Charting a Privacy Research Agenda: Responses, Agreements, and Reflections

PAUL M. SCHWARTZ*

Proof appears on an almost daily basis of the centrality of personal information to social, economic, and political life. The new importance of personal data has not passed unnoticed. From President Clinton's latest State of the Union address, to the Federal Trade Commission's recent action against Trans Union for sale of personal credit data, to the Internet privacy scandal of the week, everyone is talking about information privacy.[1]

In *Internet Privacy and the State*, I argue that the leading theory of information privacy, which views it as a personal right to control the use of one's data, is deeply flawed. In place of this established paradigm of privacy-control, I develop the concept of "constitutive privacy."[2] By thinking of privacy in a constitutive sense, we are able to view it as playing an important role in forming the society in which we live, and in shaping our individual identities. From this perspective, information privacy requires

---

* *Professor of Law, Brooklyn Law School.* *This essay is a response to Comments on my Article,* Internet Privacy and the State, *32 CONN. L. REV. 815 (2000). I am grateful for the thoughtful comments of the five scholars who commented on it: Anita L. Allen, Fred H. Cate, Amitai Etzioni, Michael J. Gerhardt, and Lance Liebman. I also wish to thank for their insights and assistance Ted Janger, Martin Flaherty, Paul J. Marino, Laura J. Schwartz, Stefanie Schwartz, Peter Spiro, William M. Treanor, and Ben H. Warnke.*

1. In his State of the Union address, President Clinton stated, regarding new breakthroughs in technology, "[f]irst and foremost, we have to safeguard our citizens' privacy." The White House, Office of the Press Secretary, President William J. Clinton, *State of the Union Address* (Jan. 27, 2000) <http://www.pub.whitehouse.gov/uri-res/I2R?urn:pdi://oma.eop.gov.us/2000/1/27/15.text.1>. More recently, the President proposed a federal governmental role in protecting the privacy of financial and medical information on the Internet. *See* Marc Lacey, *Clinton Calls for Stronger Measures to Protect the Privacy of Computer Users*, N.Y. TIMES, Mar. 4, 2000, at A9.

Regarding the action of the Federal Trade Commission (FTC) against Trans Union for violations of the Fair Credit Reporting Act, see FTC, *In the Matter of Trans Union Corporation* (Feb. 10, 2000) <http://www.ftc.gov/os/2000/03/transunionfinord.htm>.

2. *See* Paul M. Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815, 834-35 (2000) [hereinafter Schwartz, *Privacy and the State*]. For another discussion of this concept, see Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1658-66 (1999) [hereinafter Schwartz, *Privacy in Cyberspace*].

contextual line-drawing rather than a maximizing of individual control.[3] In that Article, I also explore possible mechanisms for establishing the necessary kinds of privacy rules and argue that the State, generally viewed with suspicion in the dominant rhetoric concerning Internet policy formation, has two important roles: (1) creating and maintaining conditions for a functioning privacy market, and (2) helping to stimulate privacy norms that prevent access to personal information that would cause too great a rate of "preference falsification" in society.[4]

In the preceding pages of the *Connecticut Law Review*, five distinguished scholars have commented on my views. Their thoughtful papers qualify as the most gracious outpouring since the preacher's kind—and perhaps not entirely justified—comments about Tom Sawyer, Huck Finn, and their comrade Joe, presumed lost but hidden in the church.[5] Like Tom, Huck, and Joe, I appreciate the comments. The commentators' generosity is more than matched, however, by their careful and rewarding analysis. In this essay, *Charting a Privacy Research Agenda: Responses, Agreements, and Reflections*, I examine each paper in turn and find that these authors' contrasting perspectives on information privacy set out crucial aspects of an agenda for future research.

I. PRIVACY AND COMMODIFICATION OF IDENTITY

In *Privacy-as-Data Control*, Anita L. Allen focuses primarily on one aspect of my Article: my rejection of the popular view that the purpose of privacy is to protect and presumably to maximize an individual's control over her personal information.[6] Professor Allen extends my argument on this point in a number of valuable ways; one of her most significant insights is that control over personal information does not, at the end of the day, equate with the condition of having privacy. As Professor Allen notes, "[c]ontrol is not sufficient for privacy, nor is it necessary."[7] Her initial example on this point is the prison inmate locked in solitary confinement who has an excess of privacy, but no control over personal information because his cell may be subject to scrutiny by physical search or surveillance camera.[8]

---

3. *See* Schwartz, *Privacy and the State*, *supra* note 2, at 834-35.

4. *See id.* at 855-58.

5. *See* MARK TWAIN, THE ADVENTURES OF TOM SAWYER (Bantam Books ed. 1981) (orig. ed. 1876) ("As the service proceeded, the clergyman drew such pictures of the graces, the winning ways, and the rare promise of the lost lads, that every soul there, thinking he recognized these pictures, felt a pang in remembering that he had persistently blinded himself to them always before, and had as persistently seen only faults and flaws in the poor boys."). *Id*. at 114.

6. *See* Anita L. Allen, *Privacy-as-Data Control: Conceptual, Practical, and Moral Limits of the Paradigm*, 32 CONN. L. REV. 861 (2000) [hereinafter Allen, *Privacy-as-Data Control*].

7. *Id*. at 868.

8. *See id.*

Professor Allen continues her examination of the control paradigm of privacy by pointing to a different extreme. She is worried about people who have control, but exercise it only to surrender as much of their privacy as possible.[9] In other words, where her hypothetical prisoner has privacy but no control, others may have control but no privacy. Here, her key example is behavior in cyberspace that demonstrates how eager some of us are to abandon our privacy. In particular, Professor Allen points to Web sites that broadcast images from a person's life. One of this genre of Web sites is the "Jennicam;" this site is run by "Jenni," who posts images from her living room, bathroom, and from journeys that she takes beyond the walls of her apartment.[10] As Professor Allen concisely states, "[t]he person in control of her data might elect to share personal information with others."[11]

Professor Allen is worried about "the moral and policy implications" of wholesale social abandonment of established privacy standards.[12] She believes that law and social norms now permit a culture of "exhibitionism and voyeurism," and that policymakers should consider adoption of "policies that require certain privacies," whether people want them or not.[13] Put more formally, she states that policymakers "may be required to undertake the formative project of creating citizens who want certain personally and socially beneficial forms of privacy."[14] Professor Allen's conclusion, which is novel and important, is that any alternative to "data control" must include recognition of the cumulative consequences of the bad privacy choices that people make.

