PRIVACY AND TECHNOLOGIES OF IDENTITY

A CROSS-DISCIPLINARY CONVERSATION

Edited by

KATHERINE J. STRANDBURG
DePaul University, College of Law
Chicago, Illinois, USA

DANIELA STAN RAICU
DePaul University, School of Computer Science, Telecommunications, and Information Systems, Chicago, Illinois, USA

Springer

Chapter 6

PRIVACY INALIENABILITY AND PERSONAL DATA CHIPS

Paul M. Schwartz
Anita and Stuart Subotnick Professor of Law, Brooklyn Law School; Visiting Professor of Law, Boalt Hall, School of Law, U.C.-Berkeley, 2005. *This essay is an abridged version of Property, Privacy and Personal Data, 117 Harvard Law Review 2055 (2004).*

Abstract: Even as new possibilities for trade in personal information promise new avenues for the creation of wealth, this controversial market 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 Essay develops a model of propertized personal information that responds to concerns about privacy and evaluates it in the context of tracking chips. It sets out the five critical elements of such a model, which is intended to fashion a market for data trade that respects individual privacy and helps 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.

Key words: tracking chips, property, inalienability, hybrid inalienability, secondary use, downstream use of personal information, data trade, right to exit, Gramm-Leach-Bliley Act, damages, privacy protecting institutions

1. INTRODUCTION

A privacy-sensitive model for personal data trade should respond to five areas: inalienabilities, defaults, a right of exit, damages, and institutions. A key element of this privacy promoting model is the employment of use-transferability restrictions in conjunction with an opt-in default. This Essay 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.

In this Essay, I first develop this privacy sensitive model for personal data trade and then apply it to the use of electronic data chips. I then analyze the model in the context of two devices: the VeriChip, an implantable chip, and the wOzNet, a wearable chip. The VeriChip 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.[1] A physician implants the VeriChip by injecting it under the skin in an outpatient procedure that requires only local anesthesia. A similar device has already been implanted in millions of pets and livestock to help their owners keep track of them. 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.

Whereas the VeriChip involves an implantable identification device, the wOzNet involves a plan to commercialize a wearable identification device.[2] 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. The broadcast of location information from the chip to the base station is done along the same 900-megahertz radio spectrum used by portable phones. 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

[1] *See* Julia Scheeres, *They Want Their ID Chips Now*, Wired News (Feb. 6, 2002), *available at* http://www.wired.com/news/privacy/0,1848,50187,00.html; Julia Scheeres, *Why, Hello, Mr. Chips*, Wired News (Apr. 4, 2002), *available 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. *See* Julia Scheeres, *ID Chip's Controversial Approval*, Wired News (Oct. 23, 2002), *available at* http:// www.wired.com/news/print/0,1294,55952,00.html.

[2] *See* Wheels of Zeus, Overview, at http://www.woz.com/about.html (last visited Apr. 10, 2004); John Markoff, *Apple Co-Founder Creates Electronic ID Tags*, N.Y. TIMES, July 21, 2003, at C3; Benny Evangelista, *Wireless Networks Could Get Personal*, S.F. CHRON., July 21, 2003, at E1; Associated Press, *Apple Co-Founder To Form Locator Network*, ABCNews.com (July 21, 2003), *available at* http://abcnews.go.com/wire/Business/ap20030721_1823.html.

to $250.

2. THE FIVE ELEMENTS OF PROPERTY IN PERSONAL INFORMATION

A dominant property metaphor is the Blackstonian idea of "sole and despotic dominion" over a thing.[3] 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.[4] 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.[5]

2.1 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."[6] As this definition makes clear, inalienabilities may consist of separate kinds of limitations on a single entitlement. 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

[3] 2 William Blackstone, COMMENTARIES ON THE LAWS OF ENGLAND 2 (facsimile ed. 1979) (1766).

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

[5] *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).

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

include a recourse to defaults.

Before turning to these two issues, however, it is important to note that propertized personal information, like all property, is necessarily subject to general limitations on account of the public interest. These limitations, in turn, take certain uses of information entirely outside of the realm of property. 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. 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. It is important to note that the focus of this Essay is not on these mandatory legal requirements that remove personal data entirely from the realm of private negotiations. Instead, this Essay focuses on those use and transferability restrictions that allow personal data to remain at least partially propertized.

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. Thus a variety of devices and systems that commodify information lead to downstream uses and onward transfers. 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.

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. 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 Essay proposes a model that combines limitations on use with limitations on transfer. Under this approach, property is an interest that "runs with the asset"; 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. A

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. From this perspective, propertization of personal information should be limited to the extent it undermines the privacy commons.

