Free Speech vs. Information Privacy: Eugene Volokh's First Amendment Jurisprudence

Paul M. Schwartz*

Eugene Volokh's masterful contribution to this symposium examines caselaw, doctrine, and theory to reach the conclusion that "information privacy rules are not easily defensible under existing free speech law."[1] Although permitting a narrow exception for privacy protection through contract, Volokh casts doubt on the constitutionality of the common law privacy tort of invasion of privacy and most governmental statutes, existing or potential, that impose information privacy on the private sector.[2] His chief worry, as he claims at a number of junctures, is less the legal protection of personal information per se than its accompanying twisting and stretching of the First Amendment. Volokh argues that the government's safeguarding of information privacy endangers a wide range of speech unrelated to personal data.[3]

To do justice to Volokh's article, I should first draw attention to its magisterial contrasting of free speech and information privacy. Volokh describes a phenomenon of the greatest significance in the Information Age: The United States has a higher law of freedom of expression, a law that functions well as a force for sweeping information into the public domain. However, it is underdeveloped concerning checks on communication in the name of personal privacy. He depicts the development of a First Amendment that emphasizes the rights of private parties "to communicate personal information about [us]."[4] His article is the clearest expression that we have of the conflict between free speech and information privacy in the context of the First Amendment.

---

* Professor of Law, Brooklyn Law School. For their suggestions and comments on this paper, I wish to thank Ted J. Janger, Laura J. Schwartz, and Stefanie Schwartz. Finally, Eugene Volokh responded with grace and insights to my commentary. All Internet citations were current as of May 22, 2000.

1. Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049 (2000).

2. *Id.* at 1050-52.

3. *Id.* at 1063-65.

4. *Id.* at 1112.

In the hopes of furthering Volokh's exploration of the nexus between the First Amendment and information privacy law, I wish to concentrate on two aspects of his article and then raise one additional issue that it provokes, but does not examine in any detail. First, I will evaluate one of his core ideas, which is that fair information practices constitute, as Volokh memorably puts it, "a right to have the government stop people from speaking about [you]."[5] Second, I will use health care privacy as a test of Volokh's claims regarding both the contract exemption under the First Amendment and the sharply negative consequences of information privacy for free speech. Third, I will argue that his approach shifts power to private commercial entities and restricts some ability of legislatures to limit explicit privacy-robbing contracts.

I. FAIR INFORMATION PRACTICES AS A SILENCING OF SPEECH

A central idea in Volokh's *Freedom of Speech* is that, when government grants rights to information privacy that extend to the private sector, it has created a speech restraint. In other words, when the common law's privacy tort or statutory law creates fair information practices, the result is the imposition of silence on speakers.[6] Volokh examines potential justifications for such action in areas of law and theory ranging from contract, property, and commercial speech, to "speech on matters of private concern."[7] In all these areas save contract, Volokh finds existing justifications to be insufficient and "information privacy speech restrictions . . . sufficiently troubling" to merit opposition.[8] As I will explain below in Part II, however, the contract exception for privacy protection is of limited use, and, as a result, Volokh opposes most privacy protections possible for the private sector.

Information privacy law is troubling for Volokh because it substitutes either judge-made common law or statutes for the strictures of the Constitution. In his estimation, the Framers already expressed the constitutional benchmark for fair information practices in the First Amendment. Their standard bars the government from deciding "what subjects speakers and listeners should concern themselves with."[9] As Volokh states, "[w]e already have a code of 'fair information practices,' and it is the First Amendment . . . ."[10]

---

5. *Id.* at 1051.

6. *See id.*

7. *Id.* at 1088-97.

8. *Id.* at 1053.

9. *Id.* at 1089.

10. *Id.* at 1051. Volokh adds that the First Amendment "generally bars the government from 'control[ing the communication] of information' either by direct regulation or through the authorization of private lawsuits), whether the communication is 'fair' or not." *Id.* (footnote omitted).

His language here is reminiscent of Justice Hugo Black's ringing dissent in *Konigsberg v. State Bar of California*: "[T]he First Amendment's unequivocal command that there shall be no

Volokh examines and rejects many possible justifications for safeguarding information privacy. He pays less attention, however, to the underlying concept of fair information practices. For him, these measures simply represent limitations on speech. The traditional idea of these standards is different, however, from Volokh's presentation of them.

