing come with a "clear and conspicuous request" for express consent from consumers.[103] Should either of these statutes be enacted, one can imagine an enthusiastic free data alienability argument for adware and other forms of distributed computing.

A believer in free alienability might even argue that Gator and related companies do not go as far as they could. Gator associates a unique number with a computer; it also promises not to combine its Web-surfing profiles with full identity information.[104] Yet, with improved notice, Gator might attempt to expand its business model by permitting customers to agree to associate their Web-surfing data with their personal identities. The company might justify this expansion with a classic free alienability argument: if people want to trade their personal data, they should be allowed to do so.

Finally, concerning compensated telemarketing, Ayres and Funk also see the question of alienability as critical. With a focus on the issue of physical privacy — that is, the right to solitude — Ayres and Funk argue that "[c]ommodification . . . would mean a switch from a regime that values physical privacy at zero (since marketers can consume it at will and without cost) to one in which physical privacy has positive value."[105] They even predict a potentially heightened taste for privacy-as-solitude under their proposal: "the switch from government-imposed worthlessness [under a statute] to market valuation should cause people to value it more highly."[106] As a result, individuals should be permitted "to freely alienate their right to market privacy — that is, their right to be left unsolicited."[107]

Information privacy in the context of telemarketing and elsewhere, however, raises issues different from those raised by physical privacy. Among the chief information-privacy issues are that of downstream data use by third parties and the consequences of this use, such as labeling of individuals following access to databases of their personal information. Nevertheless, a revised Ayres-Funk argument is possible in the context of information privacy. At present, marketers can consume personal data at will, and consumers are frequently unaware of the

---

[102] *See* Bono Bill, H.R. 2929, 108th Cong. § 4(3) (2003); Spyware Control and Privacy Protection Act of 2001, S. 197, 107th Cong. (2001) [hereinafter Edwards Bill].

[103] Bono Bill § 2(a).

[104] *See supra* p. 2065–66.

[105] Ayres & Funk, *supra* note 11, at 133.

[106] *Id.* at 133–34.

[107] *Id.* at 96.

data trade. Once consumers receive notice, commodification of personal data can change a regime that values information privacy at zero to one in which information privacy has positive value. Under this theory, a higher market value for personal data might heighten our appreciation for it.

II. AGAINST DATA TRADE: ARGUMENTS FROM PRIVACY AND PROPERTY THEORY

Many legal scholars remain skeptical of the usefulness of property rights in personal information. As Jessica Litman writes, data trade "encourages transactions in data that most of us would prefer be discouraged."[108] Or, as Mark Lemley warns, "from a privacy perspective, an intellectual property right that is regularly signed away may turn out to be less protection than we want to give individuals."[109] I have previously joined in at least part of this chorus of skepticism regarding propertization of personal data. Elsewhere, I have argued that "property rights in personal data may systematically lead to bad bargains — and ones in areas of great social importance."[110]

This Part examines and re-evaluates the skepticism regarding property rights in personal data; the following Part develops a model for propertization of personal data that accommodates these concerns. The established critique of propertization of personal data has three elements. The first critique considers the impact of propertization under current conditions in the existing "privacy market" and points to existing privacy market failures as an argument against data trade. Beyond this analysis of privacy market failure, the second critique flows from the "public good" nature of information privacy. These first two critiques are frequently conflated; this Part will separate these perspectives while also exploring how they are related. Finally, a third concern regarding propertization relates to the consequences of free alienability of personal data.

A. Privacy Market Failure

The emerging verdict of many privacy scholars is that existing markets for privacy do not function well. Due to such market failures, which are unlikely to correct themselves, propertization of personal information seems likely to lead to undesired results — even to a race to the bottom as marketplace defects lead competitors to take steps that are increasingly harmful to privacy. This perspective is found, for ex-

---

[108] Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1303 (2000).

[109] Lemley, *supra* note 4, at 1551 (emphasis omitted).

[110] Schwartz, *supra* note 5, at 763.

ample, in Julie Cohen's scholarship; in her view, a negative correlation is likely to exist between property in personal information and the resulting level of information privacy.[111] Cohen writes: "Recognizing property rights in personally-identified data risks enabling more, not less, trade and producing less, not more, privacy."[112] Market failure will cause people to trade away too much of their propertized personal data and thereby erode existing levels of privacy.[113] Or, as Lemley concludes, "there is no good market solution" for information privacy based around property rights.[114]

In previous work, I have developed a yardstick for evaluating the functioning of a market for personal information that involves assessing the extent to which "privacy price discrimination" is available for consumers.[115] The economists' standard definition of price discrimination is that a seller sets "different prices to different purchasers depending not on the costs of selling to them . . . but on the elasticity of their demand for his product."[116] In contrast, privacy price discrimination involves data-processing companies drawing distinctions between individuals based on varying preferences about the use of their personal data. One failure of the current privacy market is its inability to draw such distinctions, leaving consumers with a binary, all-or-nothing choice to permit or prohibit collection of their personal data.

To illustrate this point, one can posit two consumers: Marc, who cares deeply about how his personal information is used, and Katie, who does not.[117] A surplus from cooperation under a property regime requires at a minimum, however, that Marc and others with similar preferences receive more than their "threat value" before disclosing their personal data.[118] The term "threat value" refers to the price that Marc would place on *not* disclosing his personal information. Thus, Marc might desire a certain price in goods, services, or cash before allowing any of his personal information to be collected. Privacy price

---

111 *See* Cohen, *supra* note 4, at 1391.

112 *Id.*

113 *See id.* at 1391–1401.

114 Lemley, *supra* note 4, at 1554 (internal quotation marks omitted).

115 *See* Schwartz, *supra* note 5, at 763–66; *see also* Schwartz, *supra* note 9, at 1687. Privacy price discrimination has a close analogy in the law of intellectual property. In the context of computer software, in particular, the law has been highly attentive to price discrimination and the kinds of behavior that should be permitted among buyers and sellers of information goods. *See id.* at 1687 n.460.

116 RICHARD POSNER, ECONOMIC ANALYSIS OF LAW 283 (6th ed. 2003). For a pathbreaking discussion of the benefits of price discrimination in the production of public goods, see Harold Demsetz, *The Private Production of Public Goods*, 13 J.L. & ECON. 293 (1970).

117 For a discussion of different consumer preferences about privacy, see Katie Hafner, *Do You Know Who's Watching You? Do You Care?*, N.Y. TIMES, Nov. 11, 1999, at G1.

118 For a concise introduction to bargaining theory, see ROBERT COOTER & THOMAS ULEN, LAW AND ECONOMICS 72–74 (2d ed. 1997).

discrimination therefore requires an increased flexibility on the part of those who collect personal information to meet Marc's other privacy preferences. Marc may have strong preferences regarding initial or secondary uses of his personal information, the collection of his metadata, or the transfer of data to other companies.

Currently, however, companies generally do not need to offer Marc more goods, products, or money for his personal data than they offer Katie. Part I has discussed this phenomenon in the case of the VeriChip, the wOzNet, and distributed computing. The same situation holds for telemarketing — at least for telemarketing as it exists now, rather than as the Ayres-Funk model imagines it. Marc and Katie have only two choices under the existing model for telemarketing. They can either refuse all telemarketing or listen to calls without compensation. As a result, telemarketing companies need not distinguish between customers with different privacy preferences, but must reach all individuals in the same fashion.

In a more extreme illustration of privacy market failure, suppose that spyware companies collect the data of Marc and Katie alike without these customers' knowledge. Consumer ignorance leads to a data market in which one set of parties does not even know that "negotiating" is taking place.[119] Even if there is a sense that some personal data are collected, many individuals do not know how or whether this information is further processed and shared. Regarding the Internet, for example, Neil Netanel notes: "[M]ost users are not even aware that the websites they visit collect user information, and even if they are cognizant of that possibility, they have little conception of how personal data might be processed."[120] A recent report from the Annenberg Public Policy Center confirms Netanel's observations; it found that "the overwhelming majority of U.S. adults who use the internet at home have no clue about data flows — the invisible, cutting-edge techniques with which online organizations extract, manipulate, append, profile and share information about them."[121] The asymmetry of information available to the various players in the market — as well as the systemic disadvantage and relative vulnerability of consumers in that market — underscores concerns about commodification of personal data.

---

[119] Or, as Jeff Sovern writes, "sellers can be expected to exploit consumer ignorance." Jeff Sovern, *Opting In, Opting Out, or No Options at All: The Fight for Control of Personal Information*, 74 WASH. L. REV. 1033, 1074 (1999).

[120] Neil Weinstock Netanel, *Cyberspace Self-Governance: A Skeptical View from Liberal Democratic Theory*, 88 CAL. L. REV. 395, 476 (2000).

[121] JOSEPH TUROW, ANNENBERG PUB. POLICY CTR. OF THE UNIV. OF PA., AMERICANS AND ONLINE PRIVACY: THE SYSTEM IS BROKEN 4 (2003), *available at* http://www.asc.upenn.edu/usr/jturow/internet-privacy-report/36-page-turow-version-9.pdf.

Ultimately, the consequences of these market shortcomings resound far beyond Marc and Katie. Due to pervasive failures in the privacy market in the United States, a subsidy is given to those data-processing companies that exploit personal data. As a result, these organizations are not charged the true "cost" of the personal data they acquire.[122] One result of subsidized personal information is that companies overinvest in reaching consumers who do not wish to be contacted. To return to our hypothetical, Marc may not want to surrender his personal information at a price below his threat value, but companies who do not meet this threshold are able to obtain his information and contact him anyway. Ayres and Funk have reached a similar conclusion regarding overinvestment in telephone solicitations from direct marketers. In their view, marketers "solicit an excessively broad audience."[123] Indeed, "sellers of niche products" lack "adequate incentive[s] to target likely customers."[124]

Acquisition of personal information at below-market costs also leads companies to underinvest in technology or services that can enhance the expression of privacy preferences. One reason for this under investment is that individual privacy wishes are not felt collectively in the market. In general, savvy consumers who wish to take action to protect their privacy face serious difficulties. For example, there is a critical mass problem — at least during the initial stages of a possible move to greater privacy protection. Consumers must identify others who share their concerns and identify technology that will assist them. Moreover, information costs make it difficult for less sophisticated consumers to benefit from the knowledge and efforts of those who are more savvy about privacy. Furthermore, consumers face high, potentially prohibitive detection costs in monitoring companies and detecting those that fail to live up to their privacy promises.

Consider in this regard how the market has thus far proved far more effective at providing Privacy-Invading Technologies, or PITs, than Privacy-Enhancing Technologies, or PETs.[125] One difficulty is that it is possible for PITs to masquerade as PETs — as is the case when a link promising a privacy-enhancing product leads instead to

---

[122] Laudon reaches a similar general conclusion about privacy market failure. *See* Laudon, *supra* note 5, at 99.

[123] Ayres & Funk, *supra* note 11, at 85.

[124] *Id.*

[125] For discussion of PITs and PETs, see Philip E. Agre, *Beyond the Mirror World: Privacy and the Representational Practices of Computing*, *in* TECHNOLOGY & PRIVACY, *supra* note 3, at 29, 56; Herbert Burkert, *Privacy-Enhancing Technologies: Typology, Critique, Vision*, *in* TECHNOLOGY & PRIVACY, *supra* note 3, at 125. For an excellent website devoted to this topic, see Roger Clarke, *Roger Clarke's PITs and PETs Resources Site*, *at* http://www.anu.edu.au/people/Roger.Clarke/DV/PITsPETsRes.html (last updated Oct. 21, 2002).

software, such as Web Bugs, that spies on computer users.[126] Or, in another illustration of problems for consumers in detecting privacy violations, a popular file-sharing software, Blubster, promises to protect anonymity vis-à-vis third parties who are investigating online copyright violations, but it also smuggles in adware that tracks the computer user.[127] The result is that Blubster is a PET for fileswapping, but a PIT for other online behavior.[128]

Other problems exist within the privacy market. Information asymmetries are likely to exist between data collectors and the individuals whose personal information is collected.[129] Indeed, data collectors have an incentive to engage in smokescreen tactics to make it difficult for individuals to obtain understandable information about data collection and use. For example, "privacy notices" sometimes fail to reveal the substantive nature of a website's actual practices.[130] Websites also generally reserve the right to change their privacy policies, which means that visitors must constantly check for changes in the fine print.

Put more generally, problems with asymmetric information can be systematic enough to skew an entire class of negotiations. By analogy, in the context of real estate transactions, the seller may understand the commission that a broker receives, but may comprehend little about who receives earnest money following a purchaser's breach. As another illustration of information shortcomings, buyers of used automobiles face high transaction costs in gathering information about the most critical piece of information: whether the car is in good condition.[131] As Robert Cooter and Thomas Ulen state, "it is often the case that sellers know more about the quality of goods than do buyers. For example, a person who offers his car for sale knows far more about its quirks than does a potential buyer."[132]

The example of used cars also indicates, however, that information asymmetries need not remain in place. In fact, the distribution of information about used cars to buyers has recently improved due to information technology and private sector entrepreneurship. Using a car's unique Vehicle Identification Number (VIN), it is possible to or-

---

126 For more on Web Bugs, see Richard M. Smith, Electronic Frontier Foundation, *The Web Bug FAQ*, *at* http://www.eff.org/Privacy/Marketing/web_bug.html (Nov. 11, 1999).

127 Konstantinos Karagiannis, *File Sharing Without the Tracks*, PC MAG., Sept. 16, 2003, at 30, 30–31.

128 *See id.*

129 *See* H. JEFF SMITH, MANAGING PRIVACY: INFORMATION TECHNOLOGY AND CORPORATE AMERICA 95–138 (1994); Schwartz, *supra* note 5, at 766.

130 *See* Edward J. Janger & Paul M. Schwartz, *The Gramm-Leach-Bliley Act, Information Privacy, and the Limits of Default Rules*, 86 MINN. L. REV. 1219, 1242–44 (2002).

131 *See* COOTER & ULEN, *supra* note 118, at 41.

132 *Id.*

der an inexpensive online report that details accident reports relating to a used automobile, as well as other information about it.[133] A seller will likely still know more than the buyer about the quirks of an automobile, but the transaction costs of obtaining at least some critical information about any specific vehicle have declined dramatically thanks to these reports.

Nevertheless, entrenched information asymmetries may cause a "lemons equilibrium." Once the imbalance of information causes a sufficiently large number of buyers to cease purchasing, a seller will lose money as a result of a decision to offer more favorable terms at a higher price. The result is a lemons equilibrium, which occurs when the market offers only bad products for sale or presents only bad contract terms.[134] As Richard Craswell explains: "In that case, no seller has an incentive to offer the more favorable terms, and the result is an equilibrium in which only bad contract terms (or 'lemons') can be obtained."[135] Professor Craswell thus identifies an unfortunate consequence of an inability of buyers and sellers to agree on how to signal the presence of a good product.

Finally, the phenomenon of "bounded rationality" means that many consumers will accept whatever terms that data processors offer for their personal information. Behavioral economics scholarship has demonstrated that consumers' general inertia toward default terms is a strong and pervasive limitation on free choice.[136] Propertization may therefore benefit those who have greater power in the existing privacy market — the parties who collect, process, and transfer personal data.[137] Because the gatherers have greater power to set the terms of

---

[133] A leading purveyor of these reports is CARFAX. *See* CARFAX, Inc., *CARFAX Vehicle History Reports*, *at* http://www.carfax.com (last visited Apr. 10, 2004).

[134] Richard Craswell describes the difficulty in overcoming a lemons equilibrium:

> Because terms that are good for buyers are generally more expensive for sellers, any seller that offers better terms will charge a higher price to make the same level of profits she could make by offering less favorable terms at a lower price. However, if most buyers have good information about prices but only poor information about non-price terms, they may not notice an improvement in non-price terms, while they will definitely notice the higher price. As a result, many buyers may stop purchasing from this seller.

Richard Craswell, *Property Rules and Liability Rules in Unconscionability and Related Doctrines*, 60 U. CHI. L. REV. 1, 49 (1993).

[135] *Id.* (footnote omitted).

[136] *See* Daniel Kahneman et al., *Experimental Tests of the Endowment Effect and the Coase Theorem*, 98 J. POL. ECON. 1325, 1342–46 (1990); Amos Tversky & Daniel Kahneman, *Judgment Under Uncertainty: Heuristics and Biases*, 185 SCIENCE 1124, 1127 (1974). For an application of this body of research in a legal context, see Russell Korobkin, *Inertia and Preference in Contract Negotiation: The Psychological Power of Default Rules and Form Terms*, 51 VAND. L. REV. 1583, 1587–92 (1998).

