

2003

Privacy Property, Information Costs and the Anticommons

Edward J. Janger

Brooklyn Law School, edward.janger@yale.edu

Follow this and additional works at: <https://brooklynworks.brooklaw.edu/faculty>



Part of the [Other Law Commons](#), and the [Privacy Law Commons](#)

Recommended Citation

54 *Hastings L. J.* 899 (2002-2003)

This Article is brought to you for free and open access by BrooklynWorks. It has been accepted for inclusion in Faculty Scholarship by an authorized administrator of BrooklynWorks.

Privacy Property, Information Costs, and the Anticommons

by
EDWARD J. JANGER*

As Paul Schwartz and Joel Reidenberg have pointed out in their treatise on data privacy law, the current law of privacy is a hodgepodge of rights and remedies.¹ Some rights arise out of a specific statute, others arise out of the general common law of torts and contract. Each system for protecting privacy has its own distinctive remedial scheme. Some rights are backed by public enforcement alone, some by private rights of action, some by both. Some come with compensatory damages, others with attorneys' fees, punitive damages, or statutory damages. Even where a private right of action exists, however, that right is often enforced by civil liability, rather than property-based entitlements. In this essay, I will argue for a switch to property-based protection of personal data, but my principle task will be to take seriously (and propose techniques for minimizing) the costs associated with a regime of information property.

In an earlier article, I examined the enforcement of privacy rights held by individuals against private sector actors and asked three questions: (1) whether those rights should be cast in the form of

* Associate Professor of Law, Brooklyn Law School. Special thanks to Paul Schwartz, Henry Smith, Edward Rubin, A. Douglas Melamed, Peter Swire, and my copanelists Joel Reidenberg, Ron Plessner, Susan Henrichsen, and Lisa Rosenthal, for comments on an earlier draft. I also wish to thank Lynn LoPucki for disagreeing forcefully with an earlier piece and forcing me to think more carefully about the costs of protecting information privacy. I am indebted to Sandra Rampersaud, Matthew Cohen, and Chris Christon for excellent research assistance and to the Dean's Research Fund of the Brooklyn Law School for generous financial support of this project. Mistakes are, of course, mine alone.

This paper was originally presented at *Enforcing Privacy Rights*, a symposium sponsored by the Samuelson Law, Technology, and Public Policy Clinic at Boalt Hall School of Law, University of California, Berkeley; the Institute for Law and Economic Policy; and the *Hastings Law Journal*, November 15–16, 2002.

1. See generally PAUL M. SCHWARTZ & JOEL R. REIDENBERG, *DATA PRIVACY LAW* (1996 & Supp. 1998).

“property”- or “liability”-based rules, (2) whether they should be default rules (i.e., alienable) or mandatory rules (i.e., inalienable), and (3) whether they should be cast as rules or standards.² In that piece, I explained why I am concerned that the use of liability rules may lead to underenforcement and underarticulation of privacy norms; why I doubt that private contract is an appropriate device for specifying duties with regard to non-public personal information; and why, given the current unsettled state of consumer knowledge about how information is used, unformed consumer expectations about secondary use, and the rapid rate of technological change, I believe that crystalline safe harbors for personal information transactions are inappropriate.³

I therefore advocated a regime of “mandatory muddy property rules” for information privacy to encourage the common law development of data privacy norms.⁴ I will rehearse some of that argument here, and take the discussion a step further.

That earlier piece began a dialogue with two distinct clusters of property theorists.⁵ The first cluster I call the “norm-enforcing property theorists.” They include (though they might not characterize themselves as such) Lawrence Lessig,⁶ Lynn LoPucki,⁷ and myself.⁸ The second cluster—the “cost minimizers”—is exemplified by the work of Thomas Merrill and Henry Smith,⁹

2. Edward J. Janger, *Muddy Property: Generating and Protecting Information Privacy Norms in Bankruptcy*, 44 WM. & MARY L. REV. 1801, 1808 (2003).

3. *Id.* at 1809–17.

4. *Id.* at 1866–73.

5. *Id.* at 1801–02.

6. See LAWRENCE LESSIG, *THE FUTURE OF IDEAS* 240–61 (2001).

7. See Lynn M. LoPucki, *The Unsecured Creditor's Bargain*, 80 VA. L. REV. 1887, 1898–99 (1994) [hereinafter LoPucki, *Creditor's Bargain*]. I suspect that Professor LoPucki would be surprised at finding himself on this list since he takes a very different view of privacy rights than that articulated in this paper. See Lynn M. LoPucki, *Did Privacy Cause Identity Theft?*, 54 HASTINGS L.J. 1277 (2003). However, there are strong parallels between the arguments he makes in the torts context, those I make in the privacy context, and those Lessig makes in the intellectual property context. The difference between us turns not on property theory, but upon the norms we would choose to use property law to enforce.

8. See Edward J. Janger, *Crystals and Mud in Bankruptcy Law: Judicial Competence and Statutory Design*, 43 ARIZ. L. REV. 559, 584–86 (2001); Janger, *supra* note 2, at 1859; Carol M. Rose, *Crystals and Mud in Property Law*, 40 STAN. L. REV. 577, 600 (1988).

9. See Thomas W. Merrill & Henry E. Smith, *Optimal Standardization in the Law of Property: The Numerus Clausus Principle*, 110 YALE L.J. 1, 8 (2000) [hereinafter Merrill & Smith, *Numerus Clausus*]; Thomas W. Merrill & Henry E. Smith, *The Property/Contract Interface*, 101 COLUM. L. REV. 773, 778 (2001) [hereinafter Merrill & Smith, *Property/Contract Interface*].

Michael Heller,¹⁰ and Henry Hansmann and Reinier Kraakman.¹¹ For these purposes, my earlier work falls into the norm-enforcing camp, and it is from that perspective that I will take on the cost minimizers.

The dispute runs something like this: New forms of property are being created by law,¹² contract,¹³ and even by technology¹⁴ to help order the new economy. The role of law in regulating these new types of property is up for grabs, and raises a number of crucial questions: Should new types of property be created? If so, what institutions should create those property rights, and how should they be defined?

On one end of the spectrum, Merrill and Smith argue descriptively that property rights come in a limited number of standardized forms, and prescriptively, that such standardized forms help third parties to identify the bundle of rights held by the owner.¹⁵ On the other hand, Lawrence Lessig, in the context of copyright, Lynn LoPucki, in the context of tort law, and I, in the context of data privacy, have argued that property rights can be shaped by social policy concerns.¹⁶ For Lessig, intellectual property carries with it both a monopoly and a responsibility.¹⁷ As such, he would impose limits on

10. See Michael A. Heller, *The Boundaries of Private Property*, 108 YALE L.J. 1163, 1173-74 (1999) [hereinafter Heller, *Boundaries*]; Michael A. Heller, *The Tragedy of the Anticommons: Property in the Transition from Marx to Markets*, 111 HARV. L. REV. 621, 665-67 (1998) [hereinafter Heller, *Tragedy*].

11. See Henry Hansmann & Reinier Kraakman, *Property, Contract, and Verification: The Numerus Clausus Problem and the Divisibility of Rights*, 31 J. LEGAL STUD. 373, 374 (2002).

12. The Digital Millennium Copyright Act extends the protection accorded to digital information and brings new types of information within the scope of copyright protection. See Pub. L. No. 105-304, 112 Stat. 2860 (1998). Also, privacy advocates have argued for the propertization of non-public personal information. In Europe, this is already happening as a result of the European Union's Privacy Directive. Council Directive 95/46, 1995 O.J. (L 281/31). In the United States, personal information is protected principally by contract and tort law (and, as discussed below, by a number of statutes of narrow application), but there are a number of legislative proposals on the horizon.

13. New forms of software licensing arrangements are a staple of the "new" economy.

14. As Lessig points out, even in the absence of governing law, technologies, such as "trusted systems" can be used to prevent unauthorized access to intellectual property. LAWRENCE LESSIG, *CODE AND OTHER LAWS OF CYBERSPACE* 129-30 (1999).

15. Merrill & Smith, *Numerus Clausus*, *supra* note 9, at 8:

When property rights are created, third parties must expend time and resources to determine the attributes of these rights, both to avoid violating them and to acquire them from present holders. The existence of unusual property rights increases the cost of processing information about all property rights. Those creating or transferring idiosyncratic property rights cannot always be expected to take these increases in measurement costs fully into account, making them a true externality. Standardization of property rights reduces these measurement costs.

16. See *supra* notes 6-8.

17. LESSIG, *supra* note 14, at 127.

the scope of intellectual property rights to further the goals of innovation inherent in the copyright and patent laws.¹⁸ In my own work, I have explored how “muddy property rules” can be used to encourage the articulation of information privacy norms, while crystalline rules can place too much faith in the market, particularly in consumer contexts or where public goods are involved.¹⁹ Finally, LoPucki has argued that tort claims should be given priority over secured claims (in effect a superpriority lien), in order to encourage debtors to make reasonable investments in safety, and to encourage secured creditors to monitor that investment.²⁰ The questions are thus: (1) Should we respect the *numerus clausus* (the existing, limited forms of property); and (2) should property rights be crystalline and standardized to facilitate contracting, or should they be muddy and laden with regulatory and/or normative content to encourage norm articulation and enforcement?

While norm-enforcing property rights have important benefits, they also impose costs²¹ that should be taken seriously. In this Article, I wish to explore these costs of muddy norm-laden property regimes in the information privacy context, and to propose a number of devices that may help capture the benefits, and reduce the costs of muddy information property.