Of the difficult issues that Professor Allen raises, I wish to address only one, which concerns the commodification of identity through the sale of personality and privacy. For many first generation analysts of the Internet, this medium seemed to offer the promise of achieving self-regulation by its participants in a space free of top-down rule.[15] A few years later, however, we have the not so "cheap speech" of an increasingly commercialized Internet, which has yet to give us the next Publius, the great author of many Federalist papers, but which has lowered certain categories of

9. *See id.* at 868-69. For a further discussion, see Anita L. Allen, *Coercing Privacy*, 40 WM. & MARY L. REV. 723, 728-41 (1999) [hereinafter Allen, *Coercing Privacy*].

10. *See* Allen, *Privacy-as-Data Control*, *supra* note 6, at 867-68. For more on the Jennicam, see *Jennicam* (visited Mar. 23, 2000) <http://www.jennicam.com>. The Jennicam site provides links to tribute Web sites devoted to "Jenni," and offers Members who pay $15 a year a more rapid rate of refreshment on its images. Professor Allen also discusses the Jennicam. *See* Allen, *Coercing Privacy*, *supra* note 9, at 731.

11. Allen, *Privacy-as-Data Control*, *supra* note 6, at 867.

12. *Id.* at 869.

13. *Id.* at 872.

14. *Id*.

15. *See, e.g.*, I. Trotter Hardy, *The Proper Legal Regime for "Cyberspace,"* 55 U. PITT. L. REV. 993 (1994); David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1393 (1996).

transaction costs for Elvis and Madonna wanna-bes.[16] Today, everyone can try their hand at becoming a star—or at least at engaging in the self-revelation that our culture associates with celebrity status.[17]

The difficulty is that, while the law responds well to protecting the interests of those who wish to commodify their personality and sell their privacy, it fails to protect other interests in privacy—those that fit less neatly into a marketplace paradigm. Thus, in terms of legal doctrine, we have seen a rise in the significance of publicity rights and the tort right against appropriation of one's name and likeness.[18] These privacy interests mesh handily, moreover, with traditional intellectual property rights. The doctrinal losers are the other three branches of the tort right of privacy, and many statutory attempts to shape fair information practices for personal data use.

From the perspective of scholars of cultural studies, moreover, stardom can have a positive role in providing a range of semiotic meaning for social discussion. Thus, in Michael Madow's terms, when we buy one Madonna t-shirt and not another, we are voting about and shaping the cultural meaning of this star.[19] Professor Allen worries, however, about a society where too many of us wish to be at the center of this process. Jerry Seinfeld has summed up this troublesome, new world view. As quoted in *Forbes*, the multimillionaire comedian states, "[e]very human being is a brand. The way you socialize, who you know, what you say."[20] And, as of March 2000, Jenni has discovered traditional intellectual property law, placed a copyright on her entire Web site, and obtained a trademark on "Jennicam."[21] In face of this rampant commodification, information privacy law has much work to do if it is to maintain a non-market language for speaking about the terms of accessibility and non-accessibility to per-

16. For the pathbreaking article regarding "cheap speech" on the Internet, see Eugene Volokh, *Cheap Speech and What It Will Do*, 104 YALE L.J. 1805 (1996).

17. For an insightful analysis of the "cult of celebrity" in the United States, see Michael Madow, *Private Ownership of Public Image: Popular Culture and Publicity Rights*, 81 CAL. L. REV. 125, 227-28 (1993). The *Forbes* survey of the world's highest paid entertainers and athletes provides an annual financial assessment of the "Celebrity 100," and insights into such concerns as the overhead of different celebrity foundations. *See* William P. Barrett, *Sweet Charity*, FORBES, Mar. 20, 2000, at 180, *available in* LEXIS, News Library, Forbes File.

18. For an introduction to publicity rights, see DONALD S. CHISUM & MICHAEL A. JACOBS, UNDERSTANDING INTELLECTUAL PROPERTY LAW § 6G, at 6-66 to 6-78 (1992). For a discussion of the different tort interests in privacy, see DAN B. DOBBS, THE LAW OF TORTS 1197-1211 (2000); Joel R. Reidenberg, *Setting Standards for Fair Information Practices in the U.S. Private Sector*, 80 IOWA L. REV. 497, 504-06 (1995).

19. *See* Madow, *supra* note 17, at 143.

20. R.L.F., *Please, I'm Surfing*, FORBES, Mar. 22, 1999, at 182, *available in* LEXIS, News Library, Forbes File.

21. *See Jennicam* (visited Mar. 23, 2000) <http://www.jennicam.org>.

sonal data.[22]

II. THE COSTS OF COMMUNICATION, OR OPTING IN AND OPTING OUT

In a striking passage in *Principles of Internet Privacy*, Fred H. Cate points out that free flows of information create a "democratization of opportunity in the United States."[23] With this felicitous phrase, Professor Cate reminds us that part of the equality at the basis of American life concerns economic opportunity, and that a certain kind of flow of personal information will contribute to this goal. With reference to the text of the United States Constitution, caselaw interpreting this document, federal statutes, and a letter by Alan Greenspan, Professor Cate goes on to argue that "[o]pen information flows are not only essential to self-governance; they have also generated significant, practical benefits."[24] This argument also reflects views developed at length in Professor Cate's influential book, *Privacy in the Information Age*, to which I will return below.[25]

Professor Cate could not be more correct concerning the benefits of access to personal information, and the individual and social purposes that this flow serves. He also makes the sound observation that taking information privacy seriously requires enactment of "well-drafted, carefully targeted legislation" and that the wrong kinds of privacy laws, or, for that matter, privacy norms, can do considerable damage to important goals.[26] Yet, Professor Cate also wishes to establish an anti-privacy tilt in the ongoing policy judgments that we make regarding the pros and cons of different information privacy regimes.