[137] In some settings, individuals may even be subject to duress, as in the context of receiving health care, and may thereby easily be forced to sign away privacy interests without any real choice in the matter.

the bargain and to shape the playing field that guides individual decisions, at the end of the day negotiations in the privacy market may fall short.[138]

This Article has noted the general lack of "privacy price discrimination" in existing information markets and has identified different grounds for this shortcoming. Yet identification of market failure can justify a policy to perfect the market just as much as one to prohibit it. More specifically, if a deadweight loss occurs because of shortcomings in the privacy market, the question becomes the extent to which a market can adjust to capture this potential value. In the context of information markets, both those who wish to sell their data and those who do not will experience a deadweight loss. The goal of market-perfecting policies should be to reform the failed privacy market to reflect more completely the varying value of personal data to individuals with different preferences about whether and how that data should be used. Once the market internalizes these preferences, resulting exchanges would increase social welfare.[139] Note, however, that such an economic perspective will generally be indifferent as to whether any resulting surplus from exchanges accrues to the information collectors or the individuals to whom the personal information pertains.

Market-perfecting moves for the personal data trade would require removing or at least reducing information asymmetries between data collectors and individuals. This Article has already pointed to an example of a reduction of these asymmetries in the context of the market for used cars: one can order an online report keyed to a specific automobile's VIN that details information about the vehicle's history. Later in this Article, I discuss how legislatively created opt-in defaults to personal data trade can be "information-forcing." These requirements can reduce information asymmetries by placing pressure on the better-informed party to share relevant data.

---

[138] Self-help exists as a final tactic. Those who care about privacy can turn to a burgeoning market and purchase devices like the "telezapper," which, when hooked to one's phone, is intended to convince telemarketers that the phone has been disconnected. *See* Ayres & Funk, *supra* note 11, at 92–93. Downloadable software are also available to stop different kinds of privacy invasions on the Internet. For a discussion, see Cade Metz, *Total Security*, PC MAG., Oct. 1, 2003, at 83, 86. But the privacy arms race never stands still, and there remains a strong need to stay on the cutting edge of developments regarding information collection and to continue to purchase new and improved self-help devices and software. In an assessment of privacy-enhancing technologies, Jerry Kang concludes that "[a] significant expenditure of resources by those who would take personal information and by those who would safeguard it may, in the end, result in a final level of privacy no different from the level that existed before such expenditures." Kang, *supra* note 90, at 1245. Furthermore, the market may favor PETs over PITs due to collective action problems facing individual consumers.

[139] As Judge Easterbrook proposes, a Coasean paradigm requires only that property rights be created, that property rules be clear, and that bargaining institutions be created. Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F. 207, 210–15.

Attempts to improve the market for data trade would also draw on the teaching of behavioral economics to reduce the bite of "bounded rationality" so consumers can better trade their personal data. Previous work that I have done with Edward Janger has discussed the impact of the "framing effect" on consumer decisionmaking regarding privacy.[140] The presentation of options influences choices, and the parties who determine the form in which information about privacy is presented have considerable power to shape how consumers act.[141] As a consequence, Janger and I have proposed that governmental oversight agencies should play a role in shaping the form in which consumers receive notice of information practices.[142] I return to the topic of oversight in section III.A below.

More generally, market-perfecting activities call for attention to overcoming collective action problems. The model developed below suggests that one response to collective action difficulties is permitting liquidated damages for violations of privacy interests. Permitting liquidated damages provides an opportunity for collective valuation of information, which incorporates a diverse spectrum of preferences — that is, it tries to accommodate both Marc and Katie. It also encourages litigation, the specter of which may deter infringements of privacy.[143] It will also allow others who are not parties to the litigation to benefit from improved privacy practices that follow successful litigation. Some positive results following from liquidated damages can already be seen in the context of the Telephone Consumer Protection Act[144] (TCPA), a federal law that outlaws both "junk" faxes and unsolicited telemarketing calls. This legislation has led at least some disgruntled consumers to sue companies who violate the law.[145] These crusaders include Steve Kirsch, a Silicon Valley billionaire who has adopted the cause of fighting against junk faxes; Diana Mey, a homemaker who has been termed the "Erin Brockovich of the anti-telemarketing movement"; and Gerald Waldron, a partner at a major

---

140 Janger & Schwartz, *supra* note 130, at 1242–44.

141 *Id.*

142 *Id.* at 1258–59.

143 As an example, the Telephone Consumer Protection Act (TCPA), 47 U.S.C. § 227(b)(1) (2000), provides incentives for individual plaintiffs to bring lawsuits. *See* Texas v. Am. Blastfax, Inc., 121 F. Supp. 2d 1085, 1090 (W.D. Tex. 2000); Kenro, Inc. v. Fax Daily, Inc., 962 F. Supp. 1162, 1166 (S.D. Ind. 1997).

144 47 U.S.C. § 227(b)(1).

145 This Article also advocates the creation of rights of action for state attorneys general, as well as the Federal Trade Commission and other federal agencies, to supplement private rights of action. As discussed later, this decentralized enforcement approach already exists in some privacy statutes.

Washington, D.C. firm whose partners asked him to intervene after his firm received a deluge of junk faxes.[146]

The economist Howard Demsetz once warned against the "nirvana approach"[147] — that is, he opposed certain kinds of unfair comparisons "between an ideal norm and an existing 'imperfect' institutional arrangement."[148] According to Demsetz, "those who adopt the nirvana viewpoint" seek to identify discrepancies between the ideal and the real in order to reject available alternatives.[149] In this light, this Article can be seen as avoiding multiple nirvana fallacies. On one hand, it rejects an initial nirvana viewpoint, which would be an idealized nonmarket approach to information privacy that shuns propertization on any terms. On the other hand, this Article also rejects a second nirvana viewpoint: an idealized market-based solution unaccompanied by legislation that structures the shape of property in personal information.[150] Indeed, some law already accompanies the market, and hence the issues are whether the current combination is the best one and, if not, how the law should structure the market.[151]

B. Privacy as Public Good: The Privacy Commons

The second objection to propertization of personal data is that it will neglect important social values that information privacy should advance. From this perspective, information privacy functions as a type of public good, like clean air or national defense.[152]

---

146 Regarding the "Erin Brockovich of the anti-telemarketing movement," see Ryan J. Foley, *Telemarket Foe, Discover Card Head to Court*, WALL ST. J., Dec. 12, 2003, at B1. For an account of the lawsuits against "junk" faxes, see Lisa Napoli, *Crusaders Against Junk Faxes Brandish Lawsuits*, N.Y. TIMES, Dec. 16, 2003, at C1. The Washington law firm of Covington & Burling successfully sued Fax.com for $2.25 million after receiving a thousand unwanted faxes in one day. *Id.* The Silicon Valley billionaire in question, Steve Kirsch, even has his own website devoted to this cause. *See* Junkfax.org, *Junkfax.org: Dedicated to Helping Stop Junk Faxes*, *at* http://www.junkfax.org (last visited Apr. 10, 2004).

147 Harold Demsetz, *Information and Efficiency: Another Viewpoint*, 12 J.L. & ECON. 1, 1 (1969) (emphasis omitted).

148 *Id.*

149 *Id.*

150 *Cf.* McGeveran, *supra* note 83, at 1834–42 (rejecting in the context of P3P software protocols any reliance on a "libertarian" privacy market).

151 *See* Robert Hale, *Coercion and Distribution in a Supposedly Non-Coercive State*, 38 POL. SCI. Q. 470 (1923).

152 For an earlier discussion of the "privacy commons," see Janger & Schwartz, *supra* note 130, at 1244; Schwartz, *supra* note 9, at 1690. The scholarly literature examining different aspects of the idea of the commons includes DAVID BOLLIER, SILENT THEFT: THE PRIVATE PLUNDER OF OUR COMMON WEALTH (2002); LAWRENCE LESSIG, THE FUTURE OF IDEAS: THE FATE OF THE COMMONS IN A CONNECTED WORLD (2001); Hanoch Dagan & Michael A. Heller, *The Liberal Commons*, 110 YALE L.J. 549, 568 (2001); Robert C. Ellickson, *Property in Land*, 102 YALE L.J. 1315, 1319–20 (1993); and Garrett Hardin, *The Tragedy of the Commons*, 162 SCIENCE 1243, 1247 (1968).

The traditional problem with relying on a property regime to supply a public good follows from two of the good's qualities — nonrivalrous consumption and nonexcludability. A privacy commons illustrates both of these aspects of public goods. If the purpose of information privacy is to provide anonymous and semi-anonymous areas for interaction, it will be difficult to exclude parties from the privacy commons once erected. Those who have provided their personal data for little or no compensation will still try to obtain the benefits of the privacy information space. Another possible analogy is a hypothetical reliance on competing national defense companies to protect the nation. As one law and economics textbook observes regarding nonexcludability, "[t]he attempt to distinguish those who have from those who have not subscribed to the private defense companies is almost certain to fail."[153] The example of national defense also illustrates the nonrivalrous nature of public goods — the provision of defense for one citizen does not entail a lack of security for other citizens. As a further example, when one person listens to a CD by the Beatles, there is not any less Beatles music available for the rest of us.[154] In a similar fashion, information privacy for one person in a privacy commons does not leave less for any other person. The argument that follows from nonrivalry and nonexcludability, then, is the traditional one that a functioning market may not provide an optimal supply of public goods.

As noted earlier, moreover, this analysis is also linked to a critique of the existing privacy market. Initially, it is important to separate out the strands of a sometimes intermingled discussion of the privacy market and the privacy commons. To do so, this section considers a joint report of two leading privacy advocacy groups, the Electronic Privacy Information Center (EPIC) and Junkbusters, as well as an exchange between John McCain and Jay Rockefeller at a Senate hearing.[155] The ultimate focus of this section will be to consider the public goods critique on its own terms.

The EPIC-Junkbusters report looks at the perils and promise of technological solutions to Internet privacy. It asserts that "negotiations [for data trade] would invariably disadvantage those who could not purchase sufficient privacy and would lead to a gradual decline in the

---

153 COOTER & ULEN, *supra* note 118, at 40.

154 *See id.*

155 ELEC. PRIVACY INFO. CTR. & JUNKBUSTERS, PRETTY POOR PRIVACY: AN ASSESSMENT OF P3P AND INTERNET PRIVACY (2000), http://epic.org/reports/prettypoorprivacy.html [hereinafter PRETTY POOR PRIVACY]; *Need for Internet Privacy Legislation: Hearing of the Senate Commerce, Sci., and Transp. Comm.*, 108th Cong. (July 11, 2001) [hereinafter *Senate Hearing*], LEXIS, Federal News Service File.

level of protection available to the general public."[156] This single sentence contains two critiques of personal data trade. First, it contains a market failure argument that fits comfortably with the analysis of the preceding section — as a consequence of failure in the privacy market, a reliance on data trade will stimulate a race to the bottom. Stated differently, this argument holds that due to shortcomings in the existing system of personal information trade, recourse to the market will drive down the overall level of privacy (by causing "a gradual decline in the level of protection") and leave us all worse off.

The second critique of data trade is that a reliance on data markets places poor people and others ("those who could not purchase sufficient privacy") at a disadvantage when they trade for privacy. The EPIC-Junkbusters report argues that privacy should be seen as a basic right whose level should not be different for rich and poor.[157] As Pamela Samuelson notes: "If information privacy is a civil liberty, it may make no more sense to propertize personal data than to commodify voting rights."[158] Thus, the interest in privacy is like the interest in receiving access to the electoral franchise, clean air, or national defense: it should not depend on socioeconomic status.

Another example of a public goods discussion comes from a hearing on Internet privacy held before the Senate Commerce Committee in 2001. Much of the hearing focused on the potential economic impact of privacy legislation on e-commerce companies. Senator John McCain, who adopted a market-oriented perspective, considered personal information a commodity. In his first question to a witness, for example, Senator McCain demanded: "[Y]ou state that polls have consistently shown that many Americans decline to engage in cyberspace transactions because of concerns about privacy. Why, if it is in the businesses's interest to improve privacy protections, do you think businesses aren't doing it?"[159] This question was, on one hand, about the extent of privacy market failure and the chances for market self-correction. Underlying it, on the other hand, is a notion that personal information is a commodity and that businesses will generally meet consumer's expectations regarding privacy.

At the same hearing, however, Senator Jay Rockefeller hinted at the need for a nonmarket approach to these issues. In a statement at the start of the hearing, Senator Rockefeller compared protecting the environment to safeguarding privacy.[160] Rockefeller commented that

---

156 PRETTY POOR PRIVACY, *supra* note 155.

157 *See id.* (stating that "individuals should not be required to negotiate or choose among Fair Information Practices").

158 Samuelson, *supra* note 4, at 1143.

159 *Senate Hearing*, *supra* note 155 (statement of Sen. John McCain).

160 *Id.* (statement of Sen. Jay Rockefeller).

protecting the environment was not always justifiable on economic terms — environmental regulations might sometimes cost jobs but are nonetheless still desirable. He warned his colleagues of a similar need to choose between economic and noneconomic perspectives in the area of information privacy: "Sometimes you have got to decide [whether] you are going to go this way [or] you are going to go that way."[161] Although safeguards for privacy might have a negative economic impact, in Rockefeller's view these protections would be justifiable for noneconomic reasons.[162] Senator Rockefeller deserves praise for identifying the division between market and nonmarket justifications for information privacy protection. Moreover, while he did not speak in terms of public goods, his language is reminiscent of this idea. A public good benefits all of society and is generally viewed as something that cannot be created through an unregulated market.

Scholarly writing about privacy also sometimes conceives of privacy as a social and not merely an individual good. Like clean air and national defense, the worth of information privacy accrues to society. Thus, Julie Cohen views privacy as promoting the development of both autonomous individuals and civil society.[163] She writes: "Information privacy . . . is a constitutive element of a civil society in the broadest sense of that term."[164] In a similar sense, I have argued that privacy is necessary for both "individual self-determination" and "democratic deliberation."[165] Based in part on civic republicanism, this conception views democracy as dependent on common participatory activities, reciprocal respect, and the need for consensus about political issues.[166] To borrow a phrase from Robert Post, the process at stake is the "creation of the autonomous self required by democratic citizenship."[167] In this conception, deliberative democracy requires limits on access to personal information because Americans will hesitate to engage in democratic self-rule should widespread and secret surveillance become the norm.[168]

---

161 *Id.*

162 *Id.*

163 Cohen, *supra* note 4, at 1423–28.

164 *Id.* at 1427–28.

165 Schwartz, *supra* note 9, at 1647–58.

166 *Id.*

167 Robert C. Post, *Defending the Lifeworld: Substantive Due Process in the Taft Court Era*, 78 B.U. L. REV. 1489, 1542 (1998). For additional development of these ideas, see Robert C. Post, *Between Democracy and Community: The Legal Constitution of Social Form*, *in* NOMOS XXXV: DEMOCRATIC COMMUNITY 163 (John W. Chapman & Ian Shapiro eds., 1993). For discussion of Post's privacy jurisprudence, see Schwartz, *supra* note 9, at 1667–70; and Paul M. Schwartz & William M. Treanor, *The New Privacy*, 101 MICH. L. REV. 2163, 2177–79 (2003) (reviewing JOHN GILLION, OVERSEERS OF THE POOR: SURVEILLANCE, RESISTANCE AND THE LIMITS OF PRIVACY (2001)).

168 Schwartz, *supra* note 9, at 1658–66.

Thus, many scholars perceive information privacy as benefiting and shaping society.[169] From this vantage point, information privacy can be seen as a commons that requires some degree of social and legal control to construct and then maintain. The privacy commons is a place created through rules for information exchange. It is a multidimensional privacy territory that should be ordered through legislation that structures anonymous and semi-anonymous information spaces. As I have written, "information privacy norms should create shifting, multidimensional data preserves that insulate personal data from different kinds of observation by different parties."[170]

From this perspective, propertization of personal information should be limited to the extent it undermines the privacy commons. This point is distinct from the market failure argument but, as this Article discusses later, is related to it: a negative result for the privacy commons can occur both under privacy market failure and under a functioning market for personal data trade.

