1-1-2005

Privacy Inalienability and the Regulation of Spyware

Paul M. Schwartz
Berkeley Law

PRIVACY INALIENABILITY AND THE REGULATION OF SPYWARE

By Paul M. Schwartz

TABLE OF CONTENTS

I. 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 such a privacy-promoting 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 model follows personal information through downstream transfers and limits the negative effects that result from "one-shot" permission to all personal data trade.

After developing a privacy-sensitive model for personal data trade in Part II, this Article uses it to evaluate a recent federal bill, H.R. 29 (entitled the Securely Protect Yourself Against Cyber Trespass Act (SPY ACT)), that seeks to regulate spyware. A controversial application of networked computing, spyware is a program that "install[s] itself without your permission, run[s] without your permission, and use[s] your computer without your permission."[1] 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 deliver-

1. Tracy Baker, *Here's Looking at You, Kid: How To Avoid Spyware*, SMART COMPUTING, Sept. 2003, at 68.

ing adware or targeted advertisements to individuals surfing the Web.[2] This Article finds some strengths, but also numerous weaknesses in the proposed legislation.

II. THE FIVE ELEMENTS OF PROPERTY IN PERSONAL INFORMATION

In this Part, I develop an approach to data trade that responds to weaknesses in the current "privacy market."[3] Currently, the existing market for exchanges of personal information does not promote data trades capable of responding to different privacy preferences. In this Article, I largely focus on a strategy for transformation of the existing privacy market to match each individual's preferred privacy characteristics. It is important to note, however, that the value of information privacy also accrues beyond the individual. A privacy commons can function as an important type of public good, like clean air or national defense.

A. Inalienabilities

Propertized personal information requires the creation of inalienabilities to respond to the problem of market failure. According to Susan Rose-Ackerman's definition, an "inalienability" is "any restriction on the transferability, ownership, or use of an entitlement."[4] 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 Section first analyzes this combination and then discusses why this hybrid inalienability should include a recourse to defaults.

The current privacy market fails—in part—by providing, at best, only one opportunity to refuse an information collector's overtures. Both downstream data use and subsequent transfers of personal information may exacerbate market shortcomings. Indeed, a variety of devices and systems that commodify information lead to downstream uses and onward trans-

2. *Id.* Adware performs much the same function as some spyware by delivering targeted advertising content to computer users. The definitional line between the two depends on whether the computer user receives adequate notice of the program's installation.

3. This Part provides abridged versions of arguments that I have developed at greater length elsewhere. *See* Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055 (2004).

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

fers.[5] 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.[6] 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 one-shot permission for data trade, this Article proposes a model that combines limitations on use with limitations on transfer. Under this approach, property rights are an interest that "run[] with the asset"; the use-transferability restrictions follow the personal information through downstream transfers and thus limit the potential third-party interest in such information. Specifically, 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, this model would permit the transfer of personal data for an initial category of use, 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. 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.

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 information transferees provide notice of privacy practices to information owners. A critical issue will be the "frame" in which transferees present information about data processing.[7]

5. For expansion of this argument, see Schwartz, *supra* note 3, at 2096-98.

6. *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, 1230-32, 1241-44 (2002).

7. For more details regarding this argument, see Schwartz, *supra* note 3, at 2099.

Second, meaningful disclosure requires addressing what Henry Hansmann and Reinier Kraakman term "verification problems."[8] As they explain, "[a] verification rule sets out the conditions under which a given right in a given asset will run with the asset."[9] 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 to identify the specific rules that apply to it. In the context of propertized personal information, the requirement for verification creates a role for non-personal metadata, a tag or kind of barcode, to provide necessary background information and notice.

B. Defaults

As a further safeguard to promote individual choice, this Article advocates the use of defaults. It prefers an opt-in default because it would be information-forcing—that is, this approach places pressure on the better-informed party to disclose material information about how personal data will be used.[10] 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.[11]

The strengths of the proposed model can be illustrated through a consideration of the design and the effects, both positive and negative, of a recent American statute. In the United States, the Gramm-Leach-Bliley Act (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.[12] Moreover, consistent with the model that I have proposed, the GLB Act incorporates a transferability

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

9. *Id.*

10. For a more detailed discussion of the merits of opt-in defaults, see Schwartz, *supra* note 3, at 2103. For the classic discussions of opt-in rules in the context of contract, see Ian Ayres & Robert Gertner, *Filling Gaps in Incomplete Contracts: An Economic Theory of Default Rules*, 99 YALE L.J. 87, 93 (1989); Ian Ayres & Robert Gertner, *Strategic Contractual Inefficiency and the Optimal Choice of Legal Rules*, 101 YALE L.J. 729, 761 (1992).