During the 1970s, the United States developed fair information practices as its leading tool for privacy protection.[11] By the end of that decade, fair information practices had coalesced into their current form.[12] Although these standards differ in details, sometimes crucially, depending on the precise context of data processing, fair information practices generally require: (1) the creation of a statutory fabric that defines obligations with respect to the use of personal information; (2) the maintenance of processing systems that are understandable to the concerned individual (transparency); and (3) the assignment of limited procedural and substantive rights to the individual.[13] These standards also include a fourth element: (4) the establishment of effective oversight of data use, whether through individual litigation (self-help), a government role (external oversight), or some combination of these approaches.[14]

When the government requires fair information practices for the private sector, has it created a right to stop people from speaking about you? As an initial point, I emphasize that the majority of the core fair information prac-

---

abridgement of the rights of free speech and assembly shows that the men who drafted our Bill of Rights did all the 'balancing' that was to be done in this field." Konigsberg v. State Bar of Cal., 366 U.S. 36, 61 (1961) (Black, J., dissenting). For similar language, see Hugo L. Black, *The Bill of Rights*, 35 N.Y.U. L. REV. 865, 879 (1960).

11. Colin Bennett provides an excellent, concise description of the developments during this decade. *See* COLIN J. BENNETT, REGULATING PRIVACY 96-101 (1992). Three decisive policy moments for privacy came during the 1970's. This period saw: (1) an influential study published by the Department of Health, Education and Welfare that articulated elements of a code of fair information practices; (2) the Privacy Act of 1974, which established these practices for federal agencies; and (3) the wide-ranging final report in 1977 of the Privacy Protection Study Commission, a federal blue ribbon commission that examined the precise, potential content of fair information practices in different social contexts and assessed the functioning of the Privacy Act. *Id.* For a comparative perspective on these American developments that compares them to developments in Germany, France, Sweden, and Canada, see DAVID H. FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES 21-26, 93-103, 165-74, 243-48 (1989).

12. Perhaps the clearest evidence of this movement by the end of the 1970's comes from the Privacy Act of 1974, which in Section (e) requires fair information practices for federal agencies. 5 U.S.C. § 552a(e) (1974). For a discussion, see PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW § 5 (1996). The leading statutory embodiment from this era of these practices for the private sector is the Fair Credit Reporting Act of 1970, 15 U.S.C. § 1681 (1970).

13. For discussion of the standards, see Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 IOWA L. REV. 553, 557-64 (1995) [hereinafter Schwartz, *Privacy and Participation*]; *see also* BENNETT, *supra* note 11, at 101-11.

14. Here, too, a leading example is found in the Privacy Act, 5 U.S.C. § 552a(d), (e), (g) (1974). For analysis of these aspects of the law, see SCHWARTZ & REIDENBERG, *supra* note 12, § 5-5(b).

tices do *not* involve the government preventing disclosure of personal information. To return to the schema in the preceding paragraph, fair information practices one, two, and four regulate the business practices of private entities without silencing their speech. No prevention of speech about anyone takes place, for example, when the Fair Credit Reporting Act of 1970 requires that certain information be given to a consumer when an "investigative consumer report" is prepared about her.[15]

These nonsilencing fair information practices are akin to a broad range of other measures that regulate information use in the private sector and do not abridge the freedom of speech under any interpretation of the First Amendment. The First Amendment does not prevent the government from requiring product labels on food products or the use of "plain English" by publicly traded companies in reports sent to their investors or Form 10-Ks filed with the Securities and Exchange Commission.[16] Nor does the First Amendment forbid privacy laws such as the Children's Online Privacy Protection Act, which assigns parents a right of access to their children's online data profiles.[17] The ultimate merit of these laws depends on their specific context and precise details, but such experimentation by the State should be viewed as noncontroversial on free speech grounds.[18]

Nevertheless, one subset of fair information practices does correspond to Volokh's idea of information privacy as the right to stop people from speaking about you. As part of the State's assignment of limited procedural and substantive rights to the individual—the third category of fair information practices—privacy laws may contain disclosure restrictions.[19] Consider one example of such a statutory disclosure restriction, the Video Privacy Protection Act of 1988, also known as the Bork Bill.[20] Congress enacted this statute after a Washington, D.C., periodical published a list of then Judge Robert

---

15. 15 U.S.C. § 1681d (1970).

16. For an attempt to explain such examples of information regulation from an economic perspective, see Wesley A. Magat, *Information Regulation*, in THE NEW PALGRAVE DICTIONARY OF ECONOMICS AND THE LAW 307-10 (Peter Newman ed., 1998).