This paper will proceed in five brief steps. Part I will identify the existing sources of privacy entitlements under current law, and the applicable remedial schemes. In this Part, I will show that, while in

18. *Id.*

19. Janger, *supra* note 2, at 1815–17. While my property-based approach to information privacy and Lessig’s approach to intellectual property are similar in structure, we actually disagree over the proper approach to information privacy. Lessig advocates a simple property regime for information privacy, LESSIG, *supra* note 14, at 161 (“A property regime thus protects both those who value their privacy more than others and those who value it less, by requiring that someone who wants to take a given resource must ask. Such a regime gives us confidence that if a trade occurs, it will be at a price that makes neither party worse off.”), but a muddy one for intellectual property, *id.* at 134 (“[T]he balance that intellectual property law traditionally strikes is between the protections granted the author and the public use or access granted everyone else. The aim is to give the author sufficient incentive to produce.”), whereas I would advocate muddy regimes for both.

20. LoPucki, *Creditor’s Bargain*, *supra* note 7, at 1963 (“The priority of secured creditors over involuntary unsecured creditors cannot be justified by any coherent theory and should be abolished. Involuntary creditors should have priority over voluntary creditors, whether secured or unsecured.”).

21. Merrill & Smith, *Numerus Clausus*, *supra* note 9, at 27–28:

[I]t is useful to distinguish three classes of individuals who might be affected by the decision to create idiosyncratic property rights, or fancies First are the *originating parties*, who are the participants to the transaction creating the fancy. . . . Second are the *potential successors in interest* to the asset that is being subjected to the fancy. . . . Finally, there are the *other market participants*. . . .

certain limited contexts, personal data is given property-like protection, to the extent that broadly applicable private rights of action exist to enforce privacy entitlements, they are enforced through liability rather than property.²² In Part II, I will explore certain costs and benefits associated with liability-based enforcement, and suggest that propertization holds out important promise. In Part III, I will merge the substance and remedy question somewhat, arguing that it is a mistake to try to solve the “remedy” problem without considering the “right” problem at the same time. If the goal is to enforce a right or a norm that is well understood by parties with equal bargaining power, then a crystalline property-based fully alienable right might be appropriate. If the norm is well understood, but there are expected to be bargaining problems such as information asymmetries or coordination problems, a mandatory crystalline inalienability rule might be appropriate. Finally, if the norm is not well understood or is difficult to articulate, one underappreciated goal of a remedial scheme may be to encourage norm articulation. Where this is the case, a muddy (or norm-dependent/norm-laden) property rule might be the appropriate choice. In Part IV, I will discuss the costs of muddy property, and develop some of the tradeoffs. Finally, in Part V, I will tentatively suggest two ways to reduce such costs, first, to create a regime of “muddy standardization,” and second, to create a summary collective procedure for pre-clearing transfers of personal information. I suggest that such a procedure might be modeled loosely on the bankruptcy procedure used for selling assets of the estate free and clear of liens, encumbrances, and other interests, pursuant to section 363(f) of the Bankruptcy Code. I conclude tentatively that, if muddy standardization is linked to such a summary proceeding for quieting title, property-based protection of information privacy may be beneficial.

22. While the Electronic Communications Privacy Act and the Video Privacy Protection Act both provide for equitable relief, these only apply in the limited context of “interception” of telephone and e-mail communication and the context of video rentals. *See infra* pp. 905–06. Peter Swire points out, and I am indebted to him for this insight, that the shift from property-based enforcement to liability-based or public enforcement may also have a temporal component. Statutes enacted since the early 1990s (i.e., after the VPPA), have limited the enforcement mechanism to public enforcement or liability-based private enforcement. Audio tape: Joint Program of Sections on Antitrust and Economic Regulation, Commercial and Related Consumer Law, Property Law, and Remedies, held at the Annual Meeting of the Association of American Law Schools (Jan. 2, 2003) (on file with author).

I. Private Rights of Action: Individual Compensation v. Enforcement of Public Policy Under the Existing Remedial Schemes

Since my topic is “private rights of action,” the first question that must be asked is what private rights of action exist to enforce information privacy, and to the extent that those rights exist, what remedies are available to enforce them? As a matter of scope, I will not, therefore, be talking about substantive entitlements enforceable against the government. Constitutional protections, such as the Fourth Amendment, and the rights to intimate and expressive association are beyond the scope of this Article. Also, though they are relevant, and mentioned, I will not principally be talking about public enforcement of privacy rights by government agencies, such as the FTC.²³ My focus will be on private enforcement rights, available to individuals who have been harmed.

As a general matter, the common law of torts provides some protection in some jurisdictions through the so-called tort of invasion of privacy.²⁴ More importantly, privacy protection may be engineered as a matter of private contract.²⁵ The privacy policies that appear on web sites are an attempt by web site owners to define their rights and obligations with regard to the information that they gather. In addition, context-specific, targeted statutes govern use of personal information in the private sector. These include the Video Privacy Protection Act (“VPPA”),²⁶ which protects the privacy of video rentals, the Gramm-Leach-Bliley Act (“GLB”),²⁷ which protects financial privacy, and the Fair Credit Reporting Act (“FCRA”),²⁸ which applies to credit reporting agencies. Each statute has its own distinct remedial scheme, and each shares a certain *ad hoc* quality. To give a few examples:

23. To the extent that enforcement schemes are being judged against a standard of “optimal” enforcement, my analysis does not include the possibility of government enforcement as part of the equation. This may lead to some undercounting. However, to the extent that privacy rights violations can be prevented by a property-based regime, they alleviate the need for public enforcement.

24. RESTATEMENT (SECOND) OF TORTS § 652B (1977); Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 213 (1890).

25. Janger, *supra* note 2, at 1823. See also Walter W. Miller, Jr. & Maureen A. O'Rourke, *Bankruptcy Law v. Privacy Rights: Which Holds the Trump Card?*, 38 HOUS. L. REV. 777, 799–807 (2001) (noting that while privacy policies may be enforceable as contracts, the damages are likely to be difficult to calculate).

26. 18 U.S.C. § 2710 (2000).

27. Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified in scattered sections of 12 and 15 U.S.C.).

28. 15 U.S.C. § 1681 (2000).

- The Driver's Privacy Protection Act ("DPPA") protects personal information collected by state motor vehicles departments from disclosure to other government officials, and to private parties.²⁹ It creates a private right of action for knowing violations,³⁰ and provides for payment of actual damages to the extent that they exceed \$2500, liquidated damages of \$2500 to the extent that the plaintiff is not able to prove greater damages, punitive damages for willful violations, an award of costs and a reasonable attorney's fee, and equitable relief.³¹ The DPPA also makes it a crime to knowingly violate the act.³²
- The Fair Credit Reporting Act provides a private right of action with a similar mix of actual, statutory, and punitive relief, coupled with attorney's fees.³³ However, under the FCRA, minimum statutory damages are only \$100, and actual damages are capped at \$1000, unless there was a "knowing" violation.³⁴ The FCRA does not provide for equitable relief, but it does provide for criminal penalties for "pretexting" (knowingly obtaining consumer information on false pretenses, in violation of the FCRA).³⁵
- The Children's Online Privacy Protection Act³⁶ ("COPPA") regulates disclosure of identifiable personal information about children gathered online, makes violation of the Act a deceptive trade practice within the meaning of the FTC Act,³⁷ and confers *parens patriae* jurisdiction on state attorneys general.³⁸ As such, enforcement of the COPPA is solely by public officials, not by private right of action.
- Similarly, the GLB requires certain financial institutions to provide their customers with notice of their privacy practices and a right to opt-out (i.e., prevent any

29. 18 U.S.C. § 2721 (2000).

30. *Id.* § 2724(a) ("A person who knowingly obtains, discloses or uses personal information from a motor vehicle record, for a purpose not permitted under this chapter shall be liable to the individual to whom the information pertains, who may bring a civil action in a United States district court.").

31. *Id.* § 2724(b).

32. *Id.* § 2723.

33. 15 U.S.C. § 1681n(a).

34. *Id.*

35. *Id.* § 1681(q).

36. *Id.* §§ 6501–06.

37. *Id.* § 6502(c).

38. *Id.* § 6504(a)(1).

disclosures to non-affiliated entities).³⁹ There is no private right of action.⁴⁰

- The Electronic Communications Privacy Act ("ECPA") protects the privacy of telephone and e-mail correspondence,⁴¹ and provides for civil damages, injunctive relief, and public equitable and criminal enforcement for violations.⁴²
- The VPPA does not provide for public enforcement, but provides the most extensive scheme for private enforcement, allowing actual damages, liquidated statutory damages of not less than \$2500, attorney's fees, and preliminary and equitable relief.⁴³

All of these statutes, except the VPPA, allow for public enforcement. Some provide for public enforcement only, while others allow for private enforcement as well.