Beyond the market failure critique, a second objection to propertization of personal data concerns a categorization of information privacy as a public good. Consider also, for example, the possibility that individuals may prove incapable of adequately valuing and managing property rights in information.[171] At first glance, this argument may seem to be no more than a paternalistic one. It certainly exceeds John Stuart Mill's "harm principle," which is the classic liberal concept that people are free to do as they wish, subject only to limits that prevent harm to others.[172] But based upon a belief in the privacy commons, skepticism about information property requires a better basis than paternalism. At this stage, this Article simply seeks to show that a traditional public goods argument can be used to cast doubt, albeit only partially, on the propertization of information.

---

[169] *See* Jeffrey H. Reiman, *Privacy, Intimacy and Personhood*, *in* PHILOSOPHICAL DIMENSIONS OF PRIVACY 300 (Ferdinand David Schoeman ed., 1984); Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087 (2002).

[170] Schwartz, *supra* note 9, at 1664–65.

[171] This argument has special resonance when considered in the high-tech contexts of the VeriChip, the wOzNet, distributed computing, and compensated telemarketing. Elsewhere, I have discussed the "blinking twelve" problem, in which difficulties in designing user interfaces and the resulting simplifications and glosses of complex privacy issues shift power to those who design the technology for data trade. Schwartz, *supra* note 5, at 754–55. The term "blinking twelve" is derived from Neal Stephenson's discussion of "the blinking 12:00" that appears on VCRs in living rooms throughout the United States because of individuals who are unable to program these devices to set the correct time. NEAL STEPHENSON, IN THE BEGINNING . . . WAS THE COMMAND LINE 67 (1999).

[172] JOHN STUART MILL, ON LIBERTY, ch. IV (David Bromwich & George Kateb eds., Yale Univ. Press 2003) (1859). For a brief discussion of the harm principle, see John A. Robertson, *Human Flourishing and Limits on Markets*, 95 MICH. L. REV. 2139, 2140 (1997) (book review).

The conception of the privacy commons and the idea that the benefits of privacy flow to broader society may initially seem elusive. In the context of information privacy, more is at stake than seclusion for *individual* pieces of data and *personal* benefits. If sound rules for the use of personal data are not established and enforced, society as a whole will suffer because people will decline to engage in a range of different social interactions due to concerns about use of personal information. A public good — the privacy commons — will be degraded.[173]

A few comparisons to traditional public goods may help to shed light on the concept of privacy as a public good. In the context of national defense, the public good consists of elements such as a standing army, a missile shield, or a radar system. The benefit for the public is a strong level of national defense. In the context of the environment, the public good consists of environmental devices, such as those placed on offending smokestacks to limit their pollution, as well as governmental officials at environmental protection agencies who carry out tasks such as monitoring pollution levels. The benefit for all is protection of the environment and limits on pollution. In the context of information privacy, the public good at stake is the privacy commons — a space for anonymous and semi-anonymous interactions. The privacy commons is created through legal and other restrictions on the availability of personal information. The benefit that accrues to the public from a privacy commons is a social order based on democratic deliberation and the capacity of individuals for self-governance.

While the public goods framework suggests that propertization may fail to supply the right amount of information privacy, it also points to potential shortcomings of a complete anti-property orientation regarding personal information. In the United States, many public goods are supplied with at least some recourse to the marketplace. For example, national defense has always been accompanied by the privatization of at least certain functions: private companies manufacture weapons, uniforms, and supplies for the military, and, more recently and controversially, they have managed logistics for the Pentagon during the conflicts in Afghanistan and Iraq.[174] Furthermore, environmental law has experimented with private trade in "pollution rights."[175] Likewise, democratic discourse, the core public good in the United States, has

---

[173] Consider how many New Yorkers were reluctant to make use of Central Park in the 1970s and 1980s because of safety concerns. During this period in New York City's history, this public good, a magnificent park in the middle of Manhattan, saw a drastic reduction in its value to the public.

[174] For a discussion of the outsourcing of military support and potential problems with it, see Anthony Bianco & Stephanie Anderson Forest, *Outsourcing War*, BUS. WK., Sept. 15, 2003, at 68.

[175] *See* POSNER, *supra* note 116, at 395; Laudon, *supra* note 5, at 98.

traditionally depended on privately owned media outlets.[176] A public goods perspective on information privacy thus does not preclude the propertization of personal data.

C. *Property and Free Alienability*

Finally, some information privacy scholars are skeptical of property in personal information due to the issue of alienability. In their view, once information is propertized, it will be difficult to limit an individual's right to sign away this interest. The free alienability argument builds on the market failure argument: property entails free alienability, and this inevitable link exacerbates weaknesses in existing markets for personal data exchange.

Thus, in expressing doubts about property interests in personal data, Pamela Samuelson argues: "It is a common, if not ubiquitous, characteristic of property rights systems that when the owner of a property right sells her interest to another person, that buyer can freely transfer to third parties whatever interest the buyer acquired from her initial seller."[177] In Samuelson's assessment, property connotes free alienability.[178] Samuelson views this proposition as so uncontestable that it barely requires elaboration; she does, however, include a footnote reference to a treatise that traces a public policy in favor of free alienability back to English law and the year 1290.[179]

If property automatically entails free alienability, however, the result may be deeply problematic for information privacy. As Samuelson also notes: "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."[180] She identifies two problems of significance. The first problem is one that this Article has already identified in the context of compensated telemarketing, namely the secondary use of personal data. Samuelson writes that "[a]n 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."[181] Free alienability thus prohibits an individual from limiting another party in the use or transfer of data. In other

---

176 A key reaffirmation by the Supreme Court of limits on state action flowing from the private nature of the media came in *Miami Herald Publishing Co. v. Tornillo*, 418 U.S. 241 (1974), which declared that a "right of reply" statute imposing enforced access to the press violated the First Amendment. *Id.* at 248. For a negative assessment of concentrated corporate control of the media, see ROBERT W. MCCHESNEY, RICH MEDIA, POOR DEMOCRACY (1999).

177 Samuelson, *supra* note 4, at 1138.

178 *Id.*

179 *See id.* at 1138 n.71 (citing ROGER A. CUNNINGHAM ET AL., THE LAW OF PROPERTY § 2.2, at 33–39 (1984)).

180 *Id.* at 1138.

181 *Id.*

words, an individual cannot restrict those property interests that he signs away.

The second problem following from free alienability is the difficulty of estimating an appropriate price for secondary uses of one's personal data. Samuelson predicts that an individual 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."[182] Personal information is, after all, subject to myriad uses, and, as Samuelson points out, the subsequent acquirors may value the data more highly. Indeed, to build on Samuelson's discussion and return to an earlier example in this Article, individuals must be able to value information about their privacy metadata, which are also likely to be traded. Moreover, if data sellers and buyers are left free to set the price for information sales, they will also be setting a price for violations — that is, the cost of taking data without permission.[183]

To her credit, Samuelson has identified a critical issue concerning the propertization of personal data, and this insight relates to certain normative consequences of free alienability. To the extent, moreover, that Samuelson explores the link between free alienability and property, her work can be read as objecting to any model for propertization of personal information that does not respond to the risks flowing from unfettered data trade.

A third and final anti-propertization argument rests on the very idea of free alienability, which is considered by many to be an inevitable aspect of property. This argument is, at least in part, a historical one — albeit one based on an incomplete reading of the record. Samuelson, for example, bases the link between property and free alienability on the historical path of property regimes. Samuelson adopts the classic view of property frequently associated with Blackstone, who defined property as a "sole and despotic dominion . . . over the external things of the world."[184] Carol Rose has notably termed this conception of property the "Exclusivity Axiom."[185] This conception has even filtered into the popular debate surrounding information trade, in which the right to trade one's personal information is viewed

---

182 *Id.*

183 This Article prefers, in contrast, that legislation set damages collectively. *See infra* section III.A.4.

184 2 WILLIAM BLACKSTONE, COMMENTARIES ON THE LAWS OF ENGLAND 2 (facsimile ed. 1979) (1766).

185 Carol M. Rose, *Canons of Property Talk, or, Blackstone's Anxiety*, 108 YALE L.J. 601, 603 (1998). Rose notes that the historical basis for this view "is far from self-evident, and . . . was even less self-evident when Blackstone wrote." *Id.* She points to "earlier medieval traditions in which property ownership had been hemmed in by intricate webs of military and other obligations; . . . family ties encapsulated in such devices as the entailed fee; and . . . the general neighborly responsibilities of riparian and nuisance law." *Id.*

as an inexorable part of the underlying entitlement. As this Article has already noted, such reasoning can be restated in the following terms: "If you want to sell your personal data, do it. If you don't want to sell it, don't do it."

Yet this conception of property is based on an incomplete reading of Blackstone. Property can also take the form of incomplete interests and, just as importantly, can serve to structure social relationships. Blackstone was certainly aware of the latter point. For example, in his discussion of common law property, Blackstone carefully notes how property in land during the feudal era was a means of structuring not merely the ownership of the lord over his land, but also the relationship of the lord to his vassal or tenant. In addition to paying an oath of fealty to the lord, the tenant, "openly and humbly kneeling," would pay the lord homage, promising to follow the lord to "his courts in time of peace; and in his armies or warlike retinue, when necessity called him to the field."[186] Therefore, according to Blackstone, property is also a way of structuring social relations. Rose agrees that Blackstone goes beyond the Exclusivity Axiom, which she faults on its own terms because it has the potential "to overstate the case, concealing the interactive character of property and giving an inappropriately individualistic patina to this most profoundly sociable of human institutions."[187]

The role of alienability in property has always been more complex than the Exclusivity Axiom implies. To use a modern example, one can point to intellectual property as an illustration of how property frequently conveys less than "sole and despotic dominion" over a thing. Modern copyright law provides statutory inalienability for individual authors, permitting them to terminate any transfer of a copyright interest after a stated period of years.[188] The Second Circuit recently explained this property right in a case involving the Captain America character; the court declared that this interest gives "authors (or if deceased, their statutory heirs) an inalienable right to terminate a grant in copyright fifty-six years after the original grant notwithstanding any agreement to the contrary."[189] More generally, copyright law is premised on numerous divisible interests in a given piece of underlying in-

---

[186] 2 BLACKSTONE, *supra* note 184, at 53–54.

[187] *Id.* at 631–32.

[188] *See* 17 U.S.C.A. §§ 203(a), 304(c) (West 1996 & Supp. 2003).

[189] Marvel Characters, Inc. v. Simon, 310 F.3d 280, 282 (2d Cir. 2002) (quoting 17 U.S.C. § 304(c)(3), (5) (2000)) (internal quotation marks omitted). For a discussion of the inalienability of the termination right, see ROGER E. SCHECHTER & JOHN R. THOMAS, INTELLECTUAL PROPERTY § 8.4, at 159–65 (2003).

tellectual property; this area of law is therefore clear in its rejection of the Exclusivity Axiom.[190]

For Rose, the choice of metaphor becomes critical as one seeks to understand the nature of property. She writes: "The very notion of property as exclusive dominion is at most a cartoon or trope, as Blackstone himself must have known."[191] Correspondingly, the idea that free alienability is an inexorable aspect of information-property is also a problematic cartoon. In particular, a belief in free alienability of personal information may encourage advocacy of only rearguard policies — policies that seek to block data trade. The general idea would be that the fewer the data exchanges, the better — nonpropertized personal information may be more likely to remain uncirculated. However, such a stance at best merely locks in the current level of information privacy in the United States; the irony in such a stance is that most privacy advocates generally view this level as inadequate.[192]

Restrictions on propertization have also been made at other moments in history for essentially conservative purposes. In a classic law review article, *Property and Sovereignty*, Morris Cohen noted in 1927 that English law was only starting to remove the impediments to trade in land that had been established during the feudal period.[193] These restrictions had long played a role "in the national life of England" because the modernization of property law would make land more marketable and would undercut the power of the traditional aristocracy.[194] Cohen writes: "Once land becomes fully marketable, it can no longer be counted to remain in the hands of the landed aristocratic families; and this means the passing of their political power and the end of their

---

190 Thus, copyright is subject to notable limitations on exclusive rights, *see* 17 U.S.C.A. §§ 107–115 (West 1996 & Supp. 2003), including a compulsory license for nondramatic musical works, *see id.* § 115. Moreover, the underlying interest in copyright itself terminates after a stated period. *See id.* §§ 301–305. The constitutional implications of this aspect of copyright have been the subject of important litigation and scholarly debate. *See generally* Paul M. Schwartz & William Michael Treanor, Eldred *and* Lochner*: Copyright Term Extension and Intellectual Property as Constitutional Property*, 112 YALE L.J. 2331 (2003).

191 Rose, *supra* note 185, at 631.

192 For a sector-by-sector assessment of American privacy law, see SCHWARTZ & REIDENBERG, *supra* note 9. The European perception that a low level of privacy protection exists in the United States has led to high-level negotiations between the European Union and the United States to establish "safe harbor" procedures to allow continuing international data transfers. *See* U.S. Dep't of Commerce, *Welcome to the Safe Harbor*, *at* http:www.export.gov/safeharbor (last visited Apr. 10, 2004). For background on European and U.S. privacy law, see Paul M. Schwartz, *European Data Protection Law and Restrictions on International Data Flows*, 80 IOWA L. REV. 471 (1995). For a recent journalistic discussion of the leading role played by European privacy law, see David Scheer, *Europe's New High-Tech Role: Playing Privacy Cop to the World*, WALL ST. J., Oct. 10, 2003, at A1.

193 Morris R. Cohen, *Property and Sovereignty*, 13 CORNELL L.Q. 8 (1927).

194 *Id.* at 8.

control over the destinies of the British empire."[195] Cohen here highlights the fact that exchanges of property can alter the status quo, for better or for worse.

Similarly, trade in information property can also lead to change, a consequence which may have contributed to privacy scholars' nervousness about this trend. The change about which privacy scholars may be worried is, needless to say, quite different from the social change and concomitant loss of wealth and status about which the landed aristocrats of England were once concerned. Instead, privacy scholars are likely worried that increased data trade will increase the circulation of personal data and thus create new harms to individuals. It is unclear, however, whether greater participation by individuals in personal data trade will necessarily also increase the circulation of personal data, which, as this Article's Part I has demonstrated, is an already well-established phenomenon. Moreover — and this point provides our transition to Part III — once one conceives of property as including restrictions on alienability, data trade becomes less menacing to privacy.

III. TOWARD A MODEL OF PROPERTIZED PERSONAL INFORMATION

Having evaluated various grounds for suspicion of personal data trade, this Article now presents five critical elements of a model of propertized personal information that responds to these concerns. Many of the reservations that scholars have with applying a property regime to personal data may be traced to fear of an unadorned Blackstonian conception in which individual control over personal information is an all-or-nothing proposition. In response, I suggest that the understanding of property as a bundle of interests rather than despotic dominion over a thing helps frame a viable system of rights with respect to personal data. Moreover, these property interests are to be shaped through legal attention to five areas: inalienabilities, defaults, a right of exit, damages, and institutions. A key element of this model is the employment of *use-transferability restrictions* in conjunction with an *opt-in default*. This Article calls this model "hybrid inalienability" because it allows individuals to share, as well as to place limitations on, the future use of their personal information. The proposed hybrid inalienability follows personal information through downstream transfers and limits the negative effects that result from "one-shot" permission to all personal data trade.

---

[195] *Id.* at 12. As Cohen argued, this policy was based on the belief (which Cohen appears to have shared) that "continued leadership by great families cannot be as well founded on a money as a land economy." *Id.*

A. The Five Elements of Property in Personal Information

As noted above, one dominant property metaphor is the Blackstonian idea of "sole and despotic dominion" over a thing. An equally dominant metaphor is the idea of property as a "bundle of sticks." This idea, as Wesley Hohfeld expressed it, relates to the notion that property is "a complex aggregate" of different interests.[196] There are distinguishable classes of jural relations that relate to a single piece of property; indeed, a person's ability to possess or do something with a single stick in the bundle can be "strikingly independent" of the person's relation to another stick.[197]

This Article's aim, then, is to disaggregate, or "unpack," the elements of a model of personal information configured as property. It attempts to show how propertized personal information can be shaped to respond to privacy market failure and the need for a privacy commons. As Hanoch Dagan argues, "property is an artifact, a human creation that can be, and has been, modified in accordance with human needs and values."[198] Legal and social construction of any given form of property seeks to reach certain policy goals, and this Article explicitly explores these aims as well as possible problem areas.