Despite speaking at times of the importance of balance, Professor Cate reveals his strong preference for disclosure by emphasizing the overarching importance of open information flows, detailing many negative aspects of privacy,[27] and calling for a "specific harm" threshold before action is taken to protect privacy.[28] In my judgment, this policy preference reflects a baseline error.

It is true that privacy can be problematic, but so can open access to personal data. I tried to resolve this conflict, whether successfully or not, in *Internet Privacy and the State*. In that Article, I propose that democratic

22. *See* MARGARET JANE RADIN, CONTESTED COMMODITIES 223 (1996) (noting how "conceiving of politics in market rhetoric" may be "actively bringing about in us those very motivations and characteristics it presupposes and reifies").

23. Fred H. Cate, *Principles of Internet Privacy*, 32 CONN. L. REV. 877, 884 (2000).

24. *Id.* at 882.

25. *See* FRED H. CATE, PRIVACY IN THE INFORMATION AGE 68-71 (1997).

26. Cate, *supra* note 23, at 895.

27. Professor Cate states, "[p]rivacy . . . may reduce productivity, lead to higher prices for products and services, and make some services untenable altogether." *Id*. at 887.

28. *See id.* at 889.

community requires access to personal data.[29] It relies on an ongoing critical examination of persons and events, and this assessment in many circumstances depends on access to personal data. I also argue, however, that democratic community is not invariably furthered by heightening social access to personal data. An increase in such flow of data can heighten oppression of group members, improve the longevity of inefficient group norms, and create externalities for others.[30] In addition, just because one gives groups more personal information reveals nothing about whether or not the State's regulation will be displaced, or whether meddlesome behavior by community and government will be increased.[31]

My response to these difficulties is in viewing privacy for personal information as carrying out a constitutive function. This function frequently involves not a disjunctive—a bald choice between privacy or disclosure—but a striving for a more complex balance. Through such means as law, social norms, and the development of technological standards, society should engage in the creation of multidimensional information preserves that combine disclosure and non-disclosure rules for the same piece of information.[32]

If Professor Cate commits a baseline error through his heavy tilt for disclosure, he goes on to enshrine this preference by arguing for "opt-out" rather than "opt-in" rules.[33] To understand this distinction, we should start with opt-in, which refers to a system in which one's prior, express approval must be obtained before personal information is used for purposes beyond those associated with the initial collection purpose.[34] As Professor Cate writes, "'[o]pt-in' requires that every consumer be contacted to gain explicit permission."[35] In contrast, opt-out, which he favors, allows approval to be inferred from the customer-data processor relationship unless an individual specifically requests limits on further use.[36] By establishing one of these default rules, a statute or regulation sets a starting point for bargaining between data processors and consumers.[37]

---

29. *See* Schwartz, *Privacy and the State*, *supra* note 2, at 834-36.

30. *See id.* at 839-40.

31. *See id.*

32. *See id.* at 840. By characterizing these activities as constitutive, I wish to indicate that the resulting pattern of disclosure and non-disclosure standards plays a central role in forming the society in which we live and the nature of our individual identities. *See id.* at 835.

33. *See* Cate, *supra* note 23, at 893.

34. *See id.* For other discussions, see Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1246-58 (1998); Paul M. Schwatz, *Privacy and the Economics of Personal Health Care Information*, 76 TEX. L. REV. 1, 54-55 (1997) [hereinafter Schwartz, *Privacy and the Economics of Health Care*].

35. Cate, *supra* note 23, at 893.

36. *See id.*

37. *See* Kang, *supra* note 34, at 1246-49; Schwartz, *Privacy and the Economics of Health Care*, *supra* note 34, at 54-55; Jeff Sovern, *Opting In, Opting Out, or No Options at All: The Fight for Control of Personal Information*, 74 WASH. L. REV. 1033, 1101-16 (1999). For the classic expositions of

Professor Cate likes opt-out because requiring the consumer to take positive action reduces "the cost of communicating."[38] On this important issue, Professor Cate's views have been highly influential and will continue to be at the center of national debate. His *Privacy in the Information Age* already served as a strong influence on the Tenth Circuit's decision in *U.S. West, Inc. v. FCC*.[39] In this leading case, the Tenth Circuit invalidated on constitutional grounds a set of FCC regulations that required telecommunications carriers to obtain affirmative approval from a customer before using that customer's "customer proprietary network information" (CPNI) for marketing purposes.[40] CPNI is information about the quantity, quality, and kind of telecommunication services received by a carrier's customer that "is made available to the carrier by the customer solely by virtue of the carrier-customer relationship."[41] As the FCC explained CPNI, it is "information about whom you call, when you call, how long you talk and how you communicate."[42] In issuing the regulations under challenge in *U.S. West*, the FCC acted under a federal statute that restricted use, disclosure of, and access to CPNI, and required a carrier to obtain informed consumer consent before going beyond specified, legally permissible kinds of use.[43]

Citing Professor Cate at different points in its opinion, the Tenth Circuit adopted his view regarding the high costs that privacy can impose on society.[44] From this initial point, the *U.S. West* court went on to find that the FCC's selection of opt-in was unsupported by adequate evidence to deem it narrowly tailored under applicable First Amendment doctrine.[45] If

---

the concept of the default rule, 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, 735-40 (1992).

38. Cate, *supra* note 23, at 893.

39. 182 F.3d. 1224 (10th Cir. 1999).

40. *Id.* at 1228, 1239.

41. 47 U.S.C. § 222(f)(1)(A) (Supp. III 1997).

42. FCC, *Common Carrier Bureau's Homepage for the CPNI Proceeding* (visited Mar. 23, 2000) <http://www.fcc.gov/ccb/ppp/Cpni/welcome.html>. The FCC more formally explains CPNI as "information a telecommunications carrier obtains about a customer that relates to the quantity, technical configuration, type, destination, and amount of use of a telecommunications service subscribed to by that customer." *Id.*

As to the intersection between the First Amendment and privacy, compare Paul M. Schwartz, *Free Speech vs. Privacy: Eugene Volokh's First Amendment Jurisprudence*, 52 STAN. L. REV. (forthcoming 2000), with Eugene Volokh, *Freedom of Speech, Information Privacy, and the Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. (forthcoming 2000).

43. *See* 47 U.S.C. § 222(d) (Supp. III 1997).