17. 15 U.S.C. § 6502(b)(1)(B) (1998).

18. Such is the merit of the challenge that Volokh raises to information privacy, however, that it will be impossible after his article to point to any single doctrine or simple loophole and imagine that the First Amendment question has been neatly resolved. In this context, I should note Volokh's astute reading of the Supreme Court's Commercial Speech doctrine. Volokh, *supra* note 1, at 1080-87.

19. This comment will now concentrate on statutory rather than common law examples of information privacy because the most important recent developments have come in statutory law. On the (relative) demise of tort privacy, see Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497, 504-06 (1995) (arguing that adequate standards for the treatment of personal information are a necessary condition for citizen participation in democracy); Diane L. Zimmerman, *Requiem for a Heavyweight: A Farewell to Warren and Brandeis's Privacy Tort*, 68 CORNELL L. REV. 291, 362 (1983) (challenging prevailing tort and constitutional law that seeks to harmonize privacy and free speech).

20. U.S.C. § 2710 (1994).

Bork's video rentals.[21] Unless a disclosure falls within a narrow range of exceptions, the Bork Bill prohibits the release of a consumer's name linked to the title, description, or subject matter of any videotape that she has rented or purchased from an entity subject to the Act.[22] Viewed through the Volokhian perspective, this statute creates a right to stop video stores from talking about you and your video rentals.

In my judgment, however, the Bork Bill and similar privacy statutes do not represent an unconstitutional silencing of parties under the First Amendment. Rather, so long as they are viewpoint neutral, these laws are a necessary element of safeguarding free communication in our democratic society.[23] Volokh's reading of the First Amendment seeks to radically and permanently enshrine public discourse as the predominant sphere of communication. By shielding existing and possible future portals to this domain from almost all legal restrictions, Volokh furthers a process by which any topic or record can become the source of public scrutiny and debate. Yet, no less than public discourse, a democratic society depends on other realms of communication. As an important step in establishing the foundations of a modern information privacy jurisprudence, Robert Post provided a map of these other domains of communicative discourse, which he terms "community" (where speech can be regulated in the interests of civility and dignity) and "bureaucratic organization" (where speech can be regulated for instrumental attainment of explicit objectives).[24]

Building on Post's work, I wish to argue that fair information practices can best be thought of as fulfilling two normative roles regarding communicative discourse. First, these rules help maintain the boundary between pub-

---

21. *See* PRISCILLA M. REGAN, LEGISLATING PRIVACY 207 (1995) (examining congressional formulation and adoption of legislation to protect privacy where privacy was perceived to be threatened by new technologies).

22. *See* 18 U.S.C. § 2710(b)(1). This statute also permits a civil action when it is violated. Relief under it includes actual damages, liquidated damages in the amount of $2500, punitive damages, reasonable attorneys' fees, and other preliminary and equitable relief as a court determines appropriate. *Id.* at § 2710(c).

23. Concerning viewpoint neutrality, a privacy law would raise this issue if it selected which personal information to protect based on the viewpoint that these data revealed. Consider a hypothetical "Politically Correct Video Privacy Protection Act." In this thought experiment, the law's disclosure restrictions would be restricted to movie titles based on the political views, or other preferences, of the customer. And such a law would be unconstitutional. *See* Rosenberger v. Rector and Visitors of Univ. of Virginia, 515 U.S. 819, 828-37 (1995) (invalidating university policy that authorizes payments for student publications on basis of viewpoint). But Congress did not pass such a law. *See* Dirkes v. Borough of Runnemede, 936 F. Supp. 235, 239-40 (D. N.J. 1996) (applying Video Privacy Protection Act to case involving the disclosure of plaintiff's rental of pornographic videotapes).

24. Robert C. Post, *The Constitutional Concept of Public Discourse: Outrageous Opinion, Democratic Deliberation, and* Hustler Magazine v. Falwell, 103 HARV. L. REV. 601, 627-46 (1990) (analyzing the theory behind the Supreme Court's extension of constitutional protection to outrageous and offensive speech).

lic discourse and the other realms of communication. This role is largely fulfilled by the nondisclosure subset of fair information practices. For example, the Bork Bill's prohibition on the release of video rental information keeps these data from becoming part of public discourse.[25] To express this function within terms of free speech doctrine, one would say that it helps prop up the concepts of "the nonpublic context" and "the nonpublic figure."[26] Leading Supreme Court decisions have left these doctrines more than slightly tattered, but they are nonetheless essential.[27]