1. *Inalienabilities.* — Propertized personal information requires the creation of inalienabilities to respond to the problems of market failure and to address the need for a privacy commons. According to Susan Rose-Ackerman's definition, an "inalienability" is "any restriction on the transferability, ownership, or use of an entitlement."[199] As this definition makes clear, inalienabilities may consist of separate kinds of limitations on a single entitlement.[200] In the context of personal data trade, a single *combination* of these inalienabilities proves to be of greatest significance — namely, a restriction on the use of personal data combined with a limitation on their transferability. This Part first analyzes this combination and then discusses why this hybrid inalienability should include a recourse to defaults.

---

196 Wesley Newcomb Hohfeld, *Fundamental Legal Conceptions as Applied in Judicial Reasoning*, 26 YALE L.J. 710, 746 (1917).

197 *Id.* at 733–34, 747. Scholars have expressed views for and against the "bundle of sticks" approach to property. *See* Peter Benson, *Philosophy of Property Law*, *in* THE OXFORD HANDBOOK OF JURISPRUDENCE & PHILOSOPHY OF LAW 752, 771 (Jules Coleman & Scott Shapiro eds., 2002) (arguing that the "incidents" of property are "fully integrated and mutually connected"); Hanoch Dagan, *The Craft of Property*, 91 CAL. L. REV. 1518, 1558–70, (2003) (arguing that the "bundle metaphor" must coexist with the conception of property as forms); A.M. Honoré, *Ownership*, *in* OXFORD ESSAYS IN JURISPRUDENCE 107, 108–34 (A.G. Guest ed., 1961) (discussing the "standard incidents" of ownership).

198 Dagan, *supra* note 197, at 1532.

199 Rose-Ackerman, *supra* note 6, at 931.

200 *See id.*; *see also* Susan Rose-Ackerman, *Inalienability*, *in* 2 THE NEW PALGRAVE DICTIONARY OF ECONOMICS AND THE LAW, *supra* note 40, at 268.

Before turning to these two issues, however, it is important to note that propertized personal information, like all property, is necessarily subject to more general limitations on account of the public interest. These limitations, in turn, take certain uses of information entirely outside of the realm of property.[201] For example, law enforcement access to personal data should not be structured through recourse to a propertized model in which police are obliged to bid for access to information.[202] Likewise, and more generally, the government's acquisition and use of personal data should not be subject to eminent domain or Takings Clause jurisprudence. Rather, mandatory or immutable rules for data access and privacy are necessary. Other similar limits on propertization may become appropriate when the media obtains personal data; in general, the First Amendment serves as a strong device for removing personal data from the realm of private negotiations and increasing their availability to the public.[203] It is important to note that the focus of this Article is *not* on these mandatory legal requirements that remove personal data entirely from the realm of private negotiations.[204] Instead, this Article focuses on those use and transferability restrictions that allow personal data to remain at least partially propertized.

As suggested earlier, these restrictions must respond to concerns about private market failure and contribute to the creation of a privacy commons. Regarding privacy market failure, both downstream data use and subsequent transfers of personal information may exacerbate market shortcomings. This Article has discussed how a variety of devices and systems that commodify information lead to downstream uses and onward transfers.[205] For example, the VeriChip and the wOzNet generate tracking data, and this information is likely to be traded and shared by companies that collect it. Distributed computing in the form of spyware and adware causes computers to send personal data to a remote site, which can share this information with other entities. Finally, compensated telemarketing may lead not only to calls at

---

[201] For a discussion of such immutable restrictions on privacy control, see Paul M. Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815, 827–28 (2000).

[202] *See* Paul M. Schwartz, *Privacy and the Economics of Personal Health Care Information*, 76 TEX. L. REV. 1, 57–58 (1997) (suggesting that the privacy interest in protecting personal health data should only be overridden by "significant social need" such as that of law enforcement).

[203] For discussion of the reach of the First Amendment in the context of personal data, see Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right To Stop People from Speaking About You*, 52 STAN. L. REV. 1049 (2000); and Paul M. Schwartz, *Free Speech vs. Information Privacy: Eugene Volokh's First Amendment Jurisprudence*, 52 STAN. L. REV. 1559 (2000).

[204] *See* Schwartz, *supra* note 201, at 827 (noting that "the State and private entities remove certain kinds of personal data use entirely from the domain of two-party negotiations").

[205] *See supra* p. 2075.

the stated price, but also to additional use of an individual's personal data, including privacy metadata.

Beyond downstream data use and subsequent transfers, free alienability is problematic because information asymmetries about data collection and current processing practices are likely to resist easy fixes. The ongoing difficulties in providing understandable "privacy notices" in both online and offline contexts illustrate the challenges of supplying individuals with adequate information about privacy practices.[206] As a result, there may be real limits to a data trade model under which consumers have only a single chance to negotiate future uses of their information. To limit the negative results of this one-shot permission for data trade, this Article proposes a model that combines limitations on use with limitations on transfer. Under this approach, property is an interest that "runs with the asset";[207] the use-transferability restrictions follow the personal information through downstream transfers and thus limit the potential third-party interest in it.

The model proposed here not only addresses concerns about private market failure, but also supports the maintenance of a privacy commons. As stated above, problems for the privacy commons can arise regardless of whether a market failure problem exists. Nevertheless, because the coordination necessary to establish a functioning privacy commons may prove difficult to achieve, market failure may have especially pernicious results in this context. As Rose-Ackerman has stated elsewhere: "The coordination problem arises most clearly in the case of pure public goods . . . consumed in common by a large group."[208] As the example of PITs and PETs illustrates, the market has already fallen short in providing technological mechanisms for coordinating individual wishes for information privacy.[209] Should market failure continue, the present circumstances are unlikely to yield an optimal privacy commons.

Yet even if market failure ceases to be a problem, a well-functioning privacy market may fail to create public goods. Rose-Ackerman provides an illuminating example of this proposition in her discussion of the problem of settling a new geographic region: "Everyone is better off if other people have settled first, but no one has an in-

---

[206] To be sure, lessons from behavioral economics suggest ways to improve the manner in which consumers are given the information on which they will make their decisions. *See* Janger & Schwartz, *supra* note 130, at 1242–44 (drawing insight from behavioral economics research about consumers' bounded rationality and the "framing effect" on decisionmaking).

[207] Hansmann & Kraakman, *supra* note 7, at S374 (internal quotation marks omitted).

[208] Rose-Ackerman, *supra* note 6, at 939.

[209] *See supra* pp. 2079–80.

centive to be the first settler."[210] In this context, the market might lead to real estate speculation without any person wanting to move first to the new area. As a further example, a market in private national defense may induce some individuals to purchase protective services, but it may fail to generate an adequate level of nationwide protection.[211] In the privacy context, a market may cause people to sell personal information or to exchange it for additional services or a lower price on products, but it may not necessarily encourage coordination of individual privacy wishes and the creation of a privacy commons.

This Article proposes that the ideal alienability restriction on personal data is a hybrid one based partially on the Rose-Ackerman taxonomy. This hybrid consists of a use-transferability restriction plus an opt-in default. In practice, it would permit the *transfer* for an initial category of *use* of personal data, but only if the customer is granted an opportunity to block further transfer or use by unaffiliated entities. Any further use or transfer would require the customer to opt in — that is, it would be prohibited unless the customer affirmatively agrees to it.

As an initial example concerning compensated telemarketing, a successful pitch for Star Trek memorabilia would justify the use of personal data by the telemarketing company and the transfer of it both to process the order and for other related purposes. Any outside use or unrelated transfers of this information would, however, require obtaining further permission from the individual. Note that this restriction limits the alienability of individuals' personal information by preventing them from granting one-stop permission for all use or transfer of their information. A data processor's desire to carry out further transfers thus obligates the processor to supply additional information and provides another chance for the individual to bargain with the data collector.

This use-transferability restriction also reinforces the relation of this Article's model to ideas regarding propertization. The use-transferability restriction runs with the asset; it follows the personal information downstream.[212] Or, to suggest another metaphor, property enables certain interests to be "built in"; these interests adhere to the property.

To ensure that the opt-in default leads to meaningful disclosure of additional information, however, two additional elements are needed.

---

[210] Rose-Ackerman, *supra* note 6, at 940.

[211] *See* COOTER & ULEN, *supra* note 118, at 40–41.

[212] *Cf.* Hansmann & Kraakman, *supra* note 7, at S379 ("A tenant who rents a parcel of land . . . has a property right in the land if she can enforce her rights in the land, not just against the landlord who originally granted the lease, but also against other persons to whom the landlord subsequently transfers his own interest in the land.").

First, the government must have a significant role in regulating the way that notice of privacy practices is provided. As noted above, a critical issue will be the "frame" in which information about data processing is presented. The FTC and other agencies given oversight authority under the Gramm-Leach-Bliley Act of 1999[213] (GLB Act) are already engaged in working with banks, other financial institutions, and consumer advocacy groups to develop acceptable model annual "privacy notices."[214]

Second, meaningful disclosure requires addressing what Henry Hansmann and Reinier Kraakman term "verification problems."[215] Their scholarship points to the critical condition that third parties must be able to verify that a given piece of personal information has in fact been propertized and then identify the specific rules that apply to it. As they explain, "[a] verification rule sets out the conditions under which a given right in a given asset will run with the asset."[216] In the context of propertized personal information, the requirement for verification creates a role for nonpersonal metadata, a tag or kind of barcode, to provide necessary background information and notice.[217]

A survey of existing statutes finds that the law employs at least some of the restrictions and safeguards proposed in the model. In particular, certain transferability and use restrictions already exist in information privacy statutes. The Video Privacy Protection Act of 1988[218] (Video Act) contains one such limitation: it imposes different authorization requirements depending on the planned use or transfer of the data.[219] Moreover, this statute's transferability restriction requires a "video tape service provider" to obtain in advance a consumer's permission each time the provider shares the consumer's video sale or rental data with any third party.[220] This rule restricts data trade by preventing consumers from granting permanent authorization to all transfers of their information.[221]

---

213 Pub. L. No. 106-102, 113 Stat. 1338 (codified in scattered sections of 12 and 15 U.S.C.).

214 *Id.* § 501(a) (codified at 15 U.S.C. § 6801(a) (2000)). The GLB Act also requires the oversight agencies to establish "appropriate standards" for data security and integrity. *Id.* § 501(b) (codified at 15 U.S.C. § 6801(b)); *see also* FED. TRADE COMM'N, GETTING NOTICED: WRITING EFFECTIVE FINANCIAL PRIVACY NOTICES 1–2 (2002), *available at* http://www.ftc.gov/bcp/conline/pubs/buspubs/getnoticed.pdf.

215 Hansmann & Kraakman, *supra* note 7, at S384.

216 *Id.*

217 *See infra* section III.A.5.

218 18 U.S.C. § 2710 (2000).

219 *Id.* § 2710(b).

220 *Id.*

221 In addition to its block on permanent authorization for information disclosure, the Video Act dilutes this limit with an opt-out that allows disclosure of a certain subset of information to third parties unless the customer objects. *Id.* § 2710(b)(2)(D)(ii). Unfortunately, the consumer information covered by this opt-out is quite extensive. First, this set of exempted information in-

A second statute incorporating use and transferability limitations is the Driver's Privacy Protection Act of 1994[222] (DPPA), which places numerous restrictions on the ability of state departments of motor vehicles to transfer personal motor vehicle information to third parties.[223] The statute's general rule is to restrict use of these data to purposes relating to regulation of motor vehicles.[224] Both the Video Act and the DPPA respond to the flaws inherent in one-time permanent authorization under conditions of market failure. Moreover, combined with a default rule, this approach could have the additional positive effect of forcing the disclosure of information about data transfer and use to the individuals whose personal information is at stake. This Article now turns to the default element of its model for information property.

2. Defaults. — This Article has discussed how a variety of devices and systems that commodify information give rise to additional uses and transfers of personal data. To limit the negative results of one-shot permission for data trade, it has proposed a combined use-transfer. This Article supports the use of defaults as a further safeguard to promote individual choice. This Article prefers an opt-in default because it would be information-forcing — that is, it would place pressure on the better-informed party to disclose material information about how personal data will be used. This default promises to force the disclosure of hidden information about data-processing practices. Furthermore, this Article advocates that such a default should generally be mandatory to further encourage disclosure — that is, the law should bar parties from bargaining out of the default rule. The strengths of the proposed model can be illustrated through a considera-

---

cludes the names and addresses of customers. Video stores can release the names and addresses of their customers unless the customer has taken the affirmative step of opting out. Second, the "subject matter" of video materials may be released, subject to the opt-out with the additional restriction that "the disclosure is for exclusive use of marketing goods and services directly to the consumer." *Id.* The Video Act here draws a distinction between the subject matter of videos and their titles; the latter can be released only with explicit permission.

The exceptions to the Video Act's general ban on one-time permanent authorization for transfers of information are poorly structured. First, names and addresses are releasable for any purposes unless a customer takes affirmative action and opts out. Thus, a video store can market lists of the names and addresses of any of its customers who have not asked to be excluded from such lists. Second, the statutory distinction between the "subject matter" and "title" of videos creates another significant loophole. Consider this example: Under the Video Act, unless a consumer has taken specific action to opt out of these transfers of information, a video store can inform a third party who plans direct marketing that a consumer has rented "James Bond films" (the "subject matter" of videos). The Video Act prevents the video store only from letting direct marketers know that the customer rented *From Russia with Love*, *Thunderbolt*, *Dr. No*, or any other specific film.

222 18 U.S.C. §§ 2721–2725.

223 For a discussion of the DPPA, see PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW 32–34 (Supp. 1998).

224 *See* 18 U.S.C. § 2721(b).

tion of the design and the effects, both positive and negative, of both a long-established German statute and a recent American statute.

German law recognizes the need for mandatory protection of certain privacy interests. The Federal Data Protection Law (*Bundesdatenschutzgesetz*, or BDSG) not only assigns wide-ranging personal rights to the "data subject" but also makes certain of them "unalterable."[225] As the leading treatise on the BDSG states, this statute prevents individuals from signing away certain personal interests in any kind of "legal transaction" (*Rechtsgeschäft*).[226] The BDSG does so to protect an individual's interest in "informational self-determination," a fundamental right that the German Constitutional Court has identified in the Basic Law (*Grundgesetz*), the German constitution.[227]

In the United States, the GLB Act removed legal barriers blocking certain transactions between different kinds of financial institutions and provided new rules for financial privacy.[228] These privacy rules require financial entities to mail annual privacy notices to their customers. Moreover, consistent with the model that I have proposed, the GLB Act incorporates a transferability restriction.[229] Unlike the proposed default, however, the Act merely compels financial entities to give individuals an opportunity to opt out, or to indicate their refusal, before their personal data can be shared with unaffiliated entities.[230] Yet the GLB Act does not have a true information-forcing effect because it chooses an opt-out rule over an opt-in rule.

An assessment of the GLB Act supports the proposition that a use-transferability restriction, combined with a default regime, can lead to optimal information-sharing. Consistent with the privacy model proposed by this Article, the GLB Act obligates the relatively better-informed parties — financial institutions — to share information with

---

[225] Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung (Bundesdatenschutzgesetz) § 6, v. 27.1.1977 (BGBl. I S.201), *reprinted in* v. 14.1.2003 (BGBl. I S.66).

[226] Otto Mallman, *§ 6*, *in* KOMMENTAR ZUM BUNDESDATENSCHUTZGESETZ 545–47 (Spiros Simitis ed., 5th ed. 2003) [hereinafter BDSG TREATISE].

[227] For the critical case in which the Constitutional Court recognized this fundamental right, see BVerfGE 65, 1 (43–44). This decision has inspired an outpouring of academic commentary. *See, e.g.*, Paul Schwartz, *The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination*, 37 AM. J. COMP. L. 675, 686–92 (1989); Hans-Heinrich Trute, *Verfassungsrechtliche Grundlagen*, *in* HANDBUCH DATENSCHUTZ: DIE NEUEN GRUNDLAGEN FÜR WIRTSCHAFT UND VERWALTUNG 156, 162–71 (Alexander Rossnagel ed., 2003); Spiros Simitis, *Das Volkszählungsurteil oder der Lange Weg zur Informationsaskese*, 83 KRITISCHE VIERTELJAHRESSCHRIFT FÜR GESETZGEBUNG UND RECHTSWISSENSCHAFT 359, 368 (2000); Spiros Simitis, *Einleitung*, *in* BDSG TREATISE, *supra* note 226, at 1, 14–24.