44. *See U.S. West*, 182 F.3d at 1235 n.7.

45. *See id.* at 1237-38. In a vigorous dissent in *U.S. West*, Judge Briscoe argues, however, that no constitutional challenge had been made to the statute under which the FCC had acted and that, therefore, "the majority ignores the procedural context of this case." *Id.* at 1245. Judge Briscoe also observes, "[t]he administrative record convincingly demonstrates that, of the limited options available to

the Tenth Circuit is thereby constitutionalizing an opt-out requirement, it will squelch useful legislative and administrative experiments with different kinds of default rules. Even without that unfortunate result, the Tenth Circuit reaches a problematic conclusion concerning the high cost of opt-in.[46]

On this point, as I have noted, the appellate court agrees with Professor Cate, and I wish to conclude this section by examining their shared negative views about opt-in. Both the Tenth Circuit and Professor Cate discuss the difficulty that U.S. West faced when it voluntarily tested an opt-in system.[47] This telecommunications company had to call households an average of almost five times to reach adults who could grant consent and was forced to invest $38.00 in contacting each customer.[48] How much cheaper it appears, according to the federal appellate court and Professor Cate, to remove this burden on communication. More specifically, Professor Cate notes that opt-in causes greater privacy invasions as U.S. West practically laid siege to its customers' telephone lines in an attempt to obtain permission to use CPNI to market products to them.[49]

At best, this analysis suggests the need for additional methodological work regarding cost-benefit analysis under opt-out or opt-in. The Tenth Circuit and Professor Cate see companies under opt-in forced to waste resources in trying to reach consumers by calling them again and again. My own judgment is that this argument proves too much. The same kind of telephone harassment, or even additional such behavior, might also occur if an opt-out regime is instituted. Opt-out will lead to a barrage of marketing calls because once U.S. West and other companies analyze CPNI, they will contact customers, including those who simply failed to understand the need to take action to prevent such carrier behavior.

The goal regarding individually identified CPNI should be to find a way to permit consumers to make informed decisions about use of their information at the least cost to them.[50] To reach this goal, companies should be forced to internalize not only their own costs but at least some of their customers'. Such action, by raising the "price" of personal information and privacy violations, will improve efficiency in "privacy price dis-

---

the FCC, the opt-in method of obtaining customer approval was the most reasonable solution." *Id.* at 1246.

46. *See id.* at 1238.

47. *See id.* at 1239; Cate, *supra* note 23, at 893-94.

48. *See U.S. West*, 182 F.3d at 1239; Cate, *supra* note 23, at 893-94.

49. *See* Cate, *supra* note 23, at 894.

50. Congress expressed the conclusion regarding the need for *informed* decisions in the relevant statutory section under which the FCC enacted its regulations. *See* 47 U.S.C. § 222(d) (Supp. III 1997). This statute requires a telecommunications carrier to obtain customer approval when it wishes to use, disclose, or permit access to CPNI in a manner not specifically allowed under 47 U.S.C. § 222. *See U.S. West*, 182 F.3d at 1246 (Briscoe, J., dissenting) (noting "Congressional goal of informed customer consent").

crimination." By this term, I wish to indicate a differentiation by data processing companies among individuals with varying preferences about the use of their personal data.[51] Efficiency in the market for information privacy preferences should encourage companies to invest in less intrusive means for ascertaining consumer wishes.

III. GROUP NORMS, PRIVACY, AND INTERNET COMMUNITIES

In *Internet Privacy and the State*, I seek to identify ways for the State to enhance law and norms regarding information privacy. For Amitai Etzioni, my Article sidesteps "the resulting dilemma" of relying on "Big Brother to enhance privacy in the cyber-age."[52] At times, however, in his comment and recent book, *The Limits of Privacy*, Professor Etzioni recognizes the dangers posed by the private sector's data processing, and the need for a possible State role in response. Indeed, Professor Etzioni's analysis of the private sector's threat to privacy in his comment and in *The Limits of Privacy* is cogent and convincing.[53] He even terms private data processing entities, "Big Bucks," and in his comment admits, if only in a parenthesis, that "we shall need to rely on the government to protect us from Big Bucks."[54]

It would appear that Professor Etzioni and I therefore agree that a State role of some kind is necessary regarding information privacy. Where we differ most dramatically concerns not the State, but the community and its role in developing and enforcing standards for information privacy. As a leading communitarian as well as a distinguished multi-disciplinary scholar, Professor Etzioni places great hope in communities. As he tells us, "[i]t takes a village to prevent an indecent act."[55] If communities are granted more information about us, they will displace some of the State's oversight, and we will require less law and less governmental control for an equivalent amount of social order.[56]

Professor Etzioni argues that I have missed or otherwise misunderstood certain key aspects of communities and the communitarian movement. In response, I wish now to examine two of his observations, and then turn to the topic of the Internet and communities. First, Professor Etzioni finds

---

51. *See* Schwartz, *Privacy and the State*, *supra* note 2, at 832-33; Schwartz, *Privacy in Cyberspace*, *supra* note 2, at 1687 .

52. Amitai Etzioni, *A Communitarian Perspective on Privacy*, 32 CONN. L. REV. 897, 900 (2000) [hereinafter Etzioni, *Communitarian Perspective*].

53. *See id.* at 900-02; *see also* AMITAI ETZIONI, THE LIMITS OF PRIVACY 10, 129-30, 149-50 (1999) [hereinafter ETZIONI, LIMITS].

54. Etzioni, *Communitarian Perspective*, *supra* note 52, at 900.

55. *Id.* at 902 (emphasis omitted). For a further discussion, see ETZIONI, LIMITS, *supra* note 53, at 42.