Second, standards of fair information practices serve to safeguard deliberative democracy by shaping the terms of individual participation in social and political life. As I have argued elsewhere, a democratic order depends on both an underlying personal capacity for self-governance and the participation of individuals in community and democratic self-rule.[28] Privacy law thus has an important role in protecting individual self-determination and democratic deliberation. By providing access to one's personal data, information about how it will be processed, and other fair information practices, the law seeks to structure the terms on which individuals confront the information demands of the community, private bureaucratic entities, and the State. Attention to these issues by the legal order is essential to the health of a democracy, which ultimately depends on individual communicative competence.[29]

II. HEALTH CARE PRIVACY, THE LIMITS OF CONTRACT, AND THE NUANCED SLIPPERY SLOPE

Volokh's skepticism towards information privacy rests on his conviction that it threatens the vitality of the First Amendment. An exception for pri-

---

25. For an example of a federal district court applying this law, see *Dirkes*, 936 F. Supp at 239-40.

26. For an introduction to these ideas, see RODNEY A. SMOLLA, FREE SPEECH IN AN OPEN SOCIETY 122-48 (1992).

27. For the leading cases, see Florida Star v. B.J.F., 491 U.S. 524 (1989); Hustler Magazine v. Falwell, 485 U.S. 46 (1988); Cox Broadcasting Corp. v. Cohn, 420 U.S. 469 (1975); Gertz v. Robert Welch, 418 U.S. 323 (1974).

28. *See* Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1647-66 (1999) (arguing for certain legal limits on access to personal information in cyberspace in order to achieve greater participation of individuals in democratic and civil forums); Schwartz, *supra* note 13, at 557-64.

29. For scholarship considering different aspects of and threats to communicative competence, see Kathleen M. Sullivan, *First Amendment Intermediaries in the Age of Cyberspace*, 45 U.C.L.A. L. REV. 1653, 1664-66 (1998) (exploring reasons why speech intermediaries, such as media corporations and private universities, might sometimes enjoy a First Amendment right to restrict the speech of others); Post, *supra* note 24, at 627-46; Spiros Simitis, *Reviewing Privacy in an Information Society*, 135 U. PA. L. REV. 707, 732-37, 746 (1987) (examining the relationship between information processing and democracy, and the importance of privacy protection in securing individuals' ability to communicate and participate in democratic society).

vacy grounded in contract is permissible, however, because parties under this approach have bound themselves not to talk. I would now like to consider the topic of personal health care data and use it to evaluate both Volokh's fondness for contractual solutions and his prediction that privacy protection threatens free speech.

Volokh makes two claims regarding personal information in the medical setting. First, he indicates that protection of health care data is permissible through contract law. In his estimation, it is "proper for the government to impose confidentiality requirements on lawyers, doctors, psychotherapists, and others: When these professions say 'I'll be your advisor,' they are implicitly promising that they'll be confidential advisors, at least so long as they do not explicitly disclaim any such implicit promise."[30] A code of fair information practices can therefore be imposed by the state on medical and other professionals, at least under some circumstances, without raising First Amendment difficulties. Thus, for Volokh, when "confidentiality really is part of most people's everyday expectations," a theory of implicit contract can be used to justify information privacy.[31]

Later in his article, Volokh discusses insurance companies and employers and makes his second claim regarding personal medical data, which is that these parties should be freely permitted to gather and disseminate personal data, including health information, about their customers.[32] While such entities might use such information to engage in discriminatory or otherwise unwanted behavior, Volokh argues that the government cannot suppress speech about particular people's "race, criminal history, alcoholism, drug use, or pizza consumption, even though such advocacy may lead some people to actually engage in such discrimination."[33] Hence, in Volokh's view, privacy laws that (1) apply to professional advisors and (2) are permissible under his contract exception may not be extended to other parties. Indeed, even the contract loophole for health care professionals does not go so far as to permit "speech-restrictive terms that the government compels a party to include in a contract."[34]

In the modern era of health care services, three significant problems arise with Volokh's approach. First, Volokh's contract model looks back to an earlier era in which independent medical professionals were the most important deliverers of services, and most patients paid their own way. Today, as a result of evolving models for health care providers and insurers and accompanying alterations in the use of personal health care information, the idea of looking for explicit or implicit understandings of confidentiality

30. Volokh, *supra* note 1, at 1058.

31. *Id.* at 1059.