[228] These protections are found in Title V of the GLB Act. *See* Gramm-Leach-Bliley Act, Pub. L. No. 106-102, §§ 501–527, 113 Stat. 1338, 1436–50 (1999) (codified at 15 U.S.C. §§ 6821–6827 (2000)).

[229] *See id.* § 502 (codified at 15 U.S.C. § 6802).

[230] *See id.* § 502(a) (codified at 15 U.S.C. § 6802(a)).

other parties. Also, it sets this obligation to inform as a mandatory default: the GLB requires financial institutions to supply annual privacy notices to their customers.[231] A client cannot trade the notice away for more products and services or even opt not to receive the notices because she does not want to receive more paper. Even if many individuals do not read privacy notices, a mandatory disclosure rule is crucial to the goal of creating a critical mass of informed consumers.[232]

Unfortunately, the GLB Act's promise of informed participation in privacy protection has yet to be realized, due in large part to the relative weakness of its default rule, which allows information-sharing if consumers do not opt out. The opt-out rule fails to impose any penalty on the party with superior knowledge — the financial entity — should negotiations over further use and transfer of data fail to occur. Under the Act, information can be shared with unaffiliated parties unless individuals take the affirmative step of informing the financial entity that they refuse to allow the disclosure of their personal data.[233] In other words, the GLB Act places the burden of bargaining on the less-informed party, the individual consumer. Examination of the often confusing or misleading nature of GLB Act privacy notices confirms this Article's doubts about the efficacy of an opt-out rule:[234] an opt-out rule creates incentives for financial entities to draft privacy notices that lead to consumer inaction.[235]

On a more positive note, the agencies given oversight authority by the GLB Act have engaged in a major effort to find superior ways of providing information through privacy notices.[236] These agencies, the

---

231 *See id.*

232 On the relative lack of consumer interest in these notices, see Janger & Schwartz, *supra* note 130, at 1230–31.

233 *See* Gramm-Leach-Bliley Act § 502 (codified at 15 U.S.C. § 6802).

234 *See* Janger & Schwartz, *supra* note 130, at 1231 (citing evidence that "[n]ot only are privacy notices difficult to understand, but they are written in a fashion that makes it hard to exercise the opt-out rights that the GLB Act mandates"); *see also* Sovern, *supra* note 119, at 1085 (noting how "[c]ompanies can increase consumers' transaction costs in opting out").

For an argument defending these opt-out provisions, see Michael E. Staten & Fred H. Cate, *The Impact of Opt-In Privacy Rules on Retail Credit Markets: A Case Study of MBNA*, 52 DUKE L.J. 745 (2003). Among the shortcomings of Staten and Cate's article is that, although it considers negative impacts of data-use restrictions, it fails to consider the positive economic effects that flow from such restrictions. *See id.* at 769–83. For an attempt to consider such positive effects, see Daniel J. Solove, *The Virtues of Knowing Less*, 53 DUKE L.J. (forthcoming 2004).

235 Ayres and Funk miss this point about how opt-in defaults will force disclosure of information about data-processing practices. *See* Ayres & Funk, *supra* note 11, at 115–16. However, Ayres deserves recognition as one of the coauthors responsible for developing the idea of information-forcing defaults. *See generally* Ian Ayres & Robert Gertner, *Filling Gaps in Incomplete Contracts: An Economic Theory of Default Rules*, 99 YALE L.J. 87 (1989); Ian Ayres & Robert Gertner, *Majoritarian vs. Minoritarian Defaults*, 51 STAN. L. REV. 1591 (1999); Ian Ayres & Robert Gertner, *Strategic Contractual Inefficiency and the Optimal Choice of Legal Rules*, 101 YALE L.J. 729 (1992).

236 *See supra* note 214 and accompanying text.

most prominent of which is the FTC, have engaged both privacy advocacy organizations and the financial services industry in a discussion of the design of short forms that will attract greater public attention and convey information in a clearer fashion.[237]

An opt-in rule is therefore an improvement over an opt-out rule. More specifically, an opt-in regime improves the functioning of the privacy market by reducing information asymmetry problems. An opt-in rule forces the data processor to obtain consent to acquire, use, and transfer personal information. It creates an entitlement in personal information and places pressure on the data collector to induce the individual to surrender it. In addition to having a positive impact on the privacy market, the opt-in regime also promotes social investment in privacy.

However promising the opt-in default regime may be, it still has some weaknesses and thus is only one of several elements in the propertization scheme this Article proposes. The opt-in regime's first weakness is that many data-processing institutions are likely to be good at obtaining consent on their terms regardless of whether the default requires consumers to authorize or preclude information-sharing. Consider financial institutions, the subject of Congress's regulation in the GLB Act. These entities provide services that most people greatly desire. As a result, a customer will likely agree to a financial institution's proposed terms, if refusing permission to share information means not getting a checking account or a credit card. More generally, consumers are likely to be far more sensitive to price terms, such as the cost of a checking account, than to nonprice terms like the financial institution's privacy policies and practices. Some examples will illustrate this point about consumers' heavy emphasis on price terms.

In other contexts, evidence of consumers' focus on price terms can be found in the popularity of the marketing scheme in which companies initially quote low prices but then smuggle additional and hidden charges into consumers' final bills.[238] In a privacy context, consumers' emphasis on price terms is seen in the continuing prevalence of spyware, which, as this Article has discussed, can accompany "free" software, computer games, or songs. As the *New York Times* has noted, "free isn't what it used to be."[239] Although the downloaded products seem to come without cost, the spyware manufacturers extract value from their users in other ways, frequently without the computer users' knowledge. Thus, because price terms are so effective in inducing

---

[237] *See* FED. TRADE COMM'N, *supra* note 214, at 1–2.

[238] *See* Emily Thornton, *Fees! Fees! Fees!*, BUS. WK., Sept. 29, 2003, at 99, 99.

[239] John Schwartz, *When Free Isn't Really Free*, N.Y. TIMES, Nov. 23, 2003, § 3 (Money & Business), at 1.

consumers to opt into information-sharing, defaults may not effectively promote bargaining about critical issues.

For this reason, sophisticated consumer protection regimes do not rely exclusively on information-forcing defaults. Used car "lemon laws," for example, provide some information-forcing through standardized language in warranties and also require used car dealers to provide a written minimum guarantee of the used automobiles for a short period of time.[240] These laws also require that commercial sellers of used cars take such vehicles back from buyers if flaws persist after several attempts at repair.[241] Because better information may not cure market failure, this Article also proposes bolstering the effect of information-forcing defaults through use-transfer restrictions and other protection mechanisms such as a right to exit.

One objection to this model may be, however, that use-transferability restrictions with an opt-in requirement may create such a powerful disincentive for companies that they would deter desirable information transactions. Put differently, some may fear that the costs of approaching customers to request "downstream" permission may be higher than the extractable value of the underlying personal data. In an article from 1978, Richard Posner makes a related argument in pointing to transaction costs as a justification for generally allowing sale of personal data without customer approval.[242] With reference to the specific example of a magazine and its subscription list, Posner asserts that "the costs of obtaining subscriber approval [for sale of their names] would be high relative to the value of the list" for the periodical.[243] The assignment to publishers of exploitation rights regarding subscriber data is desirable, Posner argues, because it reaches an efficient result without subjecting the parties to costly negotiations that would reduce the overall efficiency of their exchange.[244]

---

[240] *See* N.Y. GEN. BUS. LAW § 198 (McKinney 1998 & Supp. 2004). For an introduction to New York's law, see Martha M. Post, Comment, *New York's Used-Car Lemon Law: An Evaluation*, 35 BUFF. L. REV. 971 (1986).

[241] *See, e.g.*, N.Y. GEN. BUS. LAW § 198-b(c). These statutes generally provide for strong rights for the consumer when a dealer fails to fulfill his legal obligations. *See id.*

[242] *See* Richard Posner, *John A. Sibley Lecture: The Right of Privacy*, 12 GA. L. REV. 393, 394–95 (1978).

[243] *Id.* at 398. Posner adds: "If, therefore, we believe that these lists are generally worth more to the purchasers than being shielded from possible unwanted solicitations is worth to the subscribers, we should assign the property right to the magazine; and the law does this." *Id.* This sentence begs the question, of course, how one is to compare the market value of information once aggregated with the individual value of the information to each consumer. To be sure, the market value of each discrete piece of data is smaller than the total value of the aggregated subscriber list. But it is unclear whether the price that any individual would charge for a discrete piece of personal data is high or low, or how any consumer would measure personal harms or benefits likely to follow from release of the data.

[244] *See id.*

There is good reason, however, for skepticism about these objections. First, the extractable value from personal data is far from being so limited as to make it financially unfeasible to approach customers for opt-in permission. The trafficking of personal data already constitutes a robust, multimillion-dollar market.[245] Direct marketing lists sort individuals into highly specific demographic slices, including Hispanic families with children; Asian-American mail-order buyers; women who buy wigs; gamblers; male buyers of fashion underwear; and political-minded Christians.[246] A standard pricing mechanism in the direct-marketing industry is to demand eighty dollars per thousand names.[247] Rather than worrying about limited extractable value, one should be concerned about an overinvestment of marketers in reaching individuals who are uninterested in being solicited and an underinvestment in developing efficient, low-cost ways to garner opt-in permissions.

Second, people will opt in if given the right incentives and information. As a general example, most of us already have opted into certain listservs or to the receipt of information from companies and organizations in which we are interested. Giving such assent can be as simple as clicking a box on a website or clicking a hypertext link to create a form e-mail. Moreover, people are more likely to opt in if a right of exit is reserved. The ability to change one's mind and refuse further use and transfers of personal information allows one to test the waters knowing that a choice is not permanent.

Third, technology can greatly reduce the transaction costs involved in soliciting and enabling individual preferences regarding the use of personal data and the enforcement of use-transferability restrictions. As a general example of technology's impact on privacy transaction costs, consider Microsoft Word and metadata. On the one hand, this program allows the creation of rich metadata about any document.[248] On the other hand, this same software permits individuals to minimize

---

[245] Consider two publicly traded companies, Equifax and Acxiom. In 2003, Equifax earned $274.4 million in revenue from marketing services, primarily from the sale of data to direct marketers and credit card companies. Equifax, Inc., Annual Report Pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934 for the Fiscal Year Ended December 31, 2003 (Form 10-K), File No. 001-06605, at I-21, *available at* http://www.sec.gov/Archives/edgar/data/33185/000104746904007525/a2129029z10-k.htm.

In 2003, Acxiom earned $173 million in revenue from its data and software products, primarily from the sale of lists and the sale of software to manage those lists. Acxiom Corp., Annual Report Pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934 for the Fiscal Year Ended March 31, 2003 (Form 10-K), File No. 0-13163, at F-5, *available at* http://www.shareholder.com/Common/Edgar/733269/733269-03-6/03-00.pdf.

[246] *See* SIMSON GARFINKEL, DATABASE NATION 167–68 (2000); SCHWARTZ & REIDENBERG, *supra* note 9, at 321–22.

[247] GARFINKEL, *supra* note 246, at 168.

[248] *See* Microsoft Corp., *supra* note 80.

the creation of metadata. To be sure, questions may remain about whether the Microsoft commands for minimizing metadata can be made more transparent or easier to enable.[249] But one point is clear: the additional cost of designing software to enable expression of these privacy preferences is minimal. In a similar fashion, the collection of opt-in preferences through boxes on websites or hypertext links also involves minimal costs.

3. Right of Exit. — Consent to data trade should imply not only an initial opportunity to refuse trade, but also a later chance to exit from an agreement to trade. According to Hanoch Dagan and Michael Heller, "[e]xit stands for the right to withdraw or refuse to engage: the ability to dissociate, to cut oneself out of a relationship with other persons."[250] Providing a chance to withdraw is important because current standards afford little protection to privacy. Once companies are able to establish a low level of privacy as a dominant practice, individuals may face intractable collective action problems in making their wishes heard. As a consequence, an information privacy entitlement should include a right of exit from data trades. This right of exit, for example, would allow people to turn off the tracking devices that follow them through real space, to disable spyware and adware on the Internet, and to cancel their obligations to hear compensated telemarketing pitches.

For the privacy market, a right of exit prevents initial bad bargains from having long-term consequences. As this Article has noted, most states regulate the used car market to require that commercial resellers of used cars take such vehicles back when flaws persist after multiple repair attempts. Privacy markets should similarly include a statutory right of exit to allow individuals to get out from under bad bargains.

For the privacy commons, a right of exit preserves mobility so people can make use of privacy-enhancing opportunities and otherwise reconsider initial bad bargains. Dagan and Heller have proposed that exit is a necessary element of a "liberal commons" because "well-functioning commons regimes give paramount concern to nurturing

---

[249] For those reading this Article near a personal computer, open a Word document. On the Tools menu, click "Options," and then click the "Security" tab. Select the "Remove personal information from this file on save" checkbox and then save the document. All metadata has been removed. Or, alternatively, open a Word document; then click on "File" and "Properties"; then click on the "Summary" tab. Surprised by the amount of information? Return to the start of this footnote for instructions on how to remove all metadata.

For general analysis on how the design of software and other computer interfaces is a stubborn art form, see STEVEN JOHNSON, INTERFACE CULTURE 213–14 (1997); STEPHENSON, *supra* note 171, at 68.

[250] Dagan & Heller, *supra* note 152, at 568 (citing LAURENCE H. TRIBE, AMERICAN CONSTITUTIONAL LAW §§ 15–17, at 1400–09 (2d ed. 1988)).

shared values and excluding bad cooperators."[251] A right of exit allows customers to discipline deceptive information collectors. Existing customers will leave as a result of the bad practices, and potential customers will be scared off. In this fashion, a privacy market disciplines deceptive information collectors by shrinking their customer base.

The right to exit also brings with it a related interest: the ability to re-enter data trades. Individuals may wish to alternate between privacy preferences more than once. As an illustration of the implications of the right to re-enter, a wearable chip appears relatively attractive in comparison to the implantable chip because of the lower costs involved should one have a change of heart after an exit. An implantable chip makes it not only more difficult to exit, but also more costly to re-enter and make one's personal data available again to vendors and third parties.

The possible danger of a right of exit, however, is that it might actually encourage, rather than discourage, deceptive claims from data collectors. The risk is that deceptive information collectors will encourage defections from existing arrangements that are privacy-friendly. Something analogous to this phenomenon is already occurring in telephony with "cramming" and "slamming." Cramming refers to misleading or deceptive charges on telephone bills; it takes place, for example, when a local or long-distance telephone company fails to describe accurately all relevant charges to the consumer when marketing a service.[252] Slamming refers to changes made to a customer's carrier selection without her permission.[253] The response to the risk of such deceptive behavior in the context of information privacy should include legislative regulation of the way that privacy promises are made, including regulation of privacy notices and creation of institutions to police privacy promises. This Article returns to the issues of notice and privacy-promoting institutions below.

4. Damages. — In the classic methodology of Guido Calabresi and Douglas Melamed, "property rules" are enforced by the subjective valuations of a party and injunctions for specific performance.[254] In *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, Calabresi and Melamed argue that in a property regime "the value of the entitlement is agreed upon by the seller."[255] They

---

[251] *Id.* at 571.

[252] *See* Fed. Communications Comm'n, *Unauthorized, Misleading, or Deceptive Charges Placed on Your Telephone Bill — "Cramming"*, http://www.fcc.gov/cgb/consumerfacts/cramming.html (last visited Apr. 10, 2004).

[253] *See* Fed. Communications Comm'n, *Slamming*, *at* http://www.fcc.gov/slamming/welcome.html (last visited Apr. 10, 2004).

[254] *See* Guido Calabresi & A. Douglas Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, 85 HARV. L. REV. 1089, 1092 (1972).

[255] *Id.*

contrast this approach with a state determination of damages, which they associate with a "liability rule."[256] This Article's preference when harm occurs to information privacy interests is for state determination of damages, including explicit recourse to liquidated damages. Leaving data sellers and buyers free to set the prices for privacy violations will produce inadequate obedience to these obligations.