11. *Id.*

12. 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. §§ 6821-27 (2000)).

restriction.[13] Unlike this Article's 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.[14] 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-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 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.[15] 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.[16]

An opt-in rule is, therefore, an improvement over an opt-out rule because 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 this entitlement. In addition to having a positive impact on the privacy market, the opt-in regime also promotes social investment in privacy.

13. *See id.* § 502 (codified at 15 U.S.C. § 6802 (2000)).
14. *See id.* § 502(a) (codified at 15 U.S.C. § 6802(a) (2000)).
15. *See id.*
16. *See id.* § 502 (codified at 15 U.S.C. § 6802).

However much the opt-in default regime may promise, 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.[17] 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.[18] 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 of exit.

C. 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."[19] The right of exit, for example, would allow people to disable spyware and adware on the Internet. For the privacy market, a right of exit prevents initial bad bargains from having long-term consequences. For the privacy commons, moreover, 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."[20]

Providing a chance to withdraw is especially important in the context of data trade because current standards afford little protection to privacy. Once companies are able to establish a low level of privacy as a dominant

17. Janger & Schwartz, *supra* note 6, at 1244-45.

18. *Id.* at 1237-38, 1240.

19. 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)).

20. *Id.* at 571.

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. 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 of 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.

A 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. Indeed, these deceptive information collectors may also generally hinder a privacy market from forming around an opt-in regime; they might be able to do so by scaring off consumers from privacy-friendly data collectors.

D. Damages

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.[21] Second, an individual's personal data may not have a sufficiently high market value to justify the costs of litigation. Finally, due to the difficulty of detection, many violations of privacy promises will themselves remain private. Spyware provides an 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, the monetary amount of damages should be set higher or lower de-

21. Shibley v. Time, Inc., 341 N.E.2d 337, 339 (Ohio Ct. App. 1975) (holding that the sale of magazine subscription lists to direct mail advertisers does not constitute a tortious appropriation of personality because "[t]he right of privacy does not extend to the mailbox"); Dwyer v. Am. Express Co., 652 N.E.2d 1351, 1356 (Ill. App. Ct. 1995) (holding that the sale of a credit card company's profiles of customers' spending behaviors does not deprive the cardholders of any value their personality might have).

pending on the probability of detection of the violation. Since many privacy violations have a low probability of detection, damages should be relatively high.

A state determination of damages through privacy legislation is preferable to an 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. State determination of a damages schedule will encourage companies to keep privacy promises so long as the damages are set 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. This "free riding" on increased privacy protection is a useful result of a statute that permits liquidated damages.

Existing privacy law sometimes adheres to this path by either collectively setting damages or relying on liquidated damages. The Video Privacy Protection Act allows a court to "award . . . actual damages but not less than liquidated damages in an amount of $2,500."[22] The Driver's Privacy Protection Act contains 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."[23] 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."[24]

E. Institutions

Institutions shape the legal and social structure in which property is necessarily embedded. Many types of property depend on institutional entities for their shape and maintenance.[25] For example, automobiles are a 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 legal requirements in turn create a

22. 18 U.S.C. § 2710(c)(2) (2000).

23. *Id.* § 2724(a).

24. 47 U.S.C. § 551(f) (2000).

25. Carol M. Rose, *Canons of Property Talk, or, Blackstone's Anxiety*, 108 YALE L.J. 601, 632 (1998).

dynamic of institution-building, involving public and private entities. Private companies compete to provide insurance. In California, registration of one's automobile involves hiring a private service station to test the smog emissions of automobiles as part of registration, but recourse to a state official to check one's mileage and Vehicle Identification Number.

Without these institutions automobiles could certainly exist, but their use would be more polluting (no smog inspections), more dangerous (no safety inspections by specialists), and more risky (no insurance for the inevitable occurrence of accidents). In other words, the value of automobiles would be lower in relation to their disadvantages in the absence of institutions.

Likewise, personal data would possess higher value through the intervention of institutions that shape the rights and responsibilities associated with such property. 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.