32. *See id.* at 1119-20.

33. *Id.* at 1120.

34. *Id.* at 1061.

based on "most people's everyday expectations" is to rely, at best, on guesswork.[35] In the age of managed care, health maintenance organizations, and physician practice groups, a patient's most important relationships are less with a single medical professional than with a variety of institutions.[36] The use of personal data by these organizations, which know the patient largely through her health care records, are not easily structured by searching for anyone's implicit or explicit understandings of privacy. Indeed, these understandings themselves are largely shaped by how data are used.[37] The actual circumstances of personal data use have tremendous normative power to mold our expectations of informational privacy.

Second, Volokh's reliance on contract enshrines private law in an area—health care—where public law has become dominant. Due to the importance of medical services to the nation's well-being and the government's multifaceted role in financing and regulating health care services and research, modern health care law is increasingly public law. As one indication of this flight to public law, American law increasingly refuses to allow the terms for the use of personal medical data to be shaped primarily by private parties through fully customized negotiations. The Department of Health and Human Service's (HHS) draft guidelines for personal health care information are only the most recent and elaborate of such attempts to limit private parties' contractual ability to negotiate privacy standards.[38] Freedom of contract is severely limited in the context of medical records, and Volokh's proposal to re-enshrine it seems quaint and anachronistic.[39] Depending on one's reading of the past, it may also be ahistoric. Health care confidentiality itself arguably arises in American law less from any exclusive basis in contract than from the introduction of fiduciary concepts to restrict contract.[40]

Third, rather than a single rule regarding disclosure or privacy, more complex approaches to setting standards for health care data are needed. I have termed the necessary kinds of rules as "multifunctional" in nature: Any

---

35. *Id.* at 1059.

36. For an introduction to these changing institutional providers, see CLARK C. HAVIGHURST, JAMES F. BLUMSTEIN & TROYEN A BRENNAN, HEALTH CARE LAW AND POLICY 591-789 (2d ed. 1998).

37. This point can also be made in the context of Fourth Amendment privacy. *See* SCHWARTZ & REIDENBERG, *supra* note 12, § 4-4(c)(1), at 64 ("This amendment applies only when society already awaits it. In the context of data protection, this circular approach ignores the silent ability of technology to erode our expectations of privacy.").

38. *See* Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. 59,918 (1999) [hereinafter HHS Draft Privacy Regulations].

39. For example, the state does not allow patients, physicians, and/or hospitals to negotiate to refuse to share data regarding gunshot wounds or infectious diseases. For a discussion, see Paul M. Schwartz, *The Protection of Privacy in Health Care Reform*, 48 VAND. L. REV. 295, 321 (1995).

40. *See* WILLIAM J. CURRAN, MARK A. HALL, MARY ANNE BOBINSKI & DAVID ORENTLICHER, HEALTH CARE LAW AND ETHICS 187-89 (5th ed. 1998) (arguing that physicians' duties to their patients arise from the core fiduciary nature of the treatment relationship).

effective scheme of privacy controls must be tied to and follow data through their different applications because the same personal information is increasingly shared in a multiplicity of settings.[41] Due to multi-dimensional use of health care data, two-party private contractual negotiations cannot be relied upon to develop the necessary standards for personal health care data. This third point, like the preceding two, highlights the extreme limitation of Volokh's contract exception for privacy protection. Purely private multi-party negotiations are problematic because of the public interest in how health care information is used, as well as the lack of patient privity with some of the most important data processing entities, who receive health care data far downstream from patients.[42] One significant consequence of this phenomenon of dispersed data use occurs in cyberspace, where a recent empirical survey has found that few health Web sites maintain a chain of trust with third parties on their site.[43] According to this study, even Web sites with privacy policies regarding their own use of personal data may not oversee or otherwise limit the data processing of their affiliates.[44] The example of medical data suggests that the State has ample reasons not to allow the bounds of communicative discourse regarding personal data to be hammered out by private parties alone.

Finally, I wish to comment on two aspects of Volokh's nuanced slippery slope. First, for Volokh, in concrete and specific ways, "upholding certain kinds of information privacy speech restrictions could affect the protection of other speech."[45] As he writes, "If the legal system accepts the propriety of laws mandating 'fair information practices,' people may become more sympathetic to legal mandates of, for instance, fair news reporting practices or fair political debate practices."[46] Second, in place of privacy law, Volokh argues that it is preferable to protect information privacy through privacy-enhancing techniques such as technological self-protection, market pressures, restraints on government collection and revelation of information, and recourse to social norms.[47]

In my view, however, information privacy law is less a step on a slippery slope than a necessary element in a process of line-drawing along different

---

41. *See* Paul M. Schwartz, *Privacy and the Economics of Personal Health Care Information*, 76 TEX. L. REV. 1, 51-55 (1997).