56. *See* ETZIONI, LIMITS, *supra* note 53, at 215; Etzioni, *Communitarian Perspective*, *supra* note 52, at 904-05.

that while communities may have oppressed their members in the past, "[t]hese days, communities are often much too weak to oppress people, and people . . . can choose communities they find compatible."[57] Second, he rejects my argument regarding the frequent inefficiency of social norms. For Professor Etzioni, norms have a moral basis,[58] and even if norms sometimes exact high costs, people care about things other than efficiency anyway.[59]

As to the first point, regarding how groups oppress or do not oppress their members, I think that Professor Etzioni is trying to have it both ways. On one hand, he wants us to see that less privacy will mean that groups and other "voluntary associations" will be able to displace the State's law and better control their members (i.e., we live in strong communities).[60] On the other hand, he wants us to view groups as unlikely to oppress their members and points, for example, to the frequency with which many Americans move their households (i.e., we live in weak communities).[61] Presumably, some hidden Goldilocks principle is at work here that allows communities in modern American society to get it "just right." Nevertheless, Professor Etzioni, to my judgment, has not identified why we will get the right kind of communities and the right mixture of membership in different communities to obtain this happy result.

Concerning the moral aspect of group norms, which is Etzioni's second point, I certainly agree that norms often fulfill a moral role. In *Internet Privacy and the State*, however, I did not interpret norms in a fashion inconsistent with this perspective. Rather, I sought to indicate, first, that norms that are inefficient for a community may persist, and, second, that even norms that are efficient at the group-level may fail society as a whole (the problem of externalities).[62] Third, I sought to elaborate some of the implications of group norms for information privacy. In my view, the most important of these is that community-derived rules about personal data may lead neither to the right kind of norms nor to the right level of information disclosure for society as a whole.[63]

One part of Professor Etzioni's comment can be used to illustrate the complexity of the relationship between community norms, enforcement of behavioral standards, and information privacy. In his comment, Etzioni writes, "[t]he extent to which many professionals, such as physicians and lawyers, conform to their ethical codes is also largely determined by the

57. Etzioni, *Communitarian Perspective*, *supra* note 52, at 903.

58. For example, he states "child abuse violates the norms of most communities, whether or not it is efficient." *Id*.

59. *See id*.

60. *See id*.

61. *See id.*

62. *See* Schwartz, *Privacy and the State*, *supra* note 2, at 839.

63. *See id.* at 839-42.

values their particular community upholds, and mainly governed by informal enforcement mechanisms requiring social scrutiny but reducing need for government control."[64] One aspect of this observation, namely self-governance by physicians, actually demonstrates the opposite of Etzioni's point.

Considerable evidence exists of a lack of successful self-enforcement of practice norms by physicians through means such as peer review, which involves the process of granting staff privileges at hospitals. Peer review itself is not "mainly governed by informal enforcement mechanisms," but structured through law, in particular the Health Care Quality Improvement Act of 1986 (HCQIA).[65] The HCQIA seeks to encourage peer review by providing immunity from lawsuits for physicians who participate in this process and by making information about it confidential.[66] Although HCQIA confidentiality remains in place, other laws and regulations are seeking to create greater social access to information about physician error.[67] Some of this information is even being made available online.[68] Society has not deferred to physician self-governance, and is increasingly unwilling to let these professionals alone decide how much information privacy they will get.[69]

This flight from physician self-regulation is taking place because group norms often involve payoffs that largely accrue to the group. Cyberspace raises additional issues for those who study communities and norm development. Professor Etzioni points out that communitarians seek to strengthen voluntary associations as loci for "substantive moral dialogues in which the values of the members are engaged and persuasion occurs,

64. Etzioni, *Communitarian Perspective*, *supra* note 52, at 904.

65. 42 U.S.C §§ 11101-52 (1994).

66. *See id.* Even with this statutory encouragement, an empirical study of the performance of peer review questioned whether it is "taking place with sufficient frequency to affect significantly quality of care." Susan O. Scheutzow, *State Medical Peer Review: High Costs but No Benefit—Is it Time for a Change?*, 25 AM. J.L. & MED. 7, 15 (1999). This study also finds "peer review protection and reporting statutes are ineffective in promoting peer review and in ensuring that peer review reports are properly reported." *Id.* at 12.

67. For an analysis of the implications of this trend on physician's privacy, see Julie Barker Pape, *Physician Data Banks: The Public's Right to Know Versus the Physician's Right to Privacy*, 66 FORDHAM L. REV. 975 (1997).

68. *See id.* at 984 n.58.

69. Providing access to these data is an excellent example of "regulating through information" in the context of health care. Professor William M. Sage has recently offered a groundbreaking analysis of the possibilities for reforming health care in the United States by requiring organizations and health care providers to disclose different kinds of information to the public. *See* William M. Sage, *Regulating Through Information: Disclosure Laws and American Health Care*, 99 COLUM. L. REV. 1701 (1999). His thesis is that we require information disclosures for a cluster of different reasons—and ones that can conflict with each other. *See id.* at 1711-12. Professor Sage's work supports my response to Etzioni: society has neither deferred to informational self-governance by physicians nor permitted these professionals to set their own level of information privacy. *See id.* at 1703-08.

leading to a new or recast shared definition of the good."[70] The difficulty, as he perceptively notes, is that "while there can be virtual communities, most Internet forums are not."[71]

Fleeting Web experiences do not contribute to successful norm development by Internet communities. Or, as Mark Lemley has argued, the idea that "private ordering should be able to alter or replace existing substantive law," while "clearly in the ascendancy," is problematic in cyberspace.[72] As Professor Lemley points out, Internet norms are often elusive and rapidly changing.[73] In addition, in many instances the necessary consensus is absent for norm development because group homogeneity is absent on the Internet.[74]

Already, community-based Web sites seek to respond to at least some of these concerns by altering the passive and superficial nature of many Web experiences. Yet, such deepened online experiences rely in large part on less anonymity and collection of more finely grained personal data.[75] The paradox is that increasing community on the Internet may require more processing of personal data, which, without adequate safeguards, will make people less willing to join in the necessary cyber-civic organizations. Moreover, for those people who nevertheless join in cyber-communities, the online experience will be distorted by an increase in power for those who have greater access to personal data. The Comment by Michael Gerhardt also raises critical issues regarding community on the Internet, and I now turn to it.

IV. ONLINE POLITICS AND PRIVACY

In *Privacy, Democracy, and Democracy: A Case Study*, Michael Gerhardt focuses on the impeachment and acquittal of President Clinton in exploring how media and telecommunications in the Internet age affect life in a democracy.[76] Professor Gerhardt's comment reflects his great expertise as our leading scholar of federal appointments and impeachment. In it, he draws on his academic expertise as well as his experience testifying

70. Etzioni, *Communitarian Perspective*, *supra* note 52, at 903. Similar arguments are made by Professor Etzioni in his classic exposition of communitarianism. *See* AMITAI ETZIONI, THE SPIRIT OF COMMUNITY 255-67 (1993).