As such, the various schemes can be divided into three broad categories: public enforcement, private enforcement, and dual enforcement. Where private enforcement is involved, two further divisions exist—those that protect information through liability-based protection, and those that give personal information "property"-like status (*see* Figure 1). For the most part, however, private remedies are cast in terms of compensatory damages, statutory damages, and attorney's fees. While three of the four statutes that provide for a private right of action allow for equitable relief (the ECPA, VPPA, and DPPA), those statutes cover only a narrow range of activities (video rentals, drivers' license data, and phone records). By contrast, the private right of action that applies to the broadest range of e-commerce activity, the FCRA, does not provide for equitable relief.⁴⁴ Moreover, the other, newer statutes, COPPA and GLB, do not provide for private enforcement at all. As such, private enforcement is left by and large to the common law of tort and contract and the principal remedy available for tortious acts and breach of contract is

39. Gramm-Leach-Bliley Act § 502, 113 Stat. at 1437–39. *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, 1224 (2002).

40. *Id.* at 1225.

41. 18 U.S.C. §§ 2510–20, 2701–09 (2000).

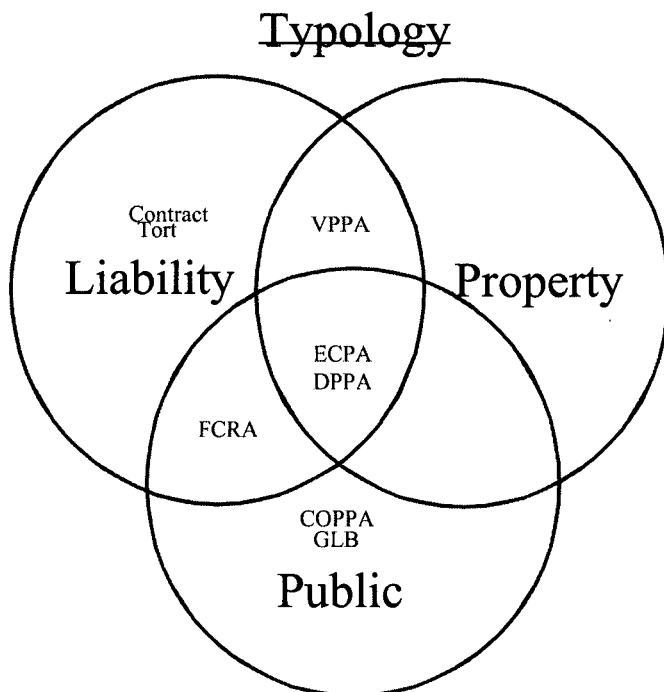
42. *Id.* §§ 2511, 2520, 2521, 2707.

43. *Id.* § 2710(c).

44. At least one court has read the fact that the FCRA grants injunctive power to the government but not as a private remedy as precluding such a remedy. *In re Trans Union Corp. Privacy Litig.*, No. 00 C 4729, 2002 WL 31028234, at **8–9 (N.D. Ill. Sept. 10, 2002). *Cf.* *Washington v. CSC Credit Serv.*, 199 F.3d 263, 268 (5th Cir. 2000) (Fair Credit Reporting Act's express grant of injunctive power to government and silence with regard to equitable relief in connection with private right of action clearly manifests an intent to preempt the district court's inherent equitable powers).

damages. Only in extraordinary cases are injunctions available, and in most cases, this will only be after a violation has already occurred.⁴⁵

Figure 1



To the extent that private rights of action exist, the purposes seem to be somewhat schizophrenic—torn between creating a party-driven scheme for public enforcement and providing a scheme for private compensation. While the common law rights are directed more toward compensation,⁴⁶ the statutory damages schemes provided for in the DPPA, VPPA, and FCRA appear to be directed at using private parties as an adjunct to, or substitute for, public enforcement. A common theme in each of the statutory remedial schemes is that recovering actual personal damages is not going to be a sufficient incentive to bring suit. This realization is further reflected in the complete reliance on public enforcement under GLB and

45. For reasons discussed below, specific performance and equitable relief may be available for invasions of privacy. As such, these rights may provide a version of the “muddy property” rights that I advocate. Because of the limited scope of the privacy tort, and the market imperfections involved in negotiating privacy policies, discussed below, they have not yet, and may never, become significant bulwarks of privacy protection.

46. The standard measure of damages in tort is to compensate the plaintiff for any harm to the plaintiff caused by the tortfeasor. The standard measure of damages in contract is to compensate the non-breaching party for any harm and any lost expectation.

COPPA, and in the addition of statutory damages and attorney's fees under the DPPA, VPPA, and FCRA. As such, these private rights of action must be looked at both in terms of their adequacy for individual compensation and their capacity for enforcing public norms through creating appropriate incentives. As I will discuss in the next section, an approach that "prices" violations rather than prohibiting them falls short on both measures.

II. Civil Liability and Its Limits

As noted above, while some targeted statutes grant the power to obtain an injunction, the broader FCRA does not,⁴⁷ and equitable remedies are not "ordinarily" available for contractual violations. Moreover, protection does not run with the information, even under the statutes that provide for equitable relief. Once information has been disclosed to a third party, there is nothing in any of these regimes that places restrictions on the use of the information by those who receive it in contravention of a duty of confidentiality. In short, the private rights of action that are available to protect most personal information are based principally in liability rather than property. In this section, I will explore the limits of liability-based protection.

There is a large literature on the distinction between property and liability rules, and a number of definitions of the two concepts have been used. For Calabresi and Melamed, the distinction between property and liability turns on remedy—in particular on whether the right is enforceable by damages or affirmative judicial sanction.⁴⁸ Hansmann and Kraakman make the difference turn on whether the right runs with the property and is enforceable against successors.⁴⁹ Finally, Merrill and Smith use a definition derived from the work of Wesley Hohfeld, calling property rights "multital" or "in rem" (running against the thing and good against the world) and liability rights "paucital" or "in personam" (running against the person).⁵⁰ Under any of these definitions, the remedies for violations of information privacy entitlements are liability-based. The defendant is

47. Indeed, in the *Trans Union* case, the court held that Congress' express grant of injunction power to the FTC under the FCRA, and the failure to so specify when granting a private right of action, manifested Congress' intent to preempt the district court's inherent equitable powers. *In re Trans Union*, 2002 WL 31028234, at **9–10.

48. Guido Calabresi & A. Douglas Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, 85 HARV. L. REV 1089, 1092–93 (1972).

49. Hansmann & Kraakman, *supra* note 11, at 378:

For our purposes, the attribute that distinguishes a property right from a contract right is that a property right is enforceable, not just against the original grantor of the right, but also against other persons to whom possession of the asset, or other rights in the asset, are subsequently transferred.

50. Merrill & Smith, *Property/Contract Interface*, *supra* note 9, at 778.

called upon to pay damages, not fined or imprisoned for contempt. Injunctions, where available, are prospective only, and once information is disclosed, no sanction runs against the recipient. The obligations do not inhere in the information itself, but run between the individual whose information is at stake and the person who has promised to keep it confidential.

Liability has its limits as a means of enforcing privacy rights. In particular, it is not likely to provide adequate enforcement of privacy norms or adequate compensation for privacy invasion for three reasons: (1) the "judgment proof" problem, (2) the fact that privacy harms are largely dignitary rather than monetary, and (3) the victims of privacy invasions are likely to face serious coordination problems.

A. Liability and the Judgment Proof Problem

A common attribute of many of the web sites and dot-coms of the late 1990s was that they were thinly capitalized. Moreover, many dot-com businesses "mined" personal data as an element of their business plan. They gathered personal data from their customers with the intention of selling it. When these companies began to fail in 2000, many sought to sell their customer data.⁵¹ To the extent that there were restrictions on the sale of personal data, they were self-imposed through published privacy policies. The *Toysmart.com* case is the classic example.⁵² There, a bankrupt online toy store sought to sell its customer list, and was challenged by the FTC.⁵³ There are other instances, both reported and unreported,⁵⁴ including recent

51. See Victoria Slind-Flor, *Privacy or Creditors: Who Holds the Trump?*, NAT'L L.J., Sept. 4, 2000, at A1 (forty-one dot-coms had shut down by August 8, 2000).

52. Stipulation and Order Establishing Conditions on Sale of Customer Information, *In re Toysmart.com*, No. 00-13995 (Bankr. D. Mass. July 20, 2000), available at <http://www.ftc.gov/os/2000/07/toysmartbankruptcy.1.htm> (last visited Mar. 25, 2003). See Jane Kaufman Winn & James R. Wrathall, *Who Owns The Customer? The Emerging Law of Commercial Transactions in Electronic Customer Data*, 56 BUS. LAW. 213, 227-28 (2001) ("Toysmart.com had retained the services of The Recovery Group, a Boston management consultant, in an effort to find buyers for its assets. A *Wall Street Journal* advertisement for Toysmart.com's asset sale listed, among other things: 'Intangibles, i.e., URL name, databases, customer lists, marketing plans, web site content, [and] software intellectual property.'"). The Toysmart case was widely reported at the time. See Matt Richtel, *Toysmart.com in Settlement with F.T.C.*, N.Y. TIMES, July 22, 2000, at C1; Laura Lorek, *When Toysmart Broke*, INTERACTIVE WK. FROM ZDWIRE, Aug. 7, 2000, available at 2000 WL 4067740. See also Stephen F. Ambrose, Jr. & Joseph W. Gelb, *Consumer Privacy Regulation and Litigation*, 56 BUS. LAW. 1157 (2001); Andrew B. Buxbaum & Louis A. Curcio, *When You Can't Sell to Your Customers, Try Selling Your Customers (But Not Under the Bankruptcy Code)*, 8 AM. BANKR. INST. L. REV. 395 (2000).