42. For a detailed chart of the parties involved in receipt and processing health care information, see GEORGETOWN UNIVERSITY INSTITUTE FOR HEALTHCARE RESEARCH AND POLICY, HEALTH PRIVACY PROJECT, EXPOSED (Dec. 1999), 8-9 <http://www.healthprivacy.org/resources/index.shtml> [hereinafter GEORGETOWN PRIVACY PROJECT] .

43. See Janlori Goldman, Zoe Hudson & Richard M. Smith, *Report on the Privacy Policies and Practices of Health Web Sites* <http://ehealth.chcf.org/priv_pol3/index_show.cfm?doc_id=33>.

44. *Id.*

45. Volokh, *supra* note 1, at 1052.

46. *Id.*

47. *See id.* at 1111.

coordinates to shape personal interests in personal data and permissible kinds of use. Consider the guarantee in the HHS draft guidelines of an individual's ability to inspect and copy one's medical records, a right which only twenty-eight states provide at present.[48] This example points to the role of fair information practices in maintaining personal integrity against the onslaught of bureaucratic organizations. For that matter, even within the Volokhian contractual perspective, individuals who are expected to negotiate the terms of information privacy will be hard pressed to do so if they are not even permitted to examine their own records.

Moreover, while Volokh's suggested privacy-enhancing measures are important, the government itself often has a necessary role in stimulating their development. To point to only two elements of Volokh's privacy wish list, the State currently has an essential role in creating conditions for a functioning privacy market and in stimulating privacy norms that prevent groups, norm entrepreneurs, and the government itself from being excessively meddlesome.[49] Rather than the slippery slope that Volokh describes, such market-correcting and norm-shaping activities can serve an important constitutive function for democratic society.

III. WINNERS AND LOSERS: INSTITUTIONAL, LEGAL, AND PROCEDURAL

As a final matter, and to extend my previous analysis, I will consider the institutional, legal, and procedural forms that Volokh's jurisprudence of privacy is likely to encourage. Here, my concern is that his approach shifts power to private commercial entities and limits at least some ability of legislatures to place limits on privacy-robbing contracts. In tracing how Volokh reaches this result, I also wish to clear up a possible misreading of his Article, which turns on his view of the scope of "implicit" privacy contracts.

Law is not an abstract monument, but, rather, a system of rules generated, administered, and enforced by different institutions drawing on a range of possible procedures.[50] By constitutionalizing out of existence privacy protections found in many legal sources, Volokh uses the First Amendment to set the stage for a reign of contract. The ultimate institutional, legal, and procedural consequences of this move depend, however, on how Volokh defines the scope of contract. Interestingly enough, Volokh permits both explicit and what he calls "implicit" agreements about privacy, and this

48. *See* HHS Privacy Regulations, *supra* note 38, at 60059; GEORGETOWN PRIVACY PROJECT, *supra* note 42, at 14.

49. I develop this argument in more detail in *Internet Privacy and the State*, 32 CONN. L. REV. 815 (2000). On excessive meddlesome behavior of the State or norm entrepreneurs, see TIMUR KURAN, PRIVATE TRUTHS, PUBLIC LIES 23-24 (1995).

50. This concept of law is also that of the legal realists'. *See, e.g.*, K.N. LLEWELLYN, THE BRAMBLE BUSH 3 (1930) (noting that "what officials do about settling disputes is the law itself").

decision has far reaching consequences, mostly positive, for his jurisprudence of privacy.

To begin with, Volokh makes clear that the government can enforce explicit privacy contracts without violating the First Amendment.[51] More subtly, however, he also permits implicit privacy contracts. In a key passage, he writes, "a legislature may indeed enact a law stating that certain legislatively identified transactions should be interpreted as implicitly containing a promise of confidentiality, unless such a promise is explicitly and prominently disclaimed by the offeror, and the contract together with the disclaimer is accepted by the offeree."[52] At this juncture, I must confess to initially being led astray by Volokh's use of the term "implicitly" in this sentence and by his overall linkage of First Amendment exceptions for explicit and implicit contracts.