71. Etzioni, *Communitarian Perspective*, *supra* note 52, at 904.

72. Mark A. Lemley, *The Law and Economics of Internet Norms*, 73 CHI.-KENT L. REV. 1257, 1265 (1999); *see also id.* at 1266-92 (discussing this further).

73. *See id.* at 1267-70.

74. *See id.* at 1270-71.

75. For one of the most thoughtful academic proposals in this area, see Jerry Kang, *Cyber-Race*, 113 HARV. L. REV. 1131 (2000). Kang proposes a "zoning" of some private sector Web sites through measures including authentication of racial identities. *See id.* at 1137.

76. *See* Michael J. Gerhardt, *Privacy, Cyberspace, and Democracy: A Case Study*, 32 CONN. L. REV. 907 (2000) [hereinafter Gerhardt, *Privacy*].

before Congress during the Clinton impeachment crisis.[77]

Professor Gerhardt analyzes such events as the posting of the Starr Report on the Internet and the pressure that the Internet placed on the established "news cycle" of traditional media in terms of content and quality of their reporting.[78] He also discusses the phenomenon of media convergence. Journalists, participants in these historical events, and the public at large gathered news about the Clinton-Lewinsky scandal by drawing, more or less simultaneously, on the Internet, radio, broadcast television, and cable.[79] Embarrassing news about President Clinton was transmitted, publicized, and debated in more media formats than ever before possible.

Professor Gerhardt also examines the Internet's impact on opinion formation during the Clinton impeachment and acquittal. During the critical period when the Starr Report was released, many more people downloaded it from various sites than ever bothered to look at the President's rebuttal.[80] Nevertheless, as Professor Gerhardt notes, support for President Clinton intensified. Indeed, President Clinton's overall approval rating increased compared to the period before the scandal started.[81] In Professor Gerhardt's judgment, "many people made up their minds relatively fast and early in the reporting process on the bottom line issue—the necessity, or lack thereof, for the President's removal."[82] On this point, he concludes, correctly in my opinion, that much more research is needed regarding how the Internet affects public opinion formation.[83]

Professor Gerhardt also considers the government's ability to engage in "democracy-enhancing reform" of the Internet.[84] In language similar to

---

77. Professor Gerhardt was the only joint witness for both the majority and minority parties at a Senate hearing concerning whether the President's misconduct met the Constitution's test of impeachable behavior. *See* Michael J. Gerhardt, *The Perils of Presidential Impeachment*, 67 U. CHI. L. REV. 293, 309 (2000) [hereinafter Gerhardt, *Perils*]. He is also the author of the leading modern study of federal impeachment. *See* MICHAEL J. GERHARDT, THE FEDERAL IMPEACHMENT PROCESS: A CONSTITUTIONAL AND HISTORICAL ANALYSIS (1996).

78. *See* Gerhardt, *Privacy*, *supra* note 76, at 911-12.

79. *See id.* at 909.

80. *See id.* at 915 n.31.

81. *See id* at 915.

82. *Id*. Elsewhere, Professor Gerhardt has also predicted that Clinton's acquittal is likely to lead Congress to "recognize a presidential zone of privacy." Gerhardt, *Perils*, *supra* note 77, at 300.

83. One of the controversies that still rages about opinion formation during the impeachment crisis is the proper role of legal academics. Both Judge Posner and Neal Devins have criticized the behavior of law professors during this period as partisan and animated by self-interest. *See* ROBERT POSNER, AN AFFAIR OF STATE: THE INVESTIGATION, IMPEACHMENT, AND TRIAL OF PRESIDENT CLINTON 218 (1999); Neal Devins, *Bearing False Witness: The Clinton Impeachment and the Future of Academic Freedom*, 145 U. PA. L. REV. 165 (1999). Devins warns that mass signing of political letters is likely to lead the profession of law teaching into disrepute. *See* Devins, *supra*, at 190. For a defense of the behavior of legal academics at that time, see Ronald Dworkin, *Philosophy & Monica Lewinsky*, N.Y. REV. BOOKS, Mar. 9, 2000, at 48, 50; Cass R. Sunstein, *Professors and Politics*, 148 U. PA. L. REV. 191 (1999).

84. Gerhardt, *Privacy*, *supra* note 76, at 920.

that of Amitai Etzioni and Mark Lemley, which I have cited above, he finds that the Internet, as currently structured, lacks essential ingredients for democratic community.[85] Indeed, the Internet may actually harm civility norms, which are already fragile in this country.[86] Finally, the government has problems at times making even basic use of cyberspace. As Professor Gerhardt writes, "government Web sites that made the Starr Report available did not just freeze but also became unusable for other purposes because of the unusually high traffic."[87]

In his case study, Professor Gerhardt evaluates a political scandal, and how communication media, online and offline, helped shape it. The migration of political life to cyberspace and the resulting collection and broadcast of personal data in it will affect other activities. In the rest of this section, I consider how political life on the Internet will affect elections, perhaps the most fundamental event in a democracy. My remarks concentrate on the voting process and campaign finance.

First, political parties are seeking to engage in online primaries—and wish to use them as a way to gather personal data. On March 11, 2000, for example, the Arizona Democratic Party allowed voting in its presidential primary to take place on the Internet.[88] This event marks the first time that an element of a legally binding election for a publicly-held office took place online. Yet, as *DM News*, a trade publication for the direct marketing industry reports, "the biggest impact" of this election "could be its value as a list compiling and data-gathering tool for political direct marketers."[89] According to *DM News*, the Arizona Democratic Party asked online voters for their email addresses and other information.[90] Unless properly managed, online primaries will touch on one of the most sacred concepts of democracy—the secret ballot.[91]

---

85. *See id.* at 913-17.