53. Stipulation and Order, *In re Toysmart.com* (No. 00-13995).

54. An online travel agency, eTour, Inc., sought to sell its customer lists to Ask Jeeves, Inc., and drew an objection from the Electronic Privacy Information Center. Letter from Marc Rotenberg and Andrew Shen to National Association of Attorneys General and

concerns raised about the possible sale of frequent flyer databases by bankrupt airlines.⁵⁵ These stories illustrate that the enforceability of these privacy policies is problematic where companies are insolvent. To the extent that privacy policies are contracts, the principal remedy is contract damages; contractual damages, however, are, as a general rule, dischargeable in bankruptcy.⁵⁶ Even if the debt were non-dischargeable,⁵⁷ which it is not,⁵⁸ to the extent that the debtor is liquidating and selling its data, recourse against an empty corporate shell is not worth much.

Legal economists have long recognized that the officers of companies that are insolvent (or nearly so) are faced with a number of morally problematic choices.⁵⁹ To honor their duty to shareholders, it may be a worthwhile gamble to violate a privacy policy, sell data, and hope that the additional money helps keep the business afloat. This is sometimes referred to as the “moral hazard” associated with insolvency. Even if the duty is to other creditors, the sale of data and breach of a privacy promise may bring in significant revenue that can then be distributed among the other claimants.⁶⁰ Thus, to the extent that the objects of privacy legislation are thinly capitalized entities, the efficacy of liability-based enforcement mechanisms is likely to be limited both inside and outside of bankruptcy.

B. Liability and “Lumping It”

Even where the party gathering data is not undercapitalized, liability-based privacy protections are not likely to provide efficient

Federal Trade Commission (May 25, 2001), *available at* <http://www.epic.org/privacy/internet/etour.html> (last visited Mar. 25, 2003).

55. Ryan Singel, *Frequent Fliers Fear Privacy Loss*, WIRED NEWS, Apr. 18, 2003, *available at* <http://www.wired.com/news/print/0,1294,58470,00.html> (last visited Apr. 19, 2003).

56. 11 U.S.C. § 1141 (2000).

57. *Id.* § 523.

58. *Id.*

59. For an introduction to the so-called “judgment proof” problem, see S. Shavell, *The Judgment Proof Problem*, 6 INT’L REV. L. & ECON. 45, 45 (1986) (“An injurer will treat liability that exceeds his assets as imposing an effective financial penalty only equal to his assets. . . .”). See also Lynn M. LoPucki, *The Death of Liability*, 106 YALE L.J. 1, 3 (1996):

Think of the liability system as a poker game. . . . Players risk their chips, that is, their wealth, by tossing them into the pot, that is, investing them in liability-generating economic activity. Chips contributed to the pot are at risk of loss; the system can take them to satisfy liability. Chips withheld are not at risk.

60. For contract-based relationships, the combined effect of the bankruptcy discharge, and the power to reject executory contracts encourages this result when the debtor is in bankruptcy. 11 U.S.C. §§ 365, 524. Indeed, the preference power sometimes allows the trustee to breach contractual obligations that the debtor sought to perform prior to bankruptcy. *Id.* § 547.

incentives to maintain privacy. A second shortcoming of liability-based remedies is the problem of “lumping it.” Invasions of privacy cause dignitary harm rather than financial harm in most cases, therefore a statute predicated on actual damages will not provide a significant incentive to bring suit. Even where statutory damages and attorney’s fees are available, the damages are not huge, and the risk associated with bringing suit will limit the availability of counsel.⁶¹ Class actions may help address this problem, but recent case law under the Fair Credit Reporting Act casts doubt on whether a class action litigation strategy is viable.⁶² As such, the protection offered either by actual damages or by statutory damages is insufficient. In short, it just doesn’t seem as if current law is serious about enforcing data privacy rights.

C. Liability and the Twin Tragedies of the Information Commons

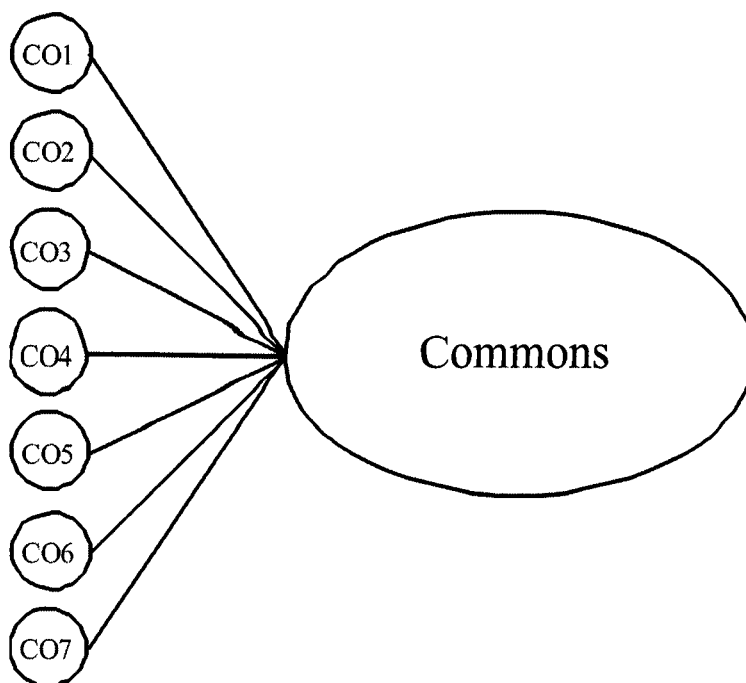
If, as the above analysis suggests, personal information is pretty much just there for the taking, or at least underprotected, then we have described personal information as a type of “common property.” The question therefore arises whether non-protection of personal information may give rise to tragic consequences. A “tragedy of the commons” (Figure 2) arises when multiple parties (Common Owners 1-6 in Figure 2 below) have a common right to use (i.e., graze sheep on) particular piece of property (the commons). Each common owner has an incentive to overuse (graze as many sheep as possible) the property, and overuse (overgrazing) in turn destroys the value of the common asset.⁶³ The answer to this question would therefore appear to be yes.

61. Edward L. Rubin, *The Code, the Consumer, and the Institutional Structure of the Common Law*, 75 WASH. U. L.Q. 11, 33 (1996).

62. See *In re Trans Union Corp. Privacy Litig.*, No. 00 C 4729, 2002 WL 31028234, at *23 (N.D. Ill. Sept. 10, 2002). In that case, the court refused to certify a class under the Fair Credit Reporting Act, under Rule 23(b)(1) (limited fund); (b)(2) (equitable relief); or (b)(3) (common questions of fact and law predominate and class action is the most efficient means of adjudication). *Id.* at **17–23. In that case, the court faced a class of 190 million members, each with a potential minimum statutory damage claim of \$100. *Id.* at *18. The court concluded that even though the aggregated statutory damage claims exceeded the net worth of the defendant, the limited fund exception did not apply because no trust or other pool of money was involved. *Id.* The court further concluded that as a matter of statutory interpretation, equitable relief was not available under the FCRA in a private right of action, *id.* at **8, 18, and finally, the court concluded that, since the size of the potential liability was so great, allowing the case to go forward as a Rule 23(b)(3) class action would not be efficient. *Id.* at **19–23. See also *Washington v. CSC Credit Serv.*, 199 F.3d 263, 267–68 (5th Cir. 2000) (denying class certification under the FCRA).

63. See, e.g., SUZANNE IUDICELLO, MICHAEL WEBER & ROBERT WIELAND, *FISH, MARKETS, AND FISHERMEN: THE ECONOMICS OF OVERFISHING* 36 (1999).

Figure 2



Indeed, two separate and distinct privacy commons appear to exist. From a dignitary perspective, routine invasions of privacy for commercial purposes are just something that we, as individuals, would prefer to avoid. However, the nature of the first privacy commons runs deeper than a simple question of whether, in the aggregate, people are less happy in a world without privacy than they might be in a world where they felt their privacy was protected. I join Paul Schwartz and others in believing that at some level, privacy is a value that is constitutive of a free society, and a necessary precondition to self-governance.⁶⁴ When viewed this way, privacy is not defined by what information we withhold from society; it is instead a regime of norms and law that shape our expectations about how information will be used once it has been shared with others. There are many such “multidimensional privacy spaces” that shape an individual’s interaction with the world. When I share information with my wife, I have one set of expectations; when I share the same information with my doctor, I have another set of expectations. When I circulate a draft paper to a close group of colleagues, I have

64. See Janger & Schwartz, *supra* note 39, at 1250–51; Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1661–64 (1999).

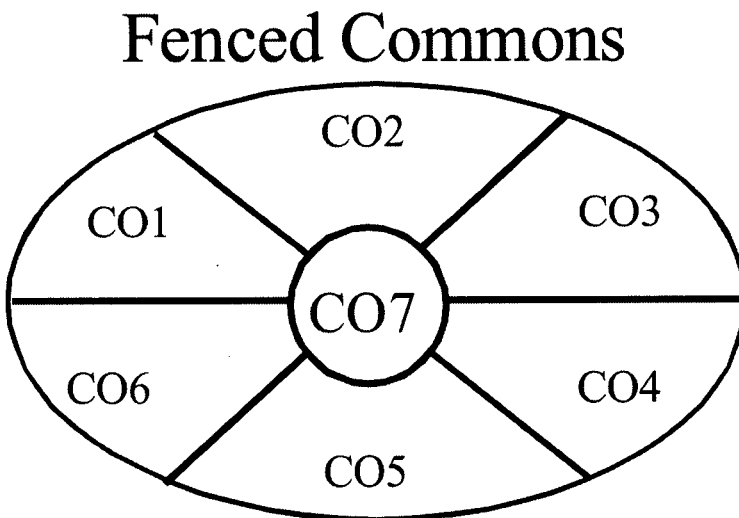
one set of expectations; when I include it in a set of symposium materials, my expectations are different. Many of these "privacy" arrangements require coordination, and many are not susceptible to creation by individual bargaining. While individuals might be willing to bargain away their privacy in return for cheaper airplane tickets, the resulting world may not be one that is socially desirable. The second, somewhat thinner, privacy commons arises from a commercial perspective. To the extent that consumers feel that their privacy is not protected on the Internet, they may refrain from engaging in transactions in cyberspace. Just as securities regulation is crucial to investor faith in the securities markets, some privacy regulation may be necessary to foster confidence in the Internet.