My first impression was that implicit contracts in the sense of Volokh's privacy jurisprudence were merely the opposite of explicit contracts. I believed that implicit contracts were restricted to the existing, but non-manifest understandings of parties to an agreement. An interpretation of the First Amendment as permitting such implicit privacy contracts as well as explicit ones—and no more—would be highly problematic, however, on two separate grounds.

One problem is that this reading of the First Amendment would transform federal judges into arbiters with the power to decide if there existed a social convention of confidentiality that merited inclusion in the First Amendment's contract exemption. Unless a federal judge decided that information privacy was part of most people's everyday expectations, or protected by an explicit enough contract, the judge would be obliged to invalidate any challenged legislation, common law tort action, or individual agreement.[53] Moreover, this transfer of power to federal courts would undercut not only legislatures and common law courts, but a wide variety of governmental agencies that scrutinize the behavior of private sector data processors and seek to encourage industry self-regulation.[54]

---

51. Volokh, *supra* note 1, at 1057-58.

52. *Id.* at 1060.

53. Among the dangers of such a role for the judiciary is that it would require courts to assess expectations of privacy not only when the state acts, as is currently the case under the Fourth Amendment, but also when the private sector is involved. For two classic criticisms of the Supreme Court in this role of assessor of privacy expectations under the Fourth Amendment, see Christopher Slobogin & Joseph E. Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permitted by Society,"* 42 DUKE L.J. 727, 735-39 (1993); Anthony J. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 403 (1974).

54. Indeed, to the extent that some movement has been made towards self-regulation by online industry, it has been encouraged by the Clinton Administration's (mild) threats of formal legislation if industry is inactive in this regard. *See, e.g.*, White House, *The Framework for Global Electronic Commerce* 12 (1997) <http://www.whitehouse.gov/WH/News/Commerce/> ("The Ad-

In reality, however, Volokh intends something quite different and more complex by his concept of implicit contracts. He uses the term to refer to not merely inherent understandings, but also wide-ranging default statutes. As he describes the merit of default privacy legislation, it can "clarify people's obligations instead of leaving courts to guess what people likely assumed."[55] Volokh indicates that he reads the First Amendment as permitting privacy statutes to go beyond reasonable or inherent understandings and to play an active role in shaping privacy understandings. Thus, his *Cohen v. Cowles* exception is potentially quite broad and allows: (1) explicit contracts, (2) implicit contracts based on inherent understandings and social circumstances that indicate confidentiality, and (3) default statutes. Volokh also adds an important constitutional restriction, however, on the last source of privacy rules.

His significant limitation on default privacy legislation is that it must allow parties the option of drawing up a different agreement. Volokh creates a constitutional obligation that all privacy statutes be, in the language of contract law, non-mandatory, or, in the terminology that E. Allan Farnsworth favors, "suppletory."[56] The legislature may set a default, but only so long as it is disclaimable.[57] In other words, Volokh reads the First Amendment as requiring that parties be permitted to disclaim any requirement of confidentiality that the law obliges. The danger here is *not* that parties to the contract will have surprises hidden from them in contracts or clickwrap provisions; Volokh does permit a statutory requirement that privacy disclaimers be in bold print or agreed to separately.[58] Nonetheless, Volokh's requirement of bilateral opting out from privacy statutes is flawed for two reasons.

---

ministration considers data protection critically important. We believe that private efforts of industry working in cooperation with consumer groups are preferable to government regulation, but if effective privacy protection cannot be provided in this way, we will reevaluate this policy."). This threat would become hollow if companies had an incentive to engage in constitutional litigation rather than self-regulation.

55. Volokh, *supra* note 1, at 1060.

56. E. ALLAN FARNSWORTH, CONTRACTS 33 (2d ed. 1990). On privacy default contracts, see Jeff Sovern, *Opting In, Opting Out, or No Options At All: The Fight for Control of Personal Information*, 74 WASH. L. REV. 1033, 1101-1116 (1999); Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1246-49 (1998); Schwartz, *supra* note 41, at 54-55. For the classic expositions of the concept of the default rule, see Ian Ayres & Robert Gertner, *Strategic Contractual Inefficiency and the Optimal Choice of Legal Rules*, 101 YALE L.J. 729, 735-40 (1992); Ian Ayres & Robert Gertner, *Filling Gaps in Incomplete Contracts: An Economic Theory of Default Rules*, 99 YALE L.J. 87, 93 (1989).