First, actual damages are frequently difficult to show in the context of privacy. Already, in two notable instances, litigation for privacy violations under a tort theory has foundered because courts determined that the actual harm that the plaintiffs suffered was de minimis.[257] In *Shibley v. Time, Inc.*,[258] the Ohio Court of Appeals held that it was not a tortious invasion of privacy for a publisher to sell subscription list information to a direct mail advertising company.[259] While such a transaction revealed information about an individual's lifestyle, it did not cause "mental suffering, shame or humiliation to a person of ordinary sensibilities."[260] In a second case, *Dwyer v. American Express Co.*,[261] the Appellate Court of Illinois looked not to harm but to value.[262] The *Dwyer* court declared that the American Express Company, which created and rented "information regarding cardholder spending habits,"[263] was not violating any tort right of privacy, but rather creating value.[264] The court noted that "an individual name has value only when it is associated with one of defendants' lists."[265]

Second, an individual's personal data may not have a high enough market value to justify the costs of litigation. Thus, in *Dwyer*, had the court found harm to the plaintiff class, it might have valued the injury

---

256 *See id.*

257 For a suggestion that current codifications of privacy law be revisited, see Lance Liebman, *An Institutional Emphasis*, 32 CONN. L. REV. 923 (2000). For an extensive discussion of the weakness of the privacy tort as it is currently conceptualized, see Solove, *supra* note 97, at 1432–35. In contrast to Solove's analysis of the weakness of the privacy tort, Andrew McClurg has called for a reconceptualization of the appropriation branch of the tort. *See* Andrew J. McClurg, *A Thousand Words Are Worth a Picture: A Privacy Tort Response to Consumer Data Profiling*, 98 NW. U. L. REV. 63 (2003). McClurg's model makes a consumer's consent the key trigger for allowing companies to market personal data; in doing so, he cites the fundamental common law principle, *volenti non fit injuria* ("to one who is willing, no wrong is done"). *Id.* at 128. McClurg argues: "If people validly consent to invasions of their privacy, there is little room for objection for others." *Id.* at 129. This Article argues, however, that there are important areas in which consent should *not* be considered adequate for permitting data trade and that legal restrictions are needed on use and transfer of personal data.

258 341 N.E.2d 337, 339 (Ohio Ct. App. 1975).

259 *Id.* at 339.

260 *Id.* (quoting *Housh v. Peth*, 133 N.E.2d 340 (Ohio 1956)).

261 652 N.E.2d 1351, 1356 (Ill. App. Ct. 1995).

262 *Id.*

263 *Id.* at 1353.

264 *See id.* at 1356.

265 *Id.*

to each person simply by dividing the cost of the mailing list by the number of names on it. The resulting sum would probably not have been sufficient to justify litigation.

Finally, due to the difficulty of detection, many violations of privacy promises will themselves remain private. Often, identity theft victims do not realize that their identities have been stolen.[266] Spyware provides another example of a privacy invasion that is difficult to notice. If damages are to reflect an implicit price payable for violation of a legal right, this price should be set higher or lower depending on the probability of detection of the violation. Since many privacy violations have a low probability of detection, damages should be higher.

A state determination of damages through privacy legislation is preferable to the Calabresi-Melamed approach of enforcing the subjective valuations of private parties with injunctions.[267] Schemes providing for liquidated damages will assist the operation of the privacy market and the construction and maintenance of a privacy commons. It will encourage companies to keep privacy promises by setting damages high enough to deter potential violators and encourage litigation to defend privacy entitlements. In addition, damages support a privacy commons by promoting social investment in privacy protection. Such damages may also reduce the adverse impact of collective action problems in the privacy market by allowing consumers who do not litigate to benefit from the improved privacy practices that follow from successful litigation.

Existing privacy law sometimes adheres to this path by either collectively setting damages or relying on liquidated damages. Thus, the Video Privacy Protection Act allows a court to "award . . . actual damages but not less than liquidated damages in an amount of $2,500."[268] The Driver's Privacy Protection Act contains for similar language regarding damage awards against a "person who knowingly obtains, discloses or uses personal information, from a motor vehicle record, for a purpose not permitted under this chapter."[269] Finally, the Cable Communications Policy Act, which safeguards cable subscriber information, allows a court to award "liquidated damages computed at the rate of $100 a day for each day of violation or $1,000, whichever is higher."[270]

---

[266] Daniel J. Solove, *Identity Theft, Privacy, and the Architecture of Vulnerability*, 54 HASTINGS L.J. 1227, 1248 (2003).

[267] Calabresi & Melamed, *supra* note 254, at 1092.

[268] 18 U.S.C. § 2710(c)(2) (2000).

[269] *Id.* § 2724.

[270] 47 U.S.C. § 551(f) (2000).

5. Institutions. — Institutions shape the legal and social structure in which property is necessarily embedded. Just as Carol Rose speaks of property as "the most profoundly sociable of human institutions,"[271] it is also an institution that depends on other entities for its shape and maintenance. For example, intellectual property has been fostered by the performing rights societies such as the American Society of Composers, Authors, and Publishers (ASCAP) and Broadcast Music, Inc. (BMI).[272] These organizations license performance rights in nondramatic musical compositions and distribute royalties to artists.[273] Automobiles are another form of property that is structured by legal obligations; they require title recordings, annual safety inspections, and, depending on the state, different mandatory insurance policies.[274]

These requirements in turn create a dynamic of institution-building — in the automobile example, a mixture of public and private entities has been created to record title, inspect motor vehicles, and underwrite insurance. As for institutions that manage intellectual property, a court has discussed how ASCAP "maintains a surveillance system of radio and television broadcasts to detect unlicensed uses, institutes infringement actions, collects revenues from licensees and distributes royalties to copyright owners in accordance with a schedule that reflects the nature and amount of the use of their music and other factors."[275] ASCAP and BMI also employ "field agents" who monitor local entertainment establishments for unauthorized use of their members' compositions.[276]

What role should institutions play as part of a system of propertized personal data? Institutions are needed for three general purposes: to provide trading mechanisms (a "market-making" function), to verify claims to propertized personal data (a verification function), and to police compliance with agreed-upon terms and legislatively mandated safeguards (an oversight function). Institutions filling these roles will assist the privacy market by ensuring that processes exist for the exchange of data and for the detection of violations of privacy promises. Such entities can also help construct and maintain the privacy commons — the literature on commons, in fact, notes the need for

---

271 Rose, *supra* note 185, at 632.

272 For an overview of the performance rights societies, see ROBERT A. GORMAN & JANE C. GINSBURG, COPYRIGHT 569–77, 606–08 (6th ed. 2002).

273 SCHECHTER & THOMAS, *supra* note 189, § 7.4.3, at 133–35.

274 For a discussion of the resulting model of propertization in automobiles, see Schwartz, *supra* note 5, at 774–76.

275 Columbia Broad. Sys., Inc. v. Am. Soc'y of Composers, 400 F. Supp. 737, 742 (S.D.N.Y. 1975).

276 *See, e.g.*, Ocasek v. Hegglund, 116 F.R.D. 154, 155 (D. Wyo. 1987) (addressing a case in which ASCAP field agents found infringing use of copyrighted material in a dance hall in Douglas, Wyoming).

such institutions.[277] Consider how different entities police overfishing of the ocean and seek to detect pollution that degrades the environment. Consider also a fascinating recent examination of an everyday public good — parking rights at a curb — in which Richard Epstein discusses how a move away from "bottom-up rules of first possession" requires construction of parking meters or assignment of stickers to neighborhood residents.[278] Although not the focus of Epstein's analysis, these approaches also require institutions to ticket parking violations and assign parking stickers.

Two additional introductory points can be made regarding institutions. First, this Article's preferred model involves decentralization of both the market-making and the oversight functions whenever possible. Such decentralization should also include private rights of action so that citizens can participate in protecting their own rights. Second, the Federal Trade Commission (FTC) already plays an important role in privacy protection, and its activities indicate the importance both of the policing of privacy promises and of decentralized institutional infrastructures.

As to the first role of institutions, the "market-making" function is best handled through different centers for information exchange. In contrast to this view, Kenneth Laudon has proposed the establishment of a National Information Market (NIM).[279] In the NIM, "[i]ndividuals would 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."[280] These institutions would pool information assets and sell them in "baskets" on a National Information Exchange.[281] They would also allocate the resulting compensation, minus a charge for their services, to the individuals whose information comprises a given basket.[282]

The NIM would be a centralized market for propertized personal data. This vision necessitates a single institutional infrastructure that would permit "personal information to be bought and sold, conferring on the seller the right to determine how much information is divulged."[283] Unfortunately, this single market might also encourage

---

[277] *See* BOLLIER, *supra* note 152, at 189–209 (discussing strategies for protecting the commons, including the creation of social institutions); Hardin, *supra* note 152, at 1246 ("We must find ways to legitimate the needed authority of both the custodians and the corrective feedbacks.").

[278] Richard A. Epstein, *The Allocation of the Commons: Parking on Public Roads*, 31 J. LEGAL STUD. S515, S523 (2002).

[279] Laudon, *supra* note 5, at 99–104.

[280] *Id.* at 100.

[281] *See id.*

[282] *See id.*

[283] *Id.* at 99.

privacy violations because its centralized nature makes it an easy target for attacks. In response to the possibility of cheating and other abuse, Laudon calls for development of "National Information Accounts (NIAs) for suppliers (individuals and institutions) and buyers (information brokers, individuals, and institutions)."[284] He writes: "Every participating citizen would be assigned an NIA with a unique identifier number and barcode symbol."[285] In contrast, this Article calls for verification of propertized personal information through an association with nonpersonal metadata. This metadata might contain information such as the database from which the personal information originated, whether any privacy legislation covered that information, and the existence of any restrictions on further data exchange without permission from the individual to whom the data referred.[286] Such a decentralized approach would avoid the possibility of a major privacy meltdown due to the unique identifiers associated with a single NIA. Decentralized data markets also have the potential to develop privacy-friendly innovations in discrete submarkets. Given the novelty of an institutionalized data trade, it makes sense to start with multiple small markets that can draw on local knowledge rather than with Laudon's single NIM.[287]

Data trading laws should also allow private rights of action, including class actions, when privacy rights are violated. Such rights of action can be highly effective in increasing compliance with statutory standards. For example, current rules against telemarketing allow lawsuits against companies that continue to make calls after a consumer has requested that they cease. Such suits have resulted in millions of dollars in fines, and have made the words "place me on your do not call list" a potent request.[288]

The recently enacted federal anti-spam bill provides a negative example in this regard. The CAN-SPAM Act of 2003 fails to provide for an individual right of action.[289] It does provide, however, for the FTC's study of "a system for rewarding those who supply information

---

[284] *Id.* at 100.

[285] *Id.*

[286] For a somewhat analogous proposal that articulates a model of "trusted architectures," see Jonathan Zittrain, *Privicating Privacy: Reflections on Henry Greely's Commentary*, 52 STAN. L. REV. 1595, 1595–97 (2000).

[287] For development of a similar concept of local knowledge, see generally Michael C. Dorf & Charles F. Sabel, *A Constitution of Democratic Experimentalism*, 98 COLUM. L. REV. 267 (1998).

[288] *See* Foley, *supra* note 146 (discussing lawsuits brought against telemarketers under the Telephone Consumer Protection Act); Napoli, *supra* note 146 (reporting on a lawsuit against junk faxing).

[289] CAN-SPAM Act of 2003, Pub. L. No. 108-187, 117 Stat. 2699 (codified at 15 U.S.C.A. §§ 7701–7713 (West Supp. 2003)). On a more positive note, it does provide for enforcement by internet service providers, *id.* § 7(g); the FTC and other federal agencies, *id.* § 7(a)–(b); and, with some limitations, state attorneys general, *id.* § (f)(8).

about violations of the Act."[290] This proposed bounty system for those who assist the FTC follows a recommendation by Lawrence Lessig, a leading cyberlaw professor.[291] As the CAN-SPAM Act states, the FTC is to develop "procedures . . . to grant a reward of not less than 20 percent of the total civil penalty collected for a violation of [the] Act to the first person" who both "identifies the person in violation of [the] Act" and "supplies information that leads to the successful collection of a civil penalty."[292]

The bounty system calls for a mix of public and private action to increase enforcement of legal norms. It assumes, however, that the FTC's central weakness in enforcement is either informational or technical. That is, the FTC may lack adequate evidence regarding spam or the technical skills to unmask those who send unsolicited commercial e-mails. Yet the FTC already has a procedure for collecting spam, and by 2003 it was already receiving as many as 130,000 forwarded e-mails *a day* as a result.[293] Moreover, if the FTC lacks the technical skills to unmask spammers, it might simply hire additional computer scientists. The enforcement of laws against spam, junk faxes, and unauthorized use of personal data is frequently a drawn-out, resource-intensive process,[294] and the bounty-hunter approach still leaves the central burden on the FTC or other governmental agencies. A final problem with the bounty approach, as presented by Lessig and the CAN-SPAM Act, is that it rewards only a single person per spamming case.[295] A stronger mix of public and private action would encourage broader involvement by private individuals. As Diane Mey, the "Erin Brockovich of the antitelemarketing movement," notes of the benefit of private rights of action: "if enough people sting them a bunch of little stings, maybe they'll get the message and change their ways."[296]

---

290 *Id.* § 11.

291 Michael Bazeley, *New Weapon for Spam: Bounty*, SAN JOSE MERCURY NEWS, Apr. 26, 2003, http://www.mercurynews.com/mld/mercurynews/business/5722718.htm; Declan McCullagh, *A Modest Proposal To End Spam*, CNETNEWS.COM (Apr. 28, 2003), *at* http://www.news.com.com/2010-1071-998513.html.

292 CAN-SPAM Act of 2003 § 11.

293 *CAN-SPAM Act of 2003: Hearing on Spam (Unsolicited Commercial E-Mail) Before the Senate Comm. on Commerce, Sci. and Transp.*, 108th Cong. (May 21, 2003) (statement of Marc Rotenberg, Executive Director, Electronic Privacy Information Center), http://www.epic.org/privacy/junk_mail/spam/spamtestimony5.21.03.html. The website to which spam is sent is uce@ftc.gov. As the FTC website states, "[t]he FTC uses the unsolicited emails stored in this database to pursue law enforcement actions against people who send deceptive spam email." Fed. Trade Comm'n, *You've Got Spam: How To "Can" Unwanted Email*, *at* http://www.ftc.gov/bcp/conline/pubs/online/inbox.htm (last visited Apr. 10, 2004).

294 *See* Foley, *supra* note 146; Napoli, *supra* note 146.

295 CAN-SPAM Act of 2003 § 11.

296 Foley, *supra* note 146.

All of which is not to say, however, that the FTC and other governmental agencies do not have an important role to play in privacy protection. Here, the FTC's existing activities illustrate the contribution to policing possible from both public sector institutions and decentralized institutional infrastructures. The FTC has acted in a number of instances to enforce the privacy promises of companies that collect personal data, particularly those who do so on the Internet.[297] Its jurisdiction in these cases is predicated, however, on a company making false representations regarding its privacy practices. These false promises must constitute "unfair or deceptive trade practices" under the Federal Trade Commission Act for the FTC to have jurisdiction.[298] This requirement of deception means that the agency is powerless — absent a specific statutory grant of authority — to regulate the collection of personal data by companies that either make no promises about their privacy practices or tell individuals that they will engage in unrestricted use and transfer of their personal data.[299]

Even with a specific grant of authority, the FTC would likely be overwhelmed if it were the sole institution responsible for policing the personal information market. In addition, as noted above, the "bounty hunter" approach is unlikely to succeed. Innovative approaches involving multiple institutions are necessary. Thus, as noted, this Article

---

[297] For information on the FTC's enforcement role, see Federal Trade Commission, *Privacy Initiatives: Introduction*, *at* http://www.ftc.gov/privacy/index.html (last visited Apr. 10, 2004). For a discussion of independent oversight, see Schwartz, *supra* note 9, at 1679–81.

[298] Schwartz, *supra* note 9, at 1680 (internal quotation marks omitted).

[299] The FTC's general jurisdiction is also limited by statute. The FTC's enabling act restricts its powers to situations in which an unfair act or practice "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition." 15 U.S.C. § 45(n) (2000). As this statutory language indicates, the FTC is not a roving commission with unlimited power to stop unfair or deceptive trade practices. For interpretation of the circumstances under which withholding of information triggers FTC enforcement, see *Thompson Medical Co. v. FTC*, 791 F.2d 189, 196 (D.C. Cir. 1986); *In re International Harvester Co.*, 104 F.T.C. 949, ¶ 308, at 1041 (1984); PETER C. WARD, FEDERAL TRADE COMMISSION: LAW, PRACTICE, AND PROCEDURE § 5.04[2] (2002).