86. *See id.* at 917. For more on civility norms, see ROBERT C. POST, CONSTITUTIONAL DOMAINS: DEMOCRACY, COMMUNITY, MANAGEMENT 51-88 (1995). *See also* Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CAL. L. REV. 957 (1989) (arguing in favor of the common law tort of invasion of privacy as a safeguard of social norms constituting both individual and community identity).

87. Gerhardt, *Privacy*, *supra* note 76, at 919.

88. *See* Lynn Burke, *Arizona Vote: Not Who But How*, WIRED.COM (visited Mar. 12, 2000) <http://www.wired.com/news/politics/0,1283,34911,00.html>; Lynn Burke, *Arizona Vote One for the Ages*, WIRED.COM (visited Mar. 10, 2000) <http://www.wired.com/news/politics/0,1283,34844,00.html>.

89. John Schonwald, *Arizona Dems to Build E-Mail Lists With Online Primary*, DM NEWS, Jan. 10, 2000, at 1, *available in* LEXIS, News Library, DM News File.

90. *See id.* It also provided the link for its ballot from a commercial Web site. *See* <http://www.election.com>.

91. The Internet primary election in Arizona was run by a private company, election.com, which spent millions of dollars on it. In the words of *The Standard*, this election was a "kind of loss leader" for election.com which was "hoping to pump up this experiment as a crucial component of its planned IPO." James Ledbetter, *'Virtual Voting' Faces Real-World Concerns*, STANDARD (visited Mar. 16, 2000) <http://www.thestandard.com/article/display/0,1151,12981,00.html>. This example suggests

Second, politics in cyberspace tests a central element of the established structure of campaign finance law. Federal law currently requires both: (1) disclosure of all those who donate to federal election campaigns, and (2) strict privacy restrictions on using these data for further solicitations or for purposes unrelated to the electoral process.[92] Pursuant to this statute, the Federal Election Commission posts information at its Web site regarding donors.[93] Proposals exist to expand such Internet postings to include a wider range of political contributors.[94] Yet, existing legal restrictions against further use of these personal data may become meaningless in the Internet Age if an increasingly decentralized information industry ignores applicable legal prohibitions, harvests these data, and reuses them. Moreover, statutory privacy restrictions are increasingly vulnerable to attack on First Amendment grounds as indicated by *U.S. West*, which I have discussed above.[95] In the future, we may view the release of the Starr Report on the Internet as only the restrained start for politics and privacy in cyberspace.

V. A SOCIOLOGY OF PRIVATE LAW-RECOMMENDING INSTITUTIONS

Finally, in *An Institutional Emphasis*, Lance Liebman responds to my consideration of the impact on privacy of decentralized rules, markets, industry self-regulation, and contract.[96] He urges that attention also be granted "the institutions now struggling to adapt existing public rules (laws) to the opportunities and dangers newly presented by technology."[97] In his comment, Professor Liebman adopts the role of a sociologist of law-recommending institutions. As the President of the American Law Institute (ALI), he is in a unique position to take this perspective and to evaluate non-governmental institutions acting to influence law and norms alike.

Professor Liebman predicts an increasing impact on information law of private law-recommending institutions, and, as a consequence, of state rather than federal influences.[98] As an example of the law-recommending organization, he discusses the ALI, the National Conference of Commis-

---

that online companies may continue to subsidize Internet elections to help establish their market niche. It leaves unanswered questions about information privacy—as well as "digital divide" issues relating to dramatic differences in access to cyberspace.

92. *See* 2 U.S.C. § 483(a)(4) (Supp. I 1995).

93. *See Federal Election Commission* (visited Mar. 23, 2000) <http://www.fec.gov>.

94. *See* Samuel Issacharoff & Pamela S. Karlan, *The Hydraulics of Campaign Finance Reform*, 77 TEX. L. REV. 1705, 1736-37 (1999). In contrast, Ian Ayres and Jeremy Bulow have proposed complete donor secrecy. *See* Ian Ayres & Jeremy Bulow, *The Donation Booth: Mandatory Donor Anonymity to Disrupt the Market for Political Influence*, 50 STAN. L. REV. 837 (1998).

95. *See supra* notes 39-50 and accompanying text.

96. *See* Lance Liebman, *An Institutional Emphasis*, 32 CONN. L. REV. 923 (2000).

97. *Id.* at 924.

98. *See id.* at 924-25.

sioners on Uniform State Laws (NCCUSL), the ALI's long term partner, and numerous other bodies.[99] As an example of how this institutional emphasis is already present in information law, he points to the planned Article 2B of the Uniform Commercial Code which, after a decade of work, became the Uniform Computer Information Transactions Act (UCITA), and which is now under consideration by state legislatures throughout the United States.[100]

In Professor Liebman's assessment, recourse to private law-recommending institutions brings with it promises and perils. Among the perils, these institutions may be unduly responsive to moneyed interests and state political concerns; offer representatives who "come from the elite levels of the practicing bar, the judiciary, and the professoriate"; and, finally, "give access to those who choose to participate."[101] At the same time, however, private law-recommending institutions have great potential. These bodies can provide "patient consideration of difficult legal questions in a public environment where discourse is about public interest and about professional drafting."[102] Laws may emerge from this process that are more carefully drafted than many judicial opinions, and more isolated from interest group pressure than many pieces of legislation. Professional law drafting may even, according to Professor Liebman, present a model for international and multinational organizations now examining issues of information privacy.[103]

To my mind, Professor Liebman in this comment raises the issue of how the work of private law-recommending institutions is to be integrated with the efforts of other non-governmental organizations. A wide range of these other institutions already exists: (1) industry organizations that promote self-regulation by drafting codes of conduct; (2) privacy seal organizations, such as TrustE and BBBOnline; (3) infomediaries that represent consumers; (4) privacy watchdog organizations; and (5) technical bodies, such as W3C, engaged in drafting Internet transmission standards, including P3P.[104] The difficulty is that we lack even a theoretical understanding of how these organizations are to work with each other and collaborate with private law-recommending institutions in shaping law, norms, and technology for information privacy.

One important issue in this context is how social investment in law,

---

99. *See id.* at 924-27.