As to the first role of institutions, differing proposals for market-making institutions have appeared, some advocating a centralized market and some advocating a decentralized market. In a detailed proposal to create a central National Information Market ("NIM"), Kenneth Laudon calls for development of "National Information Accounts (NIAs) for suppliers (individuals and institutions) and buyers (information brokers, individuals, and institutions)."[26] In his vision of a single information market, Laudon writes: "Every participating citizen would be assigned an NIA with a unique identifier number and barcode symbol."[27]

While such a system serves the market-making function, it possesses the flaw that a single market might encourage privacy violations because its centralized nature makes it an easy target for attacks. Once someone breaks into the bank, all that it holds within is imperiled. By contrast, decentralized methods of information exchange can handle the market-making function while simultaneously proving to be an elusive target for attack. Such a system would rest on a multiplicity of dealer-customer con-

26. Kenneth C. Laudon, *Markets and Privacy*, COMMS. OF THE ACM, Sept. 1996, at 92.

27. *Id.* at 100.

tacts and sales points rather than a central repository and meeting place for information providers and consumers.

As for the second role of institutions, 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. 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. These submarkets might in turn offer the possibility to provide examples of "best privacy trading practices" to be used elsewhere. 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.

In order to meet the third function of institutions, oversight, data trading laws should allow citizens to participate in protecting their own rights through private rights of action, including class actions, when those rights are violated. This approach builds on the proposals regarding damages that this Article makes above. Such rights of action provide many swords, decentralized among the property holders, whose prodding 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.[28] 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 Federal Trade Commission (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.[29] Yet, even with a specific grant of authority, the FTC would likely be over-

28. 47 U.S.C. § 227(b)(1) (2000).

29. For information on the FTC's enforcement role, see Federal Trade Commission, *Privacy Initiatives: Introduction*, http://www.ftc.gov/privacy/index.html (last visited Aug. 22, 2005).

whelmed if it were the sole institution responsible for policing the personal information market. Innovative approaches involving multiple institutions are necessary. Thus, as noted, this Article favors a decentralized institutional model.

III. H.R. 29 AND SPYWARE

This Article now turns to spyware. How does a recent bill, H.R. 29, for regulating spyware compare with the model that this Article has developed? Introduced by Representative Mary Bono, H.R. 29 is titled the Securely Protect Yourself Against Cyber Trespass Act or SPY ACT. Although it is not without some positive aspects, H.R. 29 falls short in a number of areas.

First, concerning inalienabilities, recall that this Article calls for a use-transferability restriction plus an opt-in default. Transfer should be permitted for an initial category of use of personal data, but only if the transferee grants the customer an opportunity to block further transfer or use by unaffiliated entities. Any further use or transfer would require the customer to opt-in. H.R. 29 does set some use-transfer restrictions. It requires subsequent notice and consent from the "person who transmitted the program" if a program collects or transfers information "for a purpose that is materially different from, and outside the scope of, the type or purpose set forth in the initial or any previous notice."[30]

Moreover, H.R. 29 carefully tries to regulate the way that consumers receive notice of privacy practices to reduce the possibility for vague notice leading to uninformed consent. The proposed statute carefully defines the terms for notice and consent, which are to include "a clear description" of matters such as "the types of information to be collected and sent (if any) by the information collection program"; "the purpose for which such information is to be collected and sent"; and "the identity of any such software that is an information collection program."[31] The bill even spells out some of the language that is to be included in notices, such as "This program will collect and transmit information about you. Do you accept?"[32] Finally, H.R. 29 also gives a role to the FTC in further defining standards for notice.[33]

30. H.R. 29, 109th Cong. § 3(c)(3)(B) (2005).
31. *Id.* § 3(c)(1)(D).
32. *Id.* § 3(c)(1)(B)(i).
33. *Id.* § 3(c)(4).

Less successfully, however, this statute does not overcome what this Article has termed "verification problems."[34] Third parties will be unable to verify that a given piece of personal information has, in fact, been propertized and to identify the specific rules that apply to it. Interestingly enough, H.R. 29 does take a small step in the direction of verification in its requirement of an "identity function."[35] The statute mandates a function in a program so "that each display of an advertisement . . . is accompanied by the name of the information collection program, a logogram or trademark used for the exclusive purpose of identifying the program."[36] The identity function allows the user to know that she should link adware to a given program on her computer.

Regarding defaults, this Article has argued in favor of opt-in to avoid placing the burden of bargaining on the less-informed party, the individual consumer. H.R. 29 does require opt-in; information will not be collected unless the individual selects "an option to grant or deny consent."[37] It also safeguards the ability of individuals to walk away from a transaction in the middle of it—notice must allow the option to "abandon or cancel the transmission or execution . . . without granting or denying . . . consent."[38] In other words, inaction following notice will mean that personal data will not be collected.