Liability-based protection of personal property may therefore lead to a tragedy of the commons, both for civil society and for private commerce.

III. The Promise and Problems of Propertization

Lawrence Lessig has suggested that granting consumers a property right in personal information might solve all of these problems.⁶⁵ Stated differently, when faced with the difficulties of common property, the solution is to fence the commons.

Figure 3



65. LESSIG, *supra* note 14, at 159–62.

A hypothetical based on the *Toysmart.com* facts may be helpful to illustrate this approach.⁶⁶ Imagine that I want to purchase a baby present. To order the item, I have to give certain information to the web site. At this stage of the transaction, propertization is not particularly important. If I don't want to give Toysmart my information, I don't have to.⁶⁷ But, assume that I decide that before I give them my information, I want them to guarantee that they will only use it in certain ways, and they agree. At this point, the choice between property and liability becomes crucial because it determines how much legal protection is given to that promise.

If I am protected solely by a contractual promise, then Toysmart might decide to disclose my information and pay damages. If I am protected by a Calabresian property right, then Toysmart cannot disclose my information without my permission. At first blush, property has the potential to remedy all of the shortcomings of a liability-based regime. Granting consumers the power to veto any use of their personal information that does not conform to a prior agreement might eliminate the judgment proof problem. If disclosure is effectively prevented, then damages are not necessary. Giving consumers a pre-disclosure veto would eliminate the problem of "lumping it." Even though privacy harms are dignitary, consumers would control the terms of secondary use. And finally, by turning personal information into personal private property, the commons will be fenced and the tragedy averted. Propertization is not a panacea, however. Propertization alone may fail to solve the commons problem, and it may create other problems.

A. Propertization and Market Imperfection

Where an entitlement is protected by a liability rule, the defendant may choose to violate the right and pay damages. In other words, a non-consensual taking may precede negotiation over price. Propertization changes the order of this interaction. Either through criminal sanction, affirmative judicial order, or prohibitively high (and/or punitive) fines, a property rule makes a non-consensual taking infeasible. Transfers of property happen only through consensual transactions. Propertization of personal information means that someone who holds the information of another, subject to a property-based encumbrance, cannot transfer that information

66. See *supra* Part II.A and note 52.

67. The fact that the initial disclosure is always voluntary gives rise to the mistaken impression that consumers always control the terms under which their information is used. However, as shown below, adhesion problems, cognitive problems, coordination problems, and the absence of property-based protection render the nature of this "consent" suspect.

without consent. A company cannot sell its customer list in violation of a privacy policy without permission.

However, a number of imperfections in the personal information market render propertyization an imperfect fence for the commons. First, a property right is not worth much if you can be tricked into giving it up for free. Without putting too fine a point on it, this is the problem in the "information" marketplace. There are significant information asymmetries inherent in personal information transactions that involve consumers. Consumers do not know how the information they provide will be used, nor do they know how it could be used.⁶⁸ Moreover, even if they do insist on limitations on use, they are not in a position to police the agreement. When a telemarketer calls or "spam" appears in your e-mail box, it is virtually impossible to figure out how the tele- or cyber-marketer identified you. In many cases even if consumers could police the use of information, the contract offered would take the form of a contract of adhesion.⁶⁹ And, finally, even if there is negotiating room, consumers are not likely to know what forms of disclosure are required to accomplish the desired transaction.⁷⁰

One might argue that even where there are problems with individual transactions, the market could still provide the solution. Individual market participants might find it to their advantage to compete on the basis of privacy practices. Since detection is virtually impossible, however, the development of this practice is likely to be slow.

More importantly, economists Spence, Stiglitz, and Akerlof have shown that consumers are not good at negotiating and/or shopping on the basis of non-price terms.⁷¹ In other words, consumers, given a choice between better privacy (which they don't understand) and a better price (which they do understand), will choose the lower price every time. As a result, web sites have no incentive to compete on the basis of privacy, and the result may be what economists call a "lemons equilibrium," where the market only produces bad privacy

68. Neil Weinstock Netanel, *Cyberspace Self-Governance: A Skeptical View from Liberal Democratic Theory*, 88 CAL. L. REV. 395, 476 (2000) ("[M]ost users are not even aware that the web sites 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.").

69. Janger, *supra* note 2, at 1812.

70. Janger & Schwartz, *supra* note 39 at 1255 ("Imagine the intense level of research that consumers would be forced to carry out in evaluating the information security standards of one bank versus another.").

71. George Akerlof, Michael Spence, and Joseph E. Stiglitz won the 2001 Nobel Prize in Economics for their work on the effect of asymmetric information on markets. See George A. Akerlof, *The Market for "Lemons": Quality Uncertainty and the Market Mechanism*, 84 Q.J. ECON. 488, 488 (1970); Michael Spence, *Consumer Misperceptions, Product Failure and Producer Liability*, 44 REV. ECON. STUD. 561, 561 (1977).

practices.⁷² For these reasons, a crystalline, fully alienable property right is not likely to protect the privacy of web site customers or to prevent the destruction of either of the privacy commons.

B. Muddy Property: A Solution?

In my earlier article, entitled *Muddy Property: Generating and Protecting Information Privacy Norms in Bankruptcy*, I argued that the “commons” and market imperfection problems that infect privacy transactions could be alleviated through the use of a “muddy” property rule.⁷³ The rationale behind “muddy property” is threefold. First, as property, it gives information holders a veto over involuntary disclosure, and imposes sanctions on subsequent use of that information.⁷⁴ Second, because it is muddy, it encourages dialogue among the parties about privacy-related behavior.⁷⁵ And third, where the parties cannot agree, it encourages common law adjudication of those rights, and the resulting public articulation of privacy norms by judges.⁷⁶ Since we as a society are still in the process of developing and articulating the norms that will govern personal data transactions, the norms need to be articulated by some public institution—a legislature, a court, or an agency. A muddy property rule has the potential both to regulate privacy transactions at the ground level and to increase the likelihood of private and public articulation of norms. A muddy, or limited, property rule encourages discussion and articulation of privacy norms both inside and outside the judicial system.

I am not the first to advocate the imperfect fencing of a commons. In separate works on intellectual property, privacy, and torts, Lawrence Lessig, Paul Schwartz, and Lynn LoPucki have each shown that certain types of common property are necessary to the creation and maintenance of a society that is respectively innovative,

72. As I discuss in detail below, propertization creates a number of other costs as well. Since both of these problems are accentuated when “muddy property” is involved, I reserve a detailed discussion for that section, but any form of new property may also create a mirror of the “commons problem.” Michael Heller has noted that where property rights are highly fragmented—in other words, where the commons is divided into pieces that are exceedingly small—the result may be that the same coordination problems which result in overuse in a “commons” will produce underuse. Heller, *Tragedy*, *supra* note 8, at 623–24. Heller calls this a “tragedy of the anticommons.” *Id.* Multiple rights to exclude lead to underuse, or non-use of the asset. *Id.* Finally, propertizing personal information may create what Thomas Merrill and Henry Smith have called “information costs.” Merrill & Smith, *Numerus Clausus*, *supra* note 7, at 8–9. It may be difficult to determine whether personal information is encumbered by a privacy policy or not.

73. Janger, *supra* note 2, at 1809.

74. *Id.*

75. *Id.* at 1815.

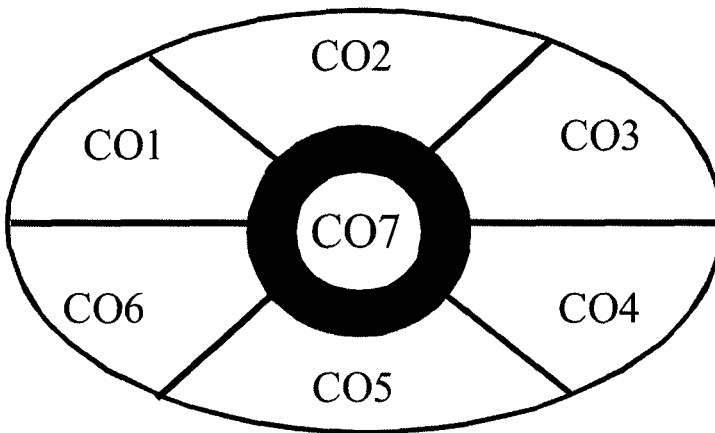
76. *Id.*

free, and safe.⁷⁷ Each has argued that enforcement of a social norm or common value requires the limitation on an otherwise crystalline property regime. Lessig describes what he calls the “innovation commons.”⁷⁸ Schwartz describes what he calls “constitutive privacy,” or a privacy commons.⁷⁹ LoPucki describes the need to encourage social investment in safety.⁸⁰ Preventing one “tragedy of the commons” can thus create another that might be termed the “tragedy of fencing.”