100. *See id.* at 922-23. UCITA has been controversial. For recent reports, see Stephen Manes, *Click Here for a Bogus New Law*, FORBES, Mar. 20, 2000, at 296, *available in* LEXIS, News Library, Forbes File; Declan McCullagh, *Furor Over Virginia E-Biz Law*, WIRED.COM (visited Mar. 15, 2000) <http://www.wired.com/news/politics/0,1283,34947,00.html>.

101. Liebman, *supra* note 96, at 925.

102. *Id.* at 926.

103. *See id.* at 926-27.

104. *See* Schwartz, *Privacy in Cyberspace*, *supra* note 2, at 1694-96; Schwartz, *Privacy and the State*, *supra* note 2, at 854-55.

norms, and technology can reduce transactional bottlenecks. We have already seen such bottlenecks regarding the use of CPNI. Telecommunications companies want to use this information to market additional services and products; some consumers do not want these data used for such purposes. The transactional bottlenecks concern apportionment of different costs of communicating privacy preferences; how and where to set default rules; and the effect on data flow of consumer inaction. Regarding CPNI, Congress and the FCC acted to end this bottleneck both by mandating that telecommunications carriers obtain consumer approval outside of a narrow range of exceptions, and by establishing some of the conditions under which consumer approval was to be obtained.

A role for private law-recommending institutions might also exist in reducing transactional bottlenecks. One task would be the creation of a Restatement of the Law of Privacy, a possibility that Professor Liebman raises.[105] Yet, a further issue promptly emerges. Drafters of a Restatement of the Law of Privacy will face a fundamental choice between property and liability rules. Like the choice between opt-in and opt-out, this decision represents one between different starting points that are likely to lead to dramatically different results. This choice can be understood through the foundational framework of Calabresi-Melamed on legal entitlements.[106] In this framework, a property rule can only be infringed after bargaining with the holder of the interest.[107] This approach permits the holder to set the price for infringing ex ante. In contrast, a liability rule first allows infringement and follows this behavior with ex post determination by a tribunal of the appropriate compensation.[108]

The challenge for a potential privacy Restatement is that in various data processing contexts, the merits will be on different sides of the divide between property rules and liability rules. As a result, a Restatement of Privacy will be obliged to incorporate both kinds of rules within its framework and make complex choices between these standards. Drafters of this hypothetical, and perhaps future Restatement, will face no simple task in

105. *See* Liebman, *supra* note 96, at 925.

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

107. *See id.* at 1105-08.

108. *See id; see generally* Robert Merges, *Contracting into Liability Rules: Intellectual Property Rights and Collective Rights Organizations*, 84 CAL. L. REV. 1293 (1996) [hereinafter Merges, *Contracting*]; Robert Merges, *Of Property Rules, Coase, and Intellectual Property*, 94 COLUM. L. REV. 2655 (1994). Merges' contribution to the scholarship of property-liability rules is to propose that collective rights institutions, such as ASCAP and BMI in the music industry, promote efficient exchanges by promulgating rules and procedures that place an initial monetary value on members' property rights. *See* Merges, *Contracting*, *supra*, at 1318-26. By establishing a property baseline, these organizations allow a contracting into customized liability rules, such as licenses, by parties. Today, with the emergence of the privacy organizations mentioned above, the question becomes whether investment in different kinds of privacy intermediaries through choice of property or liability rules might reduce transaction costs.

drawing on both property and liability rules.

VI. CONCLUSION

In this Response, I have explored aspects of the five comments on my Article, *Internet Privacy and the State*, and found that they chart elements of a future agenda for privacy scholarship. First, Anita Allen explores issues regarding privacy and commodification of identity. Her main concern is with people who have control over their personal data, but choose to surrender as much of it as possible. She wants information privacy law to react to the cumulative consequences of the bad privacy choices that people make. Professor Allen's work points to the need to maintain a non-market language for speaking about the terms of accessibility, and non-accessibility to personal data.

Second, Fred Cate wants a strong pro-disclosure tilt in policy judgments about flows of personal information. Professor Cate points to the high cost of privacy and argues in favor of "opt-out" rather than "opt-in" rules. A choice of one rather than the other of these two starting points is likely to lead to different results. Through an analysis of the Tenth Circuit's opinion in *U.S. West v. FCC*, an opinion in which Professor Cate's scholarship influenced the court, I argue, however, that much work remains to be done regarding the methodology of choices among these two default rules.

Third, Amitai Etzioni calls for a communitarian approach to information privacy. He believes that if communities are granted more information about us, they will displace some of the State's oversight, and we will require less law and governmental control for an equivalent amount of social order. I am not convinced, however, that this result follows from Professor Etzioni's prescription. In my judgment, he has not identified why we will necessarily obtain the right kind of communities and the right mixture of membership in different communities to cause this happy result.

Professor Etzioni also points to the current weakness of virtual communities and shortcomings in their ability to develop norms. On this point, we are in full agreement. The paradox is that increasing community on the Internet by deepening virtual experiences may require less anonymity and more collection of finely grained personal information. In the absence of effective privacy rules, however, some people will choose not to participate in community-enriching Web sites. For those that do, moreover, the online community experience may be distorted by an increase in power of those who have greater access to personal data.

Fourth, Michael Gerhardt considers the migration of political life to the Internet through a case study of the Clinton impeachment. Among his findings is that of unprecedented media convergence with information about political events now flowing from the Internet, radio, broadcast tele-

vision, and cable. Nevertheless, public opinion seems to have formed fast and early regarding the need, or rather lack thereof, for the President's removal. Professor Gerhardt's Comment also suggests that political life will continue to take place on the Internet. Electoral life, through online voting and campaign finance, will also occur in cyberspace and have significant consequences for privacy and democratic life.

Fifth and finally, Lance Liebman, acting as a sociologist of law-recommending institutions, predicts an increasing influence of these organizations on information law. Professor Liebman also wonders if it is time for a Restatement of the Law of Privacy. In such a Restatement, a central choice will be between property and liability rules. The difficulty will concern the likely necessity of incorporating both property and liability rules in one legal framework.

Perhaps the overarching theme that emerges from these comments is the ongoing tension between market and non-market perspectives on privacy. Personal information is the gold currency of the new millennium. Yet, in non-market terms, access to personal data has a profound impact on both social structure and individual identity. The difficulty for privacy law will be in finding ways to incorporate both market and non-market approaches to personal data.