H.R. 29 also provides for a more complete right of exit—one that follows an initial agreement. The statute terms this capability a "disabling function."[39] An information collection program is to allow "a user of the program to remove the program or disable operation" of the program.[40] Here, the drafters of the statute attempted to respond to warnings about what one industry expert termed "unrealistic uninstall requirements."[41] As Jeffrey Friedberg of Microsoft testified before Congress, "Requiring standardized uninstall practices for all software would be unworkable in many circumstances."[42] Friedberg was concerned about instances "where a full and complete uninstall is neither technically possible nor desirable, such

34. Hansmann & Kraakman, *supra* note 8, at S384.
35. H.R. 29, § 3(d)(2).
36. *Id.*
37. *Id.* § 3(c)(1)(C).
38. *Id.*
39. *Id.* § 3(d)(1).
40. *Id.*
41. *Safeguards Against Privacy Invasions Act: Hearing on H.R. 2929 Before the H. Subcomm. on Commerce, Trade, and Consumer Protection of the H. Comm. on Energy and Commerce*, 108th Cong. (2004), *available at* http://www.microsoft.com/presspass-/exec/friedberg/04-29spyware.mspx (testimony of Jeffrey Friedberg).
42. *Id.*

as with a software component that is in use and shared by other programs."[43] In addition, Friedberg warned about "situations where requiring uninstall could actually comprise the security of the system, such as backing out security upgrades or removing critical services."[44]

These concerns have some validity. Unfortunately, H.R. 29 responds to them with opaque language capable of covering evasion of its requirements. The proposed statute limits its requirement of disabling an information collection program to "a function that . . . (A) is easily identifiable to a user of the computer; and (B) can be performed without undue effort or knowledge by the user of the protected computer."[45] This language provides all too ample possible loopholes for spyware purveyors; they will likely argue that their program cannot easily be identified or that removing it requires undue effort or knowledge.

The proposed spyware statute also contains provisions for damages. This Article has proposed use of liquidated damages and has argued in favor of both FTC-enforcement and private rights of action. In contrast, H.R. 29 gives the FTC an oversight role but ignores the benefits of decentralization of enforcement. The FTC is to enforce H.R. 29 under both the Federal Trade Commission Act and in cases of a "pattern or practice" that violates core provisions of the Act, it may seek civil penalties.[46] H.R. 29 adds that the remedies that it proposes are to be exclusive ones.[47] In this fashion, the proposed statute makes explicit its intention to close the door to any private enforcement actions.

Finally, this Article has proposed an essential role for institutions in promoting a well functioning market for data trade. It has called for institutions that fulfill 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). H.R. 29 falls considerably short of providing strong institution-building directives. Admittedly, it may be asking too much of any single statute for it to fulfill all three functions. One is left wondering, however, whether a privacy-promoting market can possibly emerge upon the enactment of this statute.

H.R. 29 does not formally respond to a need for multiple decentralized markets for data exchanges. Assuming well-defined property rights and no transaction costs, a Coasian model would expect these markets to spring

43. *Id.*
44. *Id.*
45. H.R. 29, § 3(d)(1).
46. *Id.* § 4(a).
47. *Id.* § 4(c).

up. As Ronald Coase proposed, "It is always possible to modify by transactions on the market the initial legal determinations of rights. And, of course, if such market transactions are costless, such a rearrangement of rights will always take place if it would lead to an increase in the value of production."[48] Here, the lack of verification mechanisms is especially troubling. Although the statute does require a limited identity function, as noted above, H.R. 29 does not develop approaches for linking information with the person who has the property interest in trading the information. Regarding the final provision of this Article's model, which concerns policing compliance, the proposed statute assigns an exclusive enforcement role to the FTC. As this Article has argued, however, this approach is likely to lead to under-enforcement of the rights that H.R. 29 creates.

Two questions remain. First, is H.R. 29 the best privacy-promoting bargain likely to be enacted by Congress? Second, are there elements of a privacy-promoting market for data trade that Congress can comfortably enact initially, with confidence that the other elements will follow in time? This Article leaves these thorny issues for another day and publication.

IV. CONCLUSIONS

A strong conception of personal data as a commodity is emerging in the United States, and individual Americans already participate in the commodification of their personal data. This Article'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. Unfortunately, H.R. 29 does not attend sufficiently to all five areas.

Despite some strengths, such as its structuring of notice and consent to help create inalienabilities, H.R. 29 fails to overcome verification difficulties in the information privacy market and allows a considerable loophole in its attention to the right of exit. The statute also falls short regarding damages, where the proposed law does not include a private right of action, and regarding institutions. This Article concluded by raising, and leaving open, questions that addressed whether or not H.R. 29 might provide a better response than no spyware legislation at all.

48. Ronald Coase, *The Problem of Social Cost*, 3 J.L. & ECON. 1, 15 (1960).