Once a commons is fenced, there is no longer a commons. To economists this is not troubling, because the people who formerly shared the commons will now have appropriate investment incentives. As a result, the aggregate value of the once common property will be higher when it is held in private hands. However, common property may have value precisely because it is common. Protecting a residual commons (figure 4) places limits on the extent to which we, as a society, will allow the commons to be fenced.

Figure 4

Residual Commons



Lessig, in his book, *The Future of Ideas*,⁸¹ develops a concept he terms the “innovation commons.” The innovation commons is

77. LESSIG, *supra* note 6, at 19–23; LoPucki, *Creditor's Bargain*, *supra* note 7, at 1963; Schwartz, *supra* note 64, at 1613.

78. LESSIG, *supra* note 6, at 23.

79. Schwartz, *supra* note 64, at 1613.

80. LoPucki, *Creditor's Bargain*, *supra* note 7, at 1963.

81. LESSIG, *supra* note 6, at 49.

threatened by the expansion of copyright protection.⁸² Copyright and patent law have always been intended to take some ideas and works of art out of the public domain in order to encourage writers, thinkers, inventors, and artists to produce.⁸³ Without copyright, writers, musicians, and artists could not earn a living.⁸⁴ But copyright's protections have always had limits—both in duration and in scope—and these limits, Lessig argues, are important to society as well, because without a public domain the marketplace of ideas will be replaced by private monopolies.⁸⁵ To remedy this, Lessig proposes limitations on the scope of intellectual property rights such as fair use, and limited terms.⁸⁶

In his work on information privacy, Paul Schwartz has identified a similar privacy commons, which he labels “constitutive privacy.”⁸⁷ In his view, in the new economy, the private sphere has the attributes of a public good.⁸⁸ Without some limits on the rights of third-party holders of non-public personal information, Schwartz anticipates a collapse of the private sphere that is necessary to individual self-realization and to the functioning of a democratic society.⁸⁹ He argues that fair information practices, or “FIPS,” should be used to protect the privacy commons, and suggests that a mixed regime of property and liability rules might be necessary to protect personal privacy.⁹⁰ I have gone further, and proposed a regime of “muddy property” rules based on FIPS as a means of protecting the privacy commons.⁹¹

This use of property rules to enforce norms and preserve public goods is not limited to the “intellectual property” sphere. Lynn LoPucki, who disagrees with everything I have said about privacy property,⁹² has proposed his own version of norm-enforcing property in the torts context. In his extraordinary articles, *The Unsecured Creditors' Bargain*⁹³ and *The Death of Liability*,⁹⁴ LoPucki demonstrates that secured credit can be used as a judgment proofing device to insulate tortfeasors from any form of liability for invasion of

82. *Id.* at 175.

83. *Id.* at 58–59.

84. *Id.* at 59.

85. *Id.* at 201.

86. *See id.* at 240–61.

87. Schwartz, *supra* note 64, at 1613.

88. *Id.* at 1663.

89. *Id.* at 1663–64.

90. Paul M. Schwartz, *Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy Control, and Fair Information Practices*, 2000 WIS. L. REV. 743, 781–86 (2000).

91. Janger, *supra* note 2, at 1875–78.

92. Lynn M. LoPucki, *Did Privacy Cause Identity Theft?*, 54 HASTINGS L.J. 1277 (2003).

93. LoPucki, *Creditor's Bargain*, *supra* note 7, at 1903–04.

94. LoPucki, *supra* note 59, at 23–30.

privacy, product liability, or any other civil wrong. According to LoPucki, overzealous protection of the "property rights" of secured creditors will lead to social underinvestment in safety.⁹⁵ He proposes instead that tort claimants be given a superpriority lien on the assets of the tortfeasor.⁹⁶ Such a lien or priority would not only reduce the risk faced by tort victims, but it would have the salutary effect of making secured creditors worry about the safety of their rights in the loan collateral.⁹⁷ Rendering their property rights less secure encourages them to monitor the debtor's investment in safety, and should reduce risk *ex ante*.⁹⁸

At the same time, however, muddy property may increase information costs by making it more difficult to determine who holds the right to use the personal information and whether the competing claimant must consent. It also may make it more difficult and expensive to verify who the "owner" of the information is; indeed, nothing short of litigation may suffice. Finally, muddy property further fragments the right to use personal information, and may create an anticommons. In the next section, I consider the costs associated with property rights generally, and with "muddy property" rights in particular.

IV. Muddy Property, Information Cost, Verification Institutions, and the Anticommons

Property law is usually thought of as a way to allocate social resources to individuals. The language of property is the language of exclusion: "A man's home is his castle," "No trespassing," "Beware of dog." Property rights carry with them the right to "pull up the drawbridge," "call the cops," or "sic the dog" to defend against theft or invasion. While ownership may encourage investment, and investment has social benefits, property is a zero-sum game. That which is private cannot be common. Such exclusion has costs, and therefore society must be careful to delineate what can be owned, and what cannot.

Muddy property rules are a mechanism for protecting and defining the residual commons, a mechanism for balancing the externalities of exclusion against the tragic consequences of fully common property. However, recent property scholarship has recognized that there are costs associated with non-standard and incomplete conveyances of property. These costs come in two types: (1) information costs and (2) fragmentation costs. Each of these costs

95. *Id.* at 61–63.

96. *Id.*

97. *Id.*

98. *Id.*

must be considered, and, if possible, ameliorated, as legislatures and courts determine whether to create and how to shape property rights to govern novel transactions.

A. Information

Merrill and Smith note in their recent work that property rights bind third parties.⁹⁹ Trespassers and thieves may be prosecuted. People who I don't know, who don't know me, and who have not had any contact with my transferor must respect my property rights, whatever they are. Merrill and Smith argue that this third party effect of "property" gives rise to a need for, and explains the prevalence of, the limited number of, standardized forms of property—what they (and the civil law) call the "*numerus clausus*."¹⁰⁰ The negative inference from Merrill and Smith's thesis is that new forms of property are suspect because they likely add to third party confusion.¹⁰¹ This confusion is costly because it makes it difficult to contract about property—if the right's owner cannot be identified, and if the scope of their property right cannot be stated with certainty, transactions involving that property will be problematic.¹⁰² Standardization thus reduces the cost of transactions about property.¹⁰³

Hansmann and Kraakman take a different view of the information problem.¹⁰⁴ They acknowledge that transactions about property require good information about the identity of the owner and the scope of the owner's rights,¹⁰⁵ but challenge the idea that standardization is required in order to achieve this goal.¹⁰⁶ For them, the key is verification.¹⁰⁷ So long as an institution exists that will allow potential purchasers to identify the owner of the property and will allow the owner to prove the scope of his rights, then there should be no problem with slicing up the bundle of sticks in any way the owner/transferor desires.¹⁰⁸

While Merrill and Smith and Hansmann and Kraakman may differ over the question of standardization, they both agree that there should be some place where accurate information about the identity

99. Merrill & Smith, *Property/Contract Interface*, *supra* note 9, at 77. See also Merrill & Smith, *Numerus Clausus*, *supra* note 9, at 27–28.

100. Merrill & Smith, *Numerus Clausus*, *supra* note 9, at 28–34.

101. See *supra* note 21.

102. Merrill & Smith, *Numerus Clausus*, *supra* note 9, at 26–27.

103. *Id.*

104. Hansmann & Kraakman, *supra* note 11, at 373–74.

105. *Id.* at 1805.

106. *Id.*

107. *Id.* at 1805–06.

108. *Id.*

of the owner and the scope of ownership should be available.¹⁰⁹ Norm-laden property poses a problem for both a standardization-based system and a verification-based system. To the extent that the duties that encumber property are amorphous, they may operate as a cloud on title and an obstacle to transactions.

B. Fragmentation

A second concern about new types of property is raised by Michael Heller.¹¹⁰ As he sees it, information problems are not the only issue.¹¹¹ Coordination is also a problem, even once the information privacy commons is fenced.¹¹² Although the standard justification for property lies in the coordination problem faced by common owners,¹¹³ Heller points out that fragmented ownership may create precisely the same coordination problems as common ownership.¹¹⁴ The creation of many new types of property may have the effect of creating multiple fractional owners of a particular asset.¹¹⁵ When these fractional owners face coordination problems, an "anticommons" develops.¹¹⁶ Each fractional owner can exclude all other fractional owners, and a collective action problem ensues.¹¹⁷ While the classic collective action problem arises because of free riding,¹¹⁸ here each common owner has an incentive to hold out for the highest possible price in return for consent.¹¹⁹ Where each common owner has an incentive to hold out, the asset will go unused.

All three norm-laden forms of property raise fragmentation problems that would trouble Heller. Lessig's limited intellectual property rights subject the copyright or patent owner to multiple competing claims of fair use. Muddy information privacy rights are particularly problematic whenever personal information is aggregated, and its value inheres in the numerous names and characteristics embodied in the database. If a mailing list has value, granting an enforceable veto right to each name on the list would destroy any saleable value that the list might have. Finally, LoPucki's

109. *Id.* at 1814; Merrill & Smith, *Numerus Clausus*, *supra* note 9, at 26–27.