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: "The coordination problem arises most clearly in the case of pure public goods . . . consumed in common by a large group."[7] 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 incentive to be the first settler."[8] 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. 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 Essay 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

[7] *Id.* at 939.
[8] *Id.* at 940.

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 Essay's model to ideas regarding propertization. The use-transferability restriction runs with the asset; it follows the personal information downstream. 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. First, the government must have a significant role in regulating the way that notice of privacy practices is provided. 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 (GLB Act) are already engaged in working with banks, other financial institutions, and consumer advocacy groups to develop acceptable model annual "privacy notices."[9]

Second, meaningful disclosure requires addressing what Henry Hansmann and Reinier Kraakman term "verification problems."[10] 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."[11] 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.

[9] *See* Pub. L. No. 106-102, § 501(a), 113 Stat. 1338 (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. *See* § 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 (October 2002), *available at* http://www.ftc.gov/bcp/conline/pubs/buspubs/getnoticed.pdf.

[10] Henry Hansmann & Reinier Kraakman, *Property, Contract, and Verification: The Numerus Clausus Problem and the Divisibility of Rights*, 31 J. LEGAL STUD. S373, S384 (2002).

[11] *Id.*

A survey of existing statutes finds that the law already 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 (Video Act) contains one such limitation: it imposes different authorization requirements depending on the planned use or transfer of the data.[12] 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.[13] This rule restricts data trade by preventing consumers from granting permanent authorization to all transfers of their information.

A second statute incorporating use and transferability limitations is the Driver's Privacy Protection Act of 1994 (DPPA), which places numerous restrictions on the ability of state departments of motor vehicles to transfer personal motor vehicle information to third parties.[14] The statute's general rule is to restrict use of these data to purposes relating to regulation of motor vehicles. 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 Essay now turns to the default element of its model for information property.

2.2 Defaults

As a further safeguard to promote individual choice, this Essay supports the use of defaults. It 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, 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 consideration of the design and the effects, both positive and negative, of both a long-established German

[12] 18 U.S.C. § 2710(b) (2000).

[13] *Id.*

[14] 18 U.S.C. §§ 2721-2725 (2000). For a discussion of the DPPA, *see* PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW 32-34 (1st Ed. 1996 & Supp. 1998).

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."[15] 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).[16] 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.[17]

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. These privacy rules require financial entities to mail annual privacy notices to their customers.[18] Moreover, consistent with the model that I have proposed, the GLB Act incorporates a transferability restriction.[19] 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.[20] Thus, 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-

[15] 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).

[16] Otto Mallman, § 6, in KOMMENTAR ZUM BUNDESDATENSCHUTZGESETZ 545-47 (Spiros Simitis ed., 5th ed. 2003) [hereinafter BDSG Treatise].

[17] 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 17, at 1, 14-24.

[18] 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)).

[19] *See id.* § 502 (codified at 15 U.S.C. § 6802 (2000)).

[20] *See id.* § 502(a) (codified at 15 U.S.C. § 6802(a) (2000)).

transferability restriction, combined with a default regime, can lead to optimal information-sharing. Consistent with the privacy model proposed by this Essay, the GLB Act obligates the relatively better-informed parties – financial institutions – to share information with 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. 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.

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. 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 Essay's doubts about the efficacy of an opt-out rule: an opt-out rule creates incentives for financial entities to draft privacy notices that lead to consumer inaction.

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.[21] These agencies, the 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.[22]

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

[21] *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)).

[22] *See* Fed. Trade Comm'n, *Getting Noticed: Writing Effective Financial Privacy Notices* 1-2 (October 2002), *available at* http://www.ftc.gov/bcp/conline/pubs/buspubs/getnoticed.pdf.

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 should only be one of several elements in any privacy-sensitive propertization scheme for personal data. 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. Because better information may not cure market failure, the effect of information-forcing defaults should be bolstered through use-transfer restrictions and other protection mechanisms, such as a right to exit.

2.3 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."[23] 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

[23] Hanoch Dagan & Michael A. Heller, *The Liberal Commons*, 110 YALE L.J. 549, 568 (2001) (*citing* Laurence H. Tribe, AMERICAN CONSTITUTIONAL LAW §§ 15-17, at 1400-09 (2d ed. 1988)).

having long-term consequences. 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 shared values and excluding bad cooperators."[24] 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.[25] Slamming refers to changes made to a customer's carrier selection without her permission.[26] 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 Essay returns to the issues of notice and privacy-promoting institutions below.

[24] *Id.* at 571.