57. Volokh, *supra* note 1, at 1060.

58. *See id.* at 1061-62. In a similar fashion, the Uniform Commercial Code sometimes requires that terms be "conspicuous" to be enforceable. *See, e.g.*, UCC 1-201(10) ("A term or clause is conspicuous when it is so written that a reasonable person against whom it is to operate ought to have noticed it. . . . Language in the body of a form is 'conspicuous' if it is in large or other contrasting type or color.").

First, Volokh's constitutional requirement that privacy statutes be disclaimable shifts power to large commercial entities with market power and away from those individuals whose personal data are collected and processed. The resulting agreements, even when explicit in their privacy terms, may, nevertheless, be contracts of adhesion. In his classic article on this topic, Friedrich Kessler proposed in 1943 that meanings of "freedom of contract . . . change with the social importance of the type of contract and with the degree of monopoly enjoyed by the author of the standardized contract."[59] For Volokh, in contrast, the First Amendment requires that the privacy contracts be available and enforceable as a constitutional requirement.

Second, as I have noted above in Part II's discussion of personal health care data, American law places significant limits on the ability of private parties to fully shape the terms for the use of personal medical data. It restricts fully customized negotiations because of the overriding public interest in certain kinds of access and restrictions on personal data use. In health care as well as certain other societal sectors, allowing exclusive bilateral power to private parties to determine the scope of information contracts would have a negative impact on society as a whole. For example, public health in the United States would be worse off if physicians and patients were left to customize their own rules for access to medical data for health care research.[60] Under these circumstances, significant data might become inaccessible to health care researchers. Equally problematic would be fully customized rules between physicians and patients that restricted access to treatment information for fraud or malpractice purposes. Due to the central role in financing health care by such third parties as government, insurers, and employers, an exclusive interest in customizing information rules cannot rest with physicians and patients alone.[61]

IV. CONCLUSION

Eugene Volokh's contribution to this symposium is a prodigious analysis of free speech jurisprudence that reaches the conclusion that almost all information privacy law in the private sector is unconstitutional. As Volokh himself admits, however, alternative readings of existing caselaw, new judi-

---

59. Friedrich Kessler, *Contracts of Adhesion - Some Thoughts About Freedom of Contract*, 43 COLUM. L. REV. 629 (1943).

60. On current policies on research users of health information and the use of Institutional Review Boards to protect health information, see COMMITTEE ON MAINTAINING PRIVACY AND SECURITY IN HEALTH CARE APPLICATIONS ON THE NATIONAL INFORMATION INFRASTRUCTURE, NATIONAL RESEARCH COUNCIL, FOR THE RECORD: PROTECTING ELECTRONIC HEALTH INFORMATION 134-35 (1997).

61. *See* Schwartz, *supra* note 41, at 53 ("A physician and patient, or an employer and employee, cannot engage in fully customized negotiations because such bargaining might lead to excessive limits on the access to data of such parties as insurance programs (including publicly financed programs), public health agencies, and law enforcement agencies.").

cial decisions, and additional developments in legal doctrine might justify a different verdict.[62]

In this comment, I have proposed that no less than public discourse, a democratic society depends on other realms for communication. Drawing on examples from health care law, I have also questioned the usefulness of a contract exception for privacy and the likelihood of a slippery slope, nuanced or otherwise, if the law acts to protect information privacy. Finally, I have argued that Volokh's approach shifts power to private commercial entities and limits some legislative limits on privacy-robbing contracts.

Information privacy law has an important role to play in structuring communicative discourse in a deliberative democracy. Nevertheless, Volokh raises a significant gauntlet to information privacy jurisprudence. Justices and judges, policymakers, and legal scholars will have much work to do in response.[63] The challenge will be to demonstrate that information privacy law is an integral element of the mission of free speech and not its enemy.

62. Volokh, *supra* note 1, at 1051-52.

63. Two recent judicial decisions point to the likely increase in conflict in this decade between free speech and information privacy: (1) Los Angeles Police Dep't v. United Reporting Publishing Corp., 120 S.Ct. 483 (1999) (upholding a privacy law against a free speech challenge by a narrow finding that the litigation presented only a "facial challenge"); and (2) U.S. West v. Federal Communications Comm'n, 182 F.3d 1224 (10th Cir. 1999) (invalidating privacy regulations of the Federal Communications Commission for "customer proprietary network information" (CPNI) squarely on First Amendment grounds).