110. Heller, *Boundaries*, *supra* note 10, at 1165–67; Heller, *Tragedy*, *supra* note 10, at 622–25.

111. Heller, *Tragedy*, *supra* note 10, at 623.

112. *Id.* at 623–24.

113. *Id.*

114. *Id.*

115. *Id.*

116. *Id.*

117. *Id.*

118. MANCUR OLSON, *THE LOGIC OF COLLECTIVE ACTION: PUBLIC GOODS AND THE THEORY OF GROUPS* 2 (1965).

119. Heller, *Tragedy*, *supra* note 10, at 623–24.

“torts first” priority subjects the owners of property to multiple, difficult to identify, possibly unmatured claims that might prime the rights of any purchaser of the property.

The combined message of Merrill and Smith, Heller, and to a lesser extent Hansmann and Kraakman is: “Don’t create new types of property, and if you do, keep them simple and undivided, or at least verifiable.”

But there is a counter-story. Just because norm-laden property rights impose information and fragmentation costs doesn’t mean that they should be discarded as a means of norm enforcement. First, some social goals are so important that the costs may be justified. And second, with some careful thought and attention it may be possible to develop legal mechanisms that reduce the information and fragmentation costs associated with norm enforcement.

V. Cutting Costs Through Muddy Standardization and a Collective Procedure for Quieting Title

To what extent is it possible to reduce the information and fragmentation costs associated with using a norm-enforcing property rule to protect data privacy? Some of these costs are unavoidable. The very idea of norm enforcement entails competing claims. By definition, muddy property limits the extent to which rights holders can be identified with certainty. However, some information cost savings can be achieved through standardization by making the property right mandatory, while verification and fragmentation costs can be reduced by providing a collective procedure for quieting title in personal information.

A. Mandatory Muddy Standardization

Information costs cannot be completely eliminated when one is trying to use property rules to enforce norms. Standardization alone will not solve the norm-enforcement problem. The Protocol for Privacy Protection, or “P3P,” provides a good example of why this is the case. P3P is a computerized protocol under which a web surfer can set his computer to travel only to sites that provide a chosen menu of privacy protections. P3P has made some level of privacy standardization possible.¹²⁰ Privacy policies can, in some contexts, be reduced to a limited menu of terms, and those terms can be specified as a field along with the data. These standardized terms can be the subject, in turn, of standardized negotiation. However, while P3P

120. For a discussion of P3P, see Joseph M. Reagle, Jr. & Rigo Wenning, *P3P and Privacy on the Web FAQ*, Platform for Privacy Preference Project, at <http://www.w3.org/P3P/P3FAQ.html> (Apr. 18, 2000).

may solve the standardization problem, it does not solve the adhesion problem inherent in many online negotiations. Also, for the reasons discussed above, it may not be possible or desirable to specify the exact scope of the privacy obligation. The line between primary use and secondary use may be easy to draw in some contexts, but it may be difficult to draw in others. It is not fair, or wise, to require ordinary web site customers to draw a line where they do not have sufficient resources to do so.

The Gramm-Leach-Bliley Act presents another excellent example of a failed attempt to grant a standardized privacy package.¹²¹ GLB grants notice and opt-out rights to customers of a financial institution, but the opt-out rights apply only when the institution seeks to share information with a non-affiliated party. Where a bank is affiliated with an insurance company and an investment bank, GLB provides a safe harbor for “affiliate” transfers that will permit significant secondary use. Where a customer does business with a stand-alone local bank, by contrast, GLB may provide more protection.

The problem with both P3P and GLB is that they each rely on the mistaken belief that consumers *can* contract about privacy. P3P operates on the assumption that if privacy policies are simplified and standardized, consumers will be able to engage in efficient contracting about privacy. But, for the reasons stated above, I have my doubts. In my view, a standard yet muddy rule might work better. For example, a mandatory rule that simply prohibits “unreasonable secondary use” would solve part of Merrill and Smith’s problem, since any holder of information would know that they held it subject to a duty to protect reasonable expectations of privacy. Everybody would know what the legal duty was, and would be required to give it meaning in the context of a particular transaction.¹²² However, because the duty is muddy, nobody would know its exact scope. Thus, standardization of information privacy rights in muddy and mandatory form eliminates some, but not all, of the costs feared by Merrill and Smith.

121. For a more detailed discussion of GLB’s privacy provisions, see Janger & Schwartz, *supra* note 39, at 1222–30.

122. Indeed, P3P-like or other privacy enhancing technologies might operate as technological overlays, which allow a choice among different standardized muddy property rules that might apply in different contexts. For example, one standardized rule might work for medical information, while another standardized rule might apply to credit card numbers, while yet another standardized rule might apply to clickstream data about web site preferences. Note, however, that the technology is not being used here to conduct a contractual negotiation, as with P3P, but instead to determine which protocol must be applied to a particular class of data.

B. Verification

On the one hand, verification institutions don't appear to add much to the conversation. Indeed, it is not all that difficult to identify the holder of a privacy entitlement. When a company holds personal information about its customer, the duty, if any, runs to the person to whom the information relates. The difficulty lies not in determining who holds the right, but in precisely what the duty entails in particular circumstances. The only verification institution that can resolve that question is a court. Indeed, the reason for advocating a muddy rule on secondary use lies in the fact that it will require *ex post* determination of the scope of the duty, and will thus influence behavior and encourage negotiation over questionable disclosures.

However, where large databases are involved, verification problems arise in a slightly different form. While it may be possible to identify who holds an interest in a database, it may be virtually impossible to identify a person with authority (short of a judge) to speak for the group. Thus, for verification reasons and additional reasons that I discuss below, a property-based scheme for protecting information privacy might provide for the appointment of a class representative to bargain on behalf of individuals whose information is contained in large aggregated databases.

C. Fragmentation

To the extent that muddy property rules impose information costs in two-party information transactions, they may be bearable, because those very costs are what produce the systemic investment in norm-related negotiation. Prior to disclosure, the parties will have to negotiate over the appropriate scope of the secondary use. However, what looks like a benefit in the context of a two-party negotiation begins to look like a nightmare when the value of a database lies in the fact that it aggregates the data of hundreds, thousands, or millions of people. The value of each piece of information is quite small. The cost of disclosure may also be quite small, but the cost of bargaining with each person whose information is in the database is likely to be prohibitive. The result may be to deter certain appropriate primary uses, and to chill secondary uses that would be efficient and desirable simply because negotiation is not possible. Worse yet, because bargaining is not feasible, it will not occur, and the norm-articulation function of muddy rules may not be served either.

D. A Collective Solution for Verification and Fragmentation Problems

While information costs may be the price we pay for norm generation, when we choose to use a muddy property rule, fragmentation costs can be limited through the use of a collective

mechanism for quieting title in information, and verification costs could also be limited by appointing a guardian or representative for customers with an interest in a database. While there might be a number of models for such a procedure, one promising model lies in the Bankruptcy Code. Bankruptcy courts have significant experience in dealing with coordination problems. Indeed, the standard justification for business reorganizations under Chapter 11 of the Bankruptcy Code rests on a “tragedy of the commons.”¹²³ When a debtor with a viable business becomes insolvent, creditors face a coordination problem. Unless they act quickly to grab the assets of the debtor, others may get there first. This classic collective action problem often results in a “race to the courthouse,” that leads, in turn, to the inefficient liquidation of the debtor and loss of the firm’s “going concern” value.

Many of Chapter 11’s procedural mechanisms are aimed at remedying this problem and encouraging a collective solution to the debtor’s financial distress, which preserves the value of the firm. For example, the automatic stay prohibits unilateral creditor action, thus binding creditors to the collective solution.¹²⁴ Similarly, the collective action problem faced by individual small creditors, who have no incentive to participate actively in the case, is solved through the appointment of a creditors’ committee to negotiate on behalf of the unsecured creditors.¹²⁵

But Chapter 11 is not just about keeping firms together. Bankruptcy cases have always been fora for selling assets and modifying contracts. Many companies choose to liquidate in Chapter 11, and even companies that reorganize “successfully” will often shed assets during the course of their bankruptcy cases. Sometimes assets are shed in an effort to refocus the business, sometimes they are sold simply to raise cash to continue operations and sometimes bankruptcy is used to wring value out of assets that could not be sold without the blessing of a court.¹²⁶ Indeed, Chapter 11 of the Bankruptcy Code is increasingly being used not to solve the traditional “commons” problem (to preserve going concern value), but instead to resolve anticommons problems created by new forms of property—to clear title to assets that might not otherwise be

123. Douglas G. Baird, *A World Without Bankruptcy*, LAW & CONTEMP. PROBS., Spring 1987, at 173, 183.

124. 11 U.S.C. § 362 (2000).

125. *Id.* § 1102.

126. Douglas G. Baird & Robert K. Rasmussen, *The End of Bankruptcy*, 55 STAN. L. REV. 751, 751 (2002) (“Corporate reorganizations have all but disappeared. Giant corporations make headlines when they file for Chapter 11, but they are no longer using it to rescue a firm from imminent failure. Many use Chapter 11 merely to sell their assets and divide up the proceeds.”).

saleable. In this regard, property owners are taking advantage of bankruptcy's collective procedures and the availability of bankruptcy judges to resolve disputes. This aspect of the Chapter 11 process may suggest a model for information privacy law.