Specific limited jurisdictional authority for the FTC to police privacy practices has been granted, for example, by the Children's Online Privacy Protection Act of 1998 (COPPA), 15 U.S.C. §§ 6501–6506 (2000). As its cornerstone, COPPA generally forbids commercial websites from collecting information about children without parental consent. *See id.* § 6502(b)(1)(B)(ii). It also grants parents the right to access any information about their children that is collected. *See id.* § 6502(b)(1)(B)(i), (iii). The FTC has taken an active role concerning its responsibilities under COPPA; for example, it has engaged in enforcement actions and worked with industry and privacy advocates to develop streamlined procedures for gathering parental consent to data collection. For more on the FTC's efforts in this area, see Federal Trade Commission, *Children's Privacy: Enforcement*, *at* http://www.ftc.gov/privacy/privacyinitiatives/childrens_enf.html (last visited Apr. 10, 2004). As of March 2004, the FTC had engaged in eleven privacy investigations pursuant to its jurisdiction under COPPA. *Id.* In summary, then, a broad claim by the FTC of jurisdiction over privacy practices might fail to meet the existing statutory threshold.

favors a decentralized institutional model. The GLB Act offers an interesting example of this model because it divides enforcement authority between the FTC and other administrative agencies depending on the nature of the regulated financial institution.[300] The Children's Online Privacy Protection Act further decentralizes this institutional model. It permits a state attorney general to bring civil actions "on behalf of residents of the State."[301] Similarly, the Telephone Consumer Protection Act (TCPA), which places restrictions on junk faxes and telemarketing, allows suits by state attorneys general.[302]

In addition, some privacy laws have added a private right of action to this mixture. Such laws include the TCPA,[303] Video Act,[304] Fair Credit Reporting Act,[305] Cable Privacy Act,[306] and Electronic Communication Privacy Act.[307] The private right of action allows individuals to enforce statutory interests. In addition, it overcomes the weaknesses of the privacy tort, which generally has not proved useful in responding to violations of information privacy.[308]

Finally, as part of this decentralized model, the federal government should create a Data Protection Commission. In contrast to existing agencies that carry out enforcement actions, such as the FTC, a United States Data Protection Commission is needed to fill a more general oversight function.[309] This governmental entity would assist the general public, privacy advocacy groups, and the legislature in understanding the boundaries of existing information territories. With the exception of the United States, all large Western nations have created such independent privacy commissions.[310] Of the different inter-

---

300 Under the GLB Act, regulatory agencies can assess monetary fines for violations of the Act's privacy requirements and even seek criminal penalties. Gramm-Leach-Bliley Act, Pub. L. No. 106-102, § 523(b), 113 Stat. 1338, 1448 (1999) (codified at 15 U.S.C. § 6823 (2000)).

301 15 U.S.C. § 6504 (2000).

302 47 U.S.C. § 227(f) (2000). For examples of such litigation, see *Missouri v. American Blastfax, Inc.*, 323 F.3d 649 (8th Cir. 2003); and *Texas v. American Blastfax, Inc.*, 121 F. Supp. 2d 1085 (W.D. Tex. 2000).

303 47 U.S.C. § 227(b)(3) (2000).

304 18 U.S.C. § 2710(c) (2000).

305 15 U.S.C. §§ 1681n–1681o (2000).

306 47 U.S.C. § 551(f) (2000).

307 18 U.S.C. § 2707 (2000).

308 For a more detailed discussion, see Schwartz, *supra* note 9, at 1634; Kang, *supra* note 90, at 1231.

On the weaknesses of the privacy tort in real space, see Murphy, *supra* note 5, at 2388–93, and Diane L. Zimmerman, *Requiem for a Heavyweight: A Farewell to Warren and Brandeis's Privacy Tort*, 68 CORNELL L. REV. 291, 292–93 (1983).

309 *See generally* BENJAMIN R. BARBER, STRONG DEMOCRACY: PARTICIPATORY POLITICS FOR A NEW AGE 310 (1984) (calling for a greater role for ombudsmen in civil societies).

310 DAVID H. FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES: THE FEDERAL REPUBLIC OF GERMANY, SWEDEN, FRANCE, CANADA, AND THE UNITED STATES 394–97 (1989).

national models, the "advisory model," utilized in Germany, provides the most promising model for the United States.[311]

Germany's data protection commissions are independent advisory bodies that generally lacks direct enforcement powers.[312] Established at the federal and state levels, they advise the legislature, act as ombudsmen for citizen complaints, and monitor the effectiveness of existing laws.[313] The commissions also carry out the important task of informing the public and media of developments concerning data privacy.[314] In Germany, state data protection commissioners, rather than the federal commission, also generally have the power to oversee the private sector.[315] In numerous instances, these commissioners have stopped enterprises from violating privacy rights; in the state of Schleswig-Holstein, for example, the data protection commission pressured physicians and hospitals to stop dumping medical records in garbage cans, and prevented the publication of a planned Internet site that would have violated existing credit law by publishing the names of debtors.[316] Such data protection agencies have also played a significant role in other countries regulating the use of personal data that has accompanied the rise of the Internet.[317]

B. The Case Studies Revisited

In this final section, this Article revisits its initial case studies. This Article first discusses the VeriChip and the wOzNet and then turns to separate discussions of distributed computing and compensated telemarketing. For each case study, it evaluates the proper application of this Article's five-part model involving inalienabilities, defaults, a right of exit, damages, and institutions.

---

311 *Id.* at 40–47, 259–62.

312 *Id.*

313 *Id.* at 385–404; *see also* COLIN J. BENNETT, REGULATING PRIVACY: DATA PROTECTION AND PUBLIC POLICY IN EUROPE AND THE UNITED STATES 195–229 (1992).

314 Schwartz, *supra* note 192, at 492–95.

315 *See* Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung (Bundesdatenschutzgesetz) § 38, v. 27.1.1977 (BGBl. I S.201), *reprinted in* v. 14.1.2003 (BGBl. I S.66).

316 A description of these cases is available from the Annual Reports of the Independent State Center for Data Protection. *See* Unabhängiges Landeszentrum fur Datenschutz Schleswig-Holstein, *Tätigkeitsbericht 2003 § 4.8.8* (medical records), http://www.datenschutzzentrum.de/material/tb/tb25/kap4_8.htm#Tz4.8.8 (last visited Apr. 10, 2004); Unabhängiges Landeszentrum fur Datenschutz Schleswig-Holstein, *Tätigkeitsbericht 2002 § 6.2.7* (Internet posting of debtor information), http://www.datenschutzzentrum.de/material/tb/tb24/kap6.htm#Tz6.2.7 (last visited Apr. 10, 2004).

317 In addition to the data protection commissioners in each Member State of the European Union, a working group of data protection commissioners has been established at the European Commission. *See* Europa, *Tasks of the Article 29 Data Protection Working Party*, http://europa.eu.int/comm/internal_market/privacy/workingroup_en.htm (last visited Apr. 10, 2004).

1. The VeriChip and the wOzNet: Saying "No" to Implantable Chips. — The VeriChip and the wOzNet share certain characteristics. Both devices are ID chips that allow the tracking either of a bearer (in the case of the implantable VeriChip) or a wearer (in the case of the clip-on wOzNet). These devices raise two issues for consideration: first, whether a distinction should be drawn between the implantable and wearable tracking devices; and second, the extent to which this Article's five elements for information property can respond to attendant privacy risks from ID chips.

Implantable chips in particular raise such a significant threat to privacy that commercial data trades should *not* be allowed with them. As a general matter, implantable chips in humans, with or without tracking capacity, represent a wave of the future. Like the VeriChip, chip-based "micro-electromechanical systems" (MEMS) are a clear indication of this trend.[318] Yet the use of implantable chips as part of a scheme for commercial data trade is likely to impact the privacy commons in a highly negative fashion. An implantable chip for data trade creates the ultimate barcode — one located inside the human body. Once people are fitted with these barcodes, the implantable chip tracks them constantly and collects their data. This tracking, in turn, has the capacity to destroy socially necessary kinds of multidimensional information privacy spaces. For example, implantable chips undercut the protection of any information privacy statutes that restrict personal data use and transfer. These biochips also permit observation of the same individual in all sectors of physical space, and facilitate multifunctional use of their personal information. There is also a threat that companies or individuals may poach the signals from such chips. This kind of unauthorized behavior could take the form of continuous data collection by unauthorized entities, or even a new form of harassment, which I will term "frequency stalking."

Implantable chips may also resist legislative attempts to preserve a right of exit from data trade. Even if one company promises to turn off its data collection from a given implantable chip, others may continue to collect information by poaching on the first company's system and chips. Moreover, other chip-based systems, such as MEMS, might be detectable by outside companies. As a statutory safeguard, a law might require that all implantable chips be removed as soon as contracts expire or a customer wishes to discontinue data trading. This legal requirement would likely be difficult to enforce, however, and the proliferation of leftover or legacy chips would raise difficult problems. Consequently, it would be advantageous to ban commercial data trade

---

[318] *See* Robbins, *supra* note 30.

with implantable chips while other uses of these devices, such as delivering medicine through MEMS, should be permissible.

An important distinction can be drawn with wearable chips, however, which can be removed from one's clothing and even thrown out. That a wearable chip may be easily removed means that a right of exit can more easily be maintained for wearable chips. Additionally, a distinction can be drawn between the problems posed by implantable chips and Radin's concept of the double bind.[319] Concerned with the harm that market valuation may do to nonmarket conceptions of personhood, Radin proposes that "[w]hen attributes that are (or were) intrinsically part of the person come to be detached and thought of as objects of exchange, the conception of the person is problematized."[320] Drawing on examples involving trade in sex, children, and body parts, Radin contends that commodification of certain things will harm us.[321] Radin fears that people will be subject to a so-called "double bind" as a consequence of "a gap between the ideals we can formulate and the progress we can realize."[322] More concretely, the double bind is the "practical dilemma of nonideal justice"[323] — if we compromise our ideals too much, we reinforce the status quo, but if we are too utopian in our ideals, we make no progress.[324] As an example, a ban on surrogate motherhood, which Radin ultimately supports, harms poor

---

[319] *See* RADIN, *supra* note 76, at 123–30.

[320] *Id.* at 156.

[321] Radin argues that "[t]he kinds of things that deviate the most from laissez-faire are those related to human beings' homes, work, food, environment, education, communication, health, bodily integrity, sexuality, family life, and political life." *Id.* at 113. This list is clearly expansive and made at a daunting level of abstraction. In a nutshell, Radin proposes that commodification is harmful when it leads to an erosion of the concept of personhood. This Article's approach to privacy is not unrelated to Radin's, though it is at least somewhat different. It is interested in a privacy commons, in part because of the function that this space provides in safeguarding an individual capacity for decisionmaking. *See supra* section II.C.

Radin would likely also object to an implantable chip; in her terms, the problem would be the way that it erodes the concept of personhood. Radin writes:

> At present, we . . . tend to think that nuts and bolts are pretty much the "same" whether commodified or not, whereas love, friendship and sexuality are very "different"; we also tend to think that trying to keep society free of commodified love, friendship, and sexuality morally matters more than does trying to keep it free of commodified nuts and bolts.

RADIN, *supra* note 76, at 95. On the "Radin Scale," commodified data collected by implantable chips fall closer to love, friendship, and sexuality than nuts and bolts. Due to the link with bodily integrity, Radin is likely to argue that data trade will risk detaching "attributes that are (or were) intrinsically part of the person." *Id.* at 156.

[322] *Id.* at 123.

[323] *Id.* at 124.

[324] *Id.*

women who will miss out on the possible economic benefit from selling their reproductive capacity.[325]

In contrast to surrogacy, a ban on implantable chips will not disadvantage poor persons in any meaningful fashion. An opportunity to engage in data trade with wearable chips, for example, will still be available. Additionally, because data trade companies will most likely seek affluent and middle-class individuals as customers, such a ban is unlikely to deprive the poor of a significant income stream.[326] Consequently, a ban on data trade from implantable chips will not create a Radinian double bind.

A model privacy law should also regulate the collection and use of personal data with nonimplantable chips. Such legislation should incorporate the five elements for propertization of personal data, as set forth in this Article. Such a statute should legislate inalienabilities that place use-transfer restrictions on the personal information generated through wearable GPS devices. In addition, it should set opt-in default rules for transfers of tracking data.[327] A model GPS privacy law should only permit a company collecting personal information with such devices to transfer such information to third party companies following an opt-in. This law should also contain a proscription against further transfers of personal data; this restriction might be modeled on the one found in the GLB Act and might prohibit a receiving third party from disclosing such information "to any other person that is a nonaffiliated third party."[328] These use-transfer restrictions plus the default rule would serve a significant information-forcing function with great benefit to consumers.

As for the right of exit, a model GPS privacy statute should allow individuals who do business with wearable chip companies to turn off or stop wearing their tracking devices at any time. These consumers should also have a statutory right to terminate their contracts, perhaps after thirty days or after one year. In the context of automobiles, lemon laws provide owners with a right to return under certain circumstances. The lemon laws protect consumers who may not be able

---

[325] *Id.* at 136–40. For a comparative discussion of surrogacy and the family law risks that it raises, see Paul Schwartz, *Baby M. in West Germany*, 89 COLUM. L. REV. 347 (1989) (book review).

[326] *See* Laudon, *supra* note 5, at 102.

[327] In an essay published subsequent to *Contested Commodities*, Radin objects to any "waiver of all personal privacy rights" and calls on policymakers to exclude such a decision "on autonomy grounds." Margaret Jane Radin, *Humans, Computers, and Binding Commitment*, 75 IND. L.J. 1125, 1159, 1161 (2000). Inalienabilities for personal data trade will prevent precisely such sweeping waivers. With legislation that regulates collection of personal data through GPS devices, such as wOzNet, Congress would permit transfers for an initial category of use of the GPS information.

[328] Gramm-Leach-Bliley Act, Pub. L. No. 106-102, § 502(c), 113 Stat. 1338, 1437 (1999) (codified at 15 U.S.C. § 6802(c) (2000)).

to assess possible defects in an automobile prior to the purchase. In a similar manner, buyers of data chips may be unable to assess questions relating to privacy before buying the devices. At different stages of their lives, buyers of the chips may also value their privacy differently. A college student might not care that she was being tracked; this same person, who later seeks an abortion or substance abuse counseling, might object to the tracking. Moreover, the threat of "frequency stalking" exists not only for implantable chips but also for wearable ones. As a consequence, legislation should protect the right to turn tracking devices off at any time and to terminate underlying contracts at certain times.

To be sure, the danger exists that deceptive information collectors will encourage consumers to switch away from privacy-friendly arrangements. Regulation of the form of notice given to GPS consumers as well as an institutional role in policing privacy promises can help on this score. Additionally, legislation should set damages for privacy violations following collection of data by wearable chip companies. A statute should track language found in statutes such as the Video Privacy Protection Act, Driver's Privacy Protection Act, and Cable Communications Act, and should permit liquidated damages.[329]

Finally, institutions must police the privacy promises and practices of wearable chip companies. Institutions are necessary to provide trading mechanisms to help with verification of interests in propertized personal data, and to enforce compliance with agreed-upon terms and legislatively mandated safeguards. As the development of the wOzNet has shown, private entities for collecting and trading information generated from wearable chips are likely to develop. In other words, the private sector can handle a market-making function, but a privacy statute in this area is needed to provide for government enforcement of privacy standards and promises.

2. Networked Computing: Against Free Alienability. — Regarding networked computing, this Article argues that data trade that involves tracking users' activity on the Internet should be permissible. At the same time, however, a free alienability model should not be allowed. Unlike implantable chips, but like wearable chips, the tracking of Internet activity does not represent the kind of privacy threat that requires an outright ban. In contrast to implantable chips, distributed computing creates a privacy threat that involves lower removal costs — an operation on a personal computer is generally less expensive than one on a human being. Moreover, since most people replace their computers every few years or use multiple machines, spying on a computer creates less permanent and less comprehensive surveillance than

---

[329] *See supra* section III.A.4.

that following from inside the body. Finally, cyberspace is, to be sure, a locality where many of us spend much time, and the issue of privacy invasion there is significant. Nevertheless, the consequences of tracking people in real space with implantable chips exceeds the cyberthreat by far. Distributed computing requires the kinds of privacy safeguards that this Article has advocated, including restrictions on free alienability of personal data.

Unfortunately, the two bills now introduced in Congress that seek to regulate spyware fall considerably short of the model that this Article proposes. Although the Bono Bill and Edwards Bill differ, sometimes significantly, both rely on a notice-and-consent approach to information privacy.[330] The core goal of both bills is to ensure that individuals receive notice of data collection by spyware and to require their consent.[331] Once this consent is given, however, any collection of data is possible and any further use of these data permissible.