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

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

2.4 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.[27] 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."[28] They contrast this approach with a state determination of damages, which they associate with a "liability rule."[29] This Essay'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*. Second, an individual's personal data may not have a high enough market value to justify the costs of 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. 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. 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

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

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."[30] 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."[31] 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."[32]

2.5 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," it is also an institution that depends on other entities for its shape and maintenance.[33] 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). These organizations license performance rights in nondramatic musical compositions and distribute royalties to artists. 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.

These requirements in turn create a dynamic of institution-building. 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

[30] 18 U.S.C. § 2710(c)(2) (2000).
[31] *Id.* § 2724.
[32] 47 U.S.C. § 551(f) (2000).
[33] Carol M. Rose, *Canons of Property Talk, or, Blackstone's Anxiety*, 108 YALE L.J. 601, 632 (1998).

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 such institutions. 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.[34] 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 Essay'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). 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."[35] These institutions would pool information assets and sell them in "baskets" on a National Information Exchange. They would also allocate the resulting compensation, minus a charge for their services, to the individuals whose information comprises a given basket.

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." Unfortunately, this single market might also encourage privacy violations because its

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

[35] Kenneth C. Laudon, *Markets and Privacy*, COMMUNICATIONS OF THE ACM, Sept. 1996, at 100.

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)."[36] He writes: "Every participating citizen would be assigned an NIA with a unique identifier number and barcode symbol."[37]

In contrast, this Essay 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. 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.

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.[38] 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.

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. Its jurisdiction in these cases is predicated, however, on a company making false representations regarding its privacy practices.[39] These false promises must constitute "unfair or

[36] *Id.*

[37] *Id.*

[38] 47 U.S.C. § 227(b)(1) (2000).

[39] For information on the FTC's enforcement role, *see* Federal Trade Commission, *Privacy Initiatives: Introduction*, *available at* http://www.ftc.gov/privacy/index.html (last visited Apr. 10, 2004).

deceptive trade practices" under the Federal Trade Commission Act for the FTC to have jurisdiction.[40] 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.

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. Innovative approaches involving multiple institutions are necessary. Thus, as noted, this Essay 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.[41] The Children's Online Privacy Protection Act further decentralizes this institutional model.[42] It permits a state attorney general to bring civil actions "on behalf of residents of the State."[43] Similarly, the Telephone Consumer Protection Act (TCPA), which places restrictions on junk faxes and telemarketing, allows suits by state attorneys general.[44]

In addition, some privacy laws have added a private right of action to this mixture. Such laws include the TCPA, Video Act, Fair Credit Reporting Act, Cable Privacy Act, and Electronic Communication Privacy Act.[45] 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.

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. This governmental entity would assist the general public, privacy

[40] Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1680 (1999).

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

[42] 15 U.S.C. § 6504 (2000).

[43] *Id.*

[44] 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).

[45] *See* 47 U.S.C. § 227(b)(3) (2000); 18 U.S.C. § 2710(c) (2000); 15 U.S.C. §§ 1681n-1681o (2000); 47 U.S.C. § 551(f) (2000); 18 U.S.C. § 2707 (2000).

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.[46]

3. TRACKING CHIPS: WEARABLE VERSUS IMPLANTABLE CHIPS

This Essay now turns to the VeriChip, an implantable tracking device, and the wOzNet, a wearable device. It assesses the proper application of this Essay's five-part model involving inalienabilities, defaults, a right of exit, damages, and institutions.

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 Essay'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.[47] 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

[46] David H. Flaherty, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES: THE FEDERAL REPUBLIC OF GERMANY, SWEDEN, FRANCE, CANADA, AND THE UNITED STATES 394-97 (1989).

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

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 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 Margaret Radin's concept of the double bind.[48] 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."[49] Drawing on examples involving trade in sex, children, and body parts, Radin contends that commodification of certain things will harm us. 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."[50] More concretely, the double bind is the "practical dilemma of nonideal justice" – 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.[51] As an example, a ban on surrogate motherhood, which Radin ultimately supports, harms poor women who will miss out on the possible economic benefit from selling their reproductive capacity.

In contrast to surrogacy, a ban on implantable chips will not disadvantage

[48] Margaret Jane Radin, CONTESTED COMMODITIES 123-130 (1996).
[49] *Id.* at 156.
[50] *Id.* at 123.
[51] *Id.* at 124.

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. 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 Essay. 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. 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." 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 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.

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.

4. CONCLUSIONS

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 Essay's goal has been to develop a model for the propertization of personal information that also exhibits sufficient sensitivity to attendant threats to personal privacy. It 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.

This Essay 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 Essay's model for propertized personal information.

As Dagan has argued, property is a human creation, the form of which can be altered to meet human needs and reflect human values.[52] In this light, this Essay 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

[52] Dagan, supra note 5, at 1532.

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.