(1) 11 U.S.C. § 363(f)—A Model

Under section 363 of the Bankruptcy Code, the bankruptcy trustee has the power to use and sell assets of the debtor both inside and outside of the ordinary course of business. Where the sale is outside the ordinary course of business, the debtor must obtain court approval under section 363(c) and, if the asset is encumbered, under section 363(e), the holder of the property interest is entitled to "adequate protection."¹²⁷ This may include a continuation of the lien on the property in the hands of the purchaser,¹²⁸ but under section 363(f) the bankruptcy court also has the power to allow the debtor to sell property free and clear of liens, encumbrances, and other interests under certain circumstances.¹²⁹

As it is presently constituted and used, section 363(f) would not allow the debtor to sell personal information out from under a muddied property rule. Current case law limits the scope of the section to liens and liability-based covenants (i.e., covenants that do not run with the property).¹³⁰ However, there is some wiggle room. Section 363(f)(1)

127. *Id.* § 361.

128. U.C.C. § 9-315(a) (1999).

129. 11 U.S.C. § 363(f) (2000) provides:

The trustee may sell property under subsection (b) or (c) of this section free and clear of any interest in such property of an entity other than the estate, only if— (1) applicable nonbankruptcy law permits sale of such property free and clear of such interest; (2) such entity consents; (3) such interest is a lien and the price at which such property is to be sold is greater than the aggregate value of all liens on such property; (4) such interest is in bona fide dispute; or (5) such entity could be compelled, in a legal or equitable proceeding, to accept a money satisfaction of such interest.

A web site visitor's interest in personal information, to the extent it exists, is not a lien, not in dispute, and likely to be enforceable by specific performance. As such, only sections 363(f)(1) or (2) are likely to provide a means for selling personal information. Obtaining consents will work, of course, but is unlikely to be feasible. Whether or not current law allows the sale "free and clear" begs the question since current law does not create a property right in information privacy. The question that would need to be answered when designing a procedure would be: under what circumstances should a sale free and clear be allowed?

130. *Gouveia v. Tazbir*, 37 F.3d 295, 299 (7th Cir. 1994); *In re* 523 E. Fifth St. Hous. Pres. Dev. Fund Corp., 79 B.R. 568, 570–71, 576 (Bankr. S.D.N.Y. 1987); cf. Miller & O'Rourke, *supra* note 25, at 812–18 (noting that under the law's current contract based approach to privacy, it would be possible to sell information out from under a privacy policy, but that if it were given the status of property, section 363(f) would not permit such sale). See also David Gray Carlson, *Successor Liability in Bankruptcy: Some Unifying Themes of Intertemporal Creditor Priorities Created by Running Covenants, Products*

permits a sale free and clear of an interest if applicable non-bankruptcy law would allow sale free of the interest.¹³¹ Since this is a discussion of what an information privacy property right might look like, the question becomes: “Under what circumstances should applicable non-bankruptcy allow a sale free and clear of an information privacy right?” The reason that section 363 holds interest here is that it is often used as a mechanism for resolving anticommons problems.

(2) *Sale “Free and Clear” and the Anticommons—An Example*

To see the promise held out by section 363, an example might be helpful. One familiar use of bankruptcy to facilitate a sale arises where a valuable asset of the debtor is held subject to a number of liens, all of which may be superior to that of the bankruptcy trustee. Such a problem can arise in a number of ways, but here is a relatively simple scenario. The debtor is a limited partnership which owns a building which is under construction. The general contractor finds itself in financial difficulty, fails to pay subcontractors, and then files for bankruptcy. The subcontractors then file mechanics liens against the building. The developer is faced with the unattractive alternatives of paying the subs twice or abandoning the project. A buyer, however, is willing to purchase the property and complete the project, but only if it can get clear title. There is no question that the mechanics liens will have priority over the subsequent purchase, and will have to be paid. The problem is that there are dozens of different liens filed against the property, many appearing to be inflated, and the state law procedures for addressing the validity and priority of mechanics liens are cumbersome and time consuming. The buyer is not interested in waiting, and the longer the property sits, the less it will be worth.

Each of these dozens of lien claimants can effectively stop the sale, leaving everyone worse off. Under section 363(f), however, the court can approve the sale of the property “free and clear” of the mechanics liens, while allowing the liens to attach to the sale proceeds. The value of the various liens and their respective priorities can then be resolved in the ordinary course, without delaying the sale itself.

Liability, and Toxic-Waste Cleanup, LAW & CONTEMP. PROBS., Spring 1987, at 119, 141–42; Basil H. Mattingly, *Sale of Property of the Estate Free and Clear of Restrictions and Covenants in Bankruptcy*, 4 AM. BANKR. INST. L. REV. 431, 441–43 (1996) (arguing that *Gouveia* was wrongly decided, and that section 363(f) should be available to strip covenants from real property). *But see In re Trans World Airlines*, 322 F.3d 283 (3d Cir. 2003) (discharging successor liability claims against TWA).

131. 11 U.S.C. § 363(f)(1).

(3) *A Collective Procedure for Quieting Title in Personal Information*

In the absence of section 363(f), the competing lien claims against the property would destroy its value for the estate. The fragmented interest in the property would be unusable. This is a classic anticommons, and section 363(f) provides a model escape route. The question, therefore, is whether it might be possible to craft a collective solution along these lines to deal with sales of personal information. There would appear to be two principal obstacles to developing such a device. The first is giving meaning to the concept of "adequate protection" in the information privacy context, and the second is the need for a class representative. Since the value of personal information to individuals may be relatively small in the particular case, there may not be anybody with a sufficient stake to participate in the proceeding.

Both of these problems are remediable. First, to the extent that the collective proceeding is offered as an adjunct to one of the topic specific pieces of privacy legislation, the content of fair information use can be spelled out for that particular context. For example, fair information use might mean something very different in the context of credit reporting than it does in the context of video rentals. If the collective procedure was contained in the VPPA or the FCRA, these differences could be accommodated. Second, a guardian or committee could be appointed to represent the holders of information property rights.

This approach is not completely novel; state law has long provided mechanisms for quieting title to property.¹³² The current version of the Bankruptcy Reform Bill pending in Congress contains a provision—the "Leahy Amendment"—that contains a first cut at a procedure that follows this model.¹³³ I have discussed elsewhere its shortcomings.¹³⁴ Among its strengths, however, is the fact that it proposes the appointment of a "privacy ombudsmen" who would negotiate on behalf of the customers of the debtor to protect their interest in their own personal information. Similarly, another positive attribute of the Leahy Amendment is that it places a public official (in this case the bankruptcy judge) in a position to determine what

132. See, e.g., N.Y. REAL PROP. ACTS. LAW §§ 1941–43 (McKinney Supp. 2003). See also 65 AM. JUR. 2D, *Quieting Title and Determination of Adverse Claims* §§ 1, 10–11 (2001). Quiet title actions can be used to clear encumbrances that are "invalid or inoperative." *Id.* at § 13. In the context of information privacy, the analogy would be to show that a secondary use was consistent with the customer's reasonable expectations of privacy.

133. The Leahy Amendment can be found in sections 231 and 232 of the conference report to the Bankruptcy Abuse Prevention and Consumer Protection Act of 2002. See H.R. CONF. REP. NO. 107-617, at 51–52 (2002).

134. Janger, *supra* note 2, at 1873–75.

actions are necessary to protect customer interests in personal information when a data sale is proposed.¹³⁵

There are two fundamental problems with the Leahy Amendment that are relevant to this discussion.¹³⁶ The first is its failure to give any guidance on the meaning of “adequate protection” in the information privacy context, and the second is the fact that it exists only in the Bankruptcy Code. The only people given the protection of the Leahy Amendment are those who give their information to companies that actually go bankrupt. Again, both of these problems could be solved by moving the proposed device out of the Bankruptcy Code and into the remedial schemes of the various privacy statutes. If, for example, the FCRA or the VPPA contained such a collective procedure, the protection would be available inside and outside of bankruptcy, and adequate protection could be defined by reference to the particular goals of the statute.

In sum, if a standardized “muddy property” right is chosen as a means for protecting information privacy, a necessary adjunct to that right might well be a collective procedure for quieting title to personal information.

Conclusion

There may be some value to substituting a property-based private right of action for the current liability-based regime. Further benefits might result from leaving that property-based entitlement somewhat fuzzy. These benefits would be in the form of (1) enhanced protection of both data privacy and of the residual privacy commons, (2) allowing public mechanisms to remedy imperfections in the privacy marketplace, and (3) encouraging the public and private discussion and articulation of privacy norms. While these benefits come with unavoidable information and fragmentation costs, these costs can be minimized by standardizing the muddy rules in particular contexts, and by creating a collective procedure for quieting title in personal information.

135. The Leahy Amendment is not unique in its use of an appointed guardian and judicially supervised bargaining to resolve an anticommons problem. Section 1114 of the Bankruptcy Code sets forth a procedure for modifying retiree medical benefits in bankruptcy. Under that section a debtor may modify retiree medical benefits only to the minimum extent necessary to confirm a plan of reorganization. Retirees, like web site customers, are a diffuse group. In order to resolve this problem, section 1114 provides for the appointment of a committee to represent the retirees in any negotiations with the debtor. If the committee and the debtor are unable to agree on an appropriate modification of benefits, the bankruptcy court can impose modifications that it thinks are fair and equitable.

136. A third weakness is its excessive deference to published privacy policies. See Janger, *supra* note 2, at 1874–75.

7