This Article has pointed, however, both to privacy market failure and to the positive role that information privacy can play as a public good. Both perspectives caution against reliance on a notice-and-consent approach, which relies exclusively on informed individual decisionmaking to reach the optimal level of information privacy. Even with improved notice, however, unrestricted individual trade of personal information may produce suboptimal results.[332] Hence, the use-transfer restrictions proposed by this Article are especially important in regulation of the collection of personal data through distributed computing software.

In comparing the two spyware bills, the Edwards Bill has several advantages over the Bono Bill, including a right of exit. Computer software covered by the Edwards Bill must include "easily understood instructions on how to disable such [a data collection] capability without affecting the performance or operation of such computer software for the purposes for which such computer software was intended."[333] This rule means that distributed computing software must be capable of functioning without collecting personal data and that individuals must be able to turn off the data collection features of the product. By requiring companies to provide customers with the option to safeguard their personal information, the Edwards Bill inherently places pressure on companies to offer incentives to individuals to continue to allow collection of their personal information.

---

330 *See* Bono Bill, H.R. 2929, 108th Cong. § 2 (2003); Edwards Bill, S. 197, 107th Cong. § 2(a)(1) (2001).

331 *See* Bono Bill § 2(a)(1), 2(b)(2), 2(c); Edwards Bill § 2(a)(1)–(2).

332 For a discussion of the limitations of a privacy model based on individual decisionmaking, see Schwartz, *supra* note 201, at 821–30.

333 Edwards Bill § 2(a)(1)(C).

Regarding damages, the Edwards Bill is also superior to the Bono Bill. The Edwards Bill allows injured parties to enjoin violations of the statute and to recover either actual monetary losses or liquidated damages of $2,500 per violation, "not to exceed a total amount of $500,000."[334] A court can even lift this ceiling should it find that "the defendant willfully, knowingly, or repeatedly violated" the Act.[335] In contrast, the Bono Bill permits a court only to levy criminal fines in limited circumstances involving either a narrow class of knowing violations of the statute or for violations of regulations issued under it.[336]

The Edwards Bill also provides a more complete enforcement mechanism than does the Bono Bill. As an illustration, the Bono Bill allows the FTC to issue "generally applicable guidelines and, upon request, advisory opinions."[337] The Edwards Bill gives a similar institutional role to the FTC, but supplements this oversight role with a well-crafted private right of action.[338] It thus allows decentralized enforcement whereby violations are policed not only by a governmental agency, but also by private individuals. Moreover, as noted above, the Edwards Bill allows for adequate damages to induce private individuals to bring lawsuits to enforce privacy rights.[339]

3. Compensated Telemarketing: Information Forcing About Data Use and Transfers. — The Ayres-Funk proposal, which calls for a right to market one's attention to telemarketers, is inventive and meritorious.[340] It argues that people should be allowed to trade a right "not to be made unwilling listeners in their homes."[341] Thus far, this Article's analysis of this scholarly work has emphasized the extent to which the proposal involves not only a right to be let alone at home, but also an effect on the collection of personal data; it now considers the dimension of compensated telemarketing that involves the creation of personal information databases and the further use and transfer of this information.

Regarding inalienabilities, legislation ought to permit authorized intermediaries, as proposed by Ayres and Funk, to trade individuals' personal data, but only subject to the kind of use-transfer restrictions developed in section III.A.1. Indeed, Ayres and Funk appear likely to support this conclusion. To ensure informed consent, they propose that "[a] potential, existing or past consumer should have to affirma-

---

334 *Id.* § 2(e)(1)(B)(ii).
335 *Id.* § 2(e)(2).
336 *See* Bono Bill § 3(b).
337 *Id.* § 3(a)(2).
338 *See* Edwards Bill § 2(c), 2(e).
339 *See id.* § 2(e)(1)(B).
340 *See* Ayres & Funk, *supra* note 11, at 78–82.
341 *Id.* at 126.

tively waive the right to [receive compensation for being] solicited to buy additional products or services."[342] Thus, regarding further transfer, an agreement to receive calls about Star Trek or running shoes should restrict further transfer for unrelated purposes without an additional waiver for information generated through these calls. As Ayres and Funk state in general terms, "[t]he business's right to solicit without paying compensation should not be assignable to other companies — otherwise, waiving compensation from one business could effectively provide a waiver to all businesses."[343] In addition, an opt-in default is needed to ensure that individuals receive the information necessary to exercise informed consent. An individual should not be presumed to have agreed to listen to additional marketing calls unless she has explicitly consented.

An important aspect of the discussion of opt-in and opt-out provisions in the Ayres-Funk piece concerns the role of "ignorance and inertia" as one moves to a system for compensated telemarketing.[344] Ayres and Funk note that they were tempted to presume "some level of compensation that would govern all households unless the household affirmatively moved to increase or decrease the default."[345] Ayres and Funk consider, but ultimately reject, the idea of using the federal minimum wage to calculate the minimum level of compensation. They do so because "[t]he central problem is that households may not know that they have the option to be compensated and to control the amount of compensation."[346] Instead, they favor "status-quo defaults, which effectively set a zero price for daytime calls and an infinite price for nighttime calls."[347] Thus, Ayres and Funk adopt an adjustable default that permits telemarketers to make free unrestricted calls during daytime hours and that blocks them from making calls during late hours and the early morning. Ayres and Funk do propose, however, that "telemarketing calls begin with a disclosure of the offered compensation."[348] This requirement is information-forcing of the purest sort:

---

[342] *Id.* at 123.

[343] *Id.*

[344] *Id.* at 115–17.

[345] *Id.* at 115. As a possible solution, "using the federally mandated minimum wage as a focal point to measure how much people should value their time" might provide "a rough measure of what a majoritarian default would be." *Id.* In other words, everyone would be considered to have agreed to receive telemarketing calls at home for a rate that is currently nine cents per minute. *See id.* The problem with this tactic is that it would force those who currently value their free time at a rate greater than the minimum wage to opt out affirmatively. My arguments in this Article militate against placing such a burden on those who would receive calls only for a higher price.

[346] *Id.* at 116.

[347] *Id.*

[348] *Id.*

straightforward notice concerning both the price offered and the ability to opt out.

The difficulty with this approach, however, is that it forces disclosure of price terms rather than nonprice terms such as privacy practices. As this Article has noted, a lemons equilibrium can occur when a party receives good information about price but bad information about nonprice terms. The danger is that providing consumers merely with information about price at the moment they receive telemarketing calls will do little to lead telemarketers to reveal how personal data generated through these calls will be used and transferred or to encourage consumers to ask about this information. As a result, compensated telemarketing should involve use-transfer restrictions and an opt-in.

Regarding a right of exit, this Article advocates allowing consumers *at any time* to contact a telemarketer and change their preferences as to the type and timing of calls they will accept. Note the contrast with wearable data chips, for which this Article suggests both a thirty-day right to cancel any data trade agreements and an expiration of any contracts for trade after one year. The difference is not based on information privacy grounds, however, but rests on the Ayres-Funk concern about an individual's right to remain undisturbed at home. A right to exit at any time from compensated telemarketing agreements is necessary because of the extent to which daily life may change. A child's staying home with a cold, the arrival of out-of-town guests, or a kitchen remodeling are the kinds of quotidian events that dramatically alter a consumer's willingness to receive compensated telemarketing. Since these events are sometimes difficult to predict, consumers should be able to change their agreements with their information intermediaries at any time.

This Article's final points concern damages and institutions within the telemarketing context. Legislatively determined damages would serve the function of forcing telemarketers to internalize at least some of the costs of violation. Without adequate damages provisions, an intermediary that is "authorized to connect calls that meet pre-specified household . . . prerequisites" may not do an adequate job policing telemarketers or collecting money for its customers.[349] Recall as well that the intermediary is likely to be a local telephone company. The path of consumer relations with these entities since the Bell divestiture has not been smooth, and the presence of adequate damage provisions and private rights of action would be an important step

[349] *Id.* at 110.

toward encouraging these companies to comply with privacy standards.[350]

With respect to institutions, Ayres and Funk envision authorized intermediaries playing a central role in compensated telemarketing by "verifying to the consumer that a particular telemarketing call [is] in fact paying compensation."[351] This ingenious approach involves a household's registering with the intermediary and receiving a PIN code or a sound clip that would be shared only with telemarketers who agree to pay the stated price and that would be announced to the household at the start of the call.[352] The result: "People receiving a telemarketing pitch that was not preceded by the telltale tone or PIN would have immediate notice of a violation."[353]

Although these proposals are valuable, they emphasize the detection of pricing violations. A separate concern, however, is the detection of violations of rules for information use and transfer. For this set of issues, it is of greater relevance that Ayres and Funk propose a private right of action by "[g]ranting citizens a private bounty for identifying violators."[354] This bounty should take the form of liquidated damages for violations of use and transfer rules.

Finally, as a consequence of the FCC's traditional role in overseeing the use of personal data collected by telephone companies, this agency should be assigned a central institutional oversight role in compensated telemarketing. For example, the FCC should police how telephone companies are compensating consumers. As the widespread practices of slamming and cramming in telephony unfortunately demonstrate, these companies do not have a strong record of obeying consumer protection laws. The FTC should supplement the FCC's authority by overseeing the privacy compliance of telemarketers; oversight of this industry has been a traditional FTC role. Indeed, current oversight of the federal "do not call" list is divided between the two agencies.[355]

IV. CONCLUSION

A strong conception of personal data as a commodity is emerging in the United States, and individual Americans are already participating in the commodification of their personal data. This Article's goal has

---

350 For a good overview of these difficulties for consumers, see Fed. Communications Comm'n, *Consumer & Governmental Affairs Bureau*, *at* http://www.fcc.gov/cgb (last visited Apr. 10, 2004).

351 Ayres & Funk, *supra* note 11, at 112.

352 *See id.* at 112–13.

353 *Id.* at 113.

354 *Id.*

355 *See* Matt Richtel, *After Delays, U.S. Prepares To Enforce Do-Not-Call List*, N.Y. TIMES, Oct. 11, 2003, at C2.

been to develop a model for the propertization of personal information that also exhibits sufficient sensitivity to attendant threats to personal privacy. It has examined devices and systems for the commodification of personal data. These devices and systems include: the VeriChip, an implantable ID chip; the wOzNet, a wearable ID chip; spyware and adware; and compensated telemarketing, as advocated in the scholarship of Ayres and Funk. Each of these devices and systems demonstrates an application of technology that commodifies personal data, and each raises significant information privacy concerns. Moreover, each technology has been supported by a policy argument regarding free alienability, or the notion that an individual has a right to do what she wants with her personal information.

This Article then explored current arguments opposing trade in personal data. The first of these arguments pointed to privacy market failure, which is the idea that current market conditions for exchange of commodified personal data are suboptimal. The second argument against data trade viewed privacy as a public good. From this perspective, privacy in personal information matters because of its social payoff, which is the creation and maintenance of a privacy commons. Finally, under this Article's free alienability argument, propertization of personal data might prevent restrictions from being placed on one's ability to trade personal data.

This Article has been sympathetic to both the privacy market failure and the privacy commons arguments. Nonetheless, it has found that these views did not provide a convincing basis for blocking all propertization of personal data. Failures of the privacy market may justify efforts to improve data trade, but not a comprehensive ban on market mechanisms. The idea of a privacy commons also is best seen as raising questions concerning the extent to which — and precisely how — propertization might be used in a commons rather than as a justification for an outright ban on personal information as property. This Article has also been skeptical of the alienability argument because the inability to place restrictions on one's ability to trade personal data is an inevitable aspect neither of property in general nor of a particular property interest in personal information.

In section III.A, this Article developed the five critical elements of its model of propertized personal information. This model views information property as a bundle of interests to be shaped through attention to five areas: inalienabilities, defaults, a right of exit, damages, and institutions. Section III.B returned to the initial case studies and applied to them this Article's model of propertized personal data.

This Article has called for an outright ban on data trade through the use of implantable chips. Its concern is that implantable chips will permit tracking that would destroy attempts to build a privacy commons. In contrast, it has argued that data trade through wearable chips should be permissible pursuant to the restrictions found in this

Article's model for propertized personal information. As for distributed computing, this Article has pointed out shortcomings in current spyware legislation before Congress. In response, this Article calls for use-transfer restrictions for personal data collected through distributed computing. This approach would go beyond the notice-and-consent model embodied by current legislative proposals.

Finally, compensated telemarketing, as proposed by Ayres and Funk, offers a potential best-case scenario for commodification of personal data. Yet this Article has argued for modification of the Ayres-Funk model in several ways. Its most important alterations involve enactment of legislation to: (1) safeguard the ability of consumers to receive information about the use of their personal data and not merely about the price of these data; (2) grant a right of exit from any compensation agreements at any time; (3) set the cost of damages for privacy violations; and (4) institute formal oversight of privacy practices by both the FCC (for authorized intermediaries) and the FTC (for telemarketers).

As Dagan has argued, property is a human creation, the form of which can be altered to meet human needs and reflect human values.[356] In this light, this Article has sought to develop an ideal conception of personal information as property that responds to privacy market failure and to the need for a privacy commons. A critical challenge remains to persuade policymakers and individual data traders of both the benefits of information markets and the need to set appropriate restrictions on them. Moreover, future technological twists and turns are inevitable. A final cautionary point is therefore in order: in propertizing personal information and opening the door to data trade, the legal system must be willing to revisit its judgments and regulations.

New methods and devices are ceaselessly being developed to collect personal information and further data trade. There is no better way to conclude this Article than by discussing two additional examples of such methods and devices. First, TiVo, a company that markets a digital video recorder, is boldly changing the nature of broadcast television. The TiVo recorder also offers great convenience for consumers by creating recommendations based on previous viewing choices, allowing the pausing of live television, and permitting the skipping of commercials.[357] The TiVo recorder has the capacity to "tell what has been watched on a particular TiVo box, down to the second, including the number of times a moment was rewound and played again, or a commercial was skipped."[358] Generally, TiVo has chosen not to collect

---

[356] *See* Dagan, *supra* note 197, at 1532.

[357] Ben Charny, *TiVo Watchers Uneasy After Post-Super Bowl Reports*, CNETNEWS.COM (Feb. 5, 2003), *at* http://news.com.com/2100-1041-5154219.html.

[358] *Id.*

personal data concerning individual viewing habits, but it "does occasionally mine data from a random sampling of 20,000 homes watching a particular program."[359] Beyond these anonymous samples, however, TiVo has begun to sell viewing data for demographic purposes; it does so with the permission of the TiVo users whose personal data are affected.[360] Perhaps the most problematic aspect of this emerging data trade is the way in which TiVo and related devices may transform an area of once anonymous media consumption. Watching television may increasingly become an activity in which finely grained personal data are generated and traded — and this change risks destruction of an existing privacy commons.

Second, some bars and restaurants electronically scan barcodes and magnetic strips found on state drivers' licenses.[361] Drivers' licenses contain information such as name, address, age, weight, and, in some states, a Social Security number. This information allows entities to "track how often patrons come in, the hours they arrive and even identify those who arrive in groups (if the cards of friends are swiped in sequence)."[362] This information can also be combined with sales data if a customer makes purchases with a credit card.[363] The resulting databases have tremendous marketing potential. This example raises issues about the extent to which private sector organizations should be allowed to piggyback on the information collection infrastructure that the government has established for other purposes.

At its core, information privacy has both an individual and a social value. Hence, I end on a note of caution: ongoing scrutiny of regulation of personal data is needed because failure in the privacy market can harm both individual self-determination and democratic deliberation.

---

359 *Id.*

360 *See id.*; Nick Wingfield & Jennifer Saranow, *TiVo Tunes In to Its Users' Viewing Habits*, WALL ST. J., Feb. 9, 2004, at B1.

361 Kim Zetter, *Great Taste, Less Privacy*, WIRED NEWS (Feb. 6, 2004), *at* http://www.wired.com/news/privacy/0,1848,62182,00.html.

362 *Id.*

363 *See id.* For a fascinating website that provides interactive software that decodes the information stored in barcodes on drivers' licenses and estimates the worth of these data to direct marketers, see New Radio and Performing Arts, Inc., *The SWIPE Toolkit: Intro*, *at* http://turbulence.org/Works/swipe/main.html (last visited Apr. 10, 2004).