THE YALE LAW JOURNAL

PATRICIA L. BELLIA

Federalization in Information Privacy Law

ABSTRACT. In *Preemption and Privacy*, Professor Paul Schwartz argues that it would be unwise for Congress to adopt a unitary federal information privacy statute that both eliminates the sector-specific distinctions in federal information privacy law and blocks the development of stronger state regulation. That conclusion, though narrow, rests on descriptive and normative claims with broad implications for the state-federal balance in information privacy law. Descriptively, Professor Schwartz sees the current information privacy law landscape as the product of successful experimentation at the state level. That account, in turn, fuels his normative claims, and in particular his sympathy with theories of competitive federalism. As I will argue, however, we cannot ignore the federal inputs – judicial and legislative – that shape significant segments of state information privacy law. The story of information privacy law is one of federal leadership as well as state experimentation, and we should be wary – whether on the basis of observable practice or theoretical perspective – of disabling Congress from articulating and federalizing privacy norms. Moreover, even from the perspective of competitive federalism, the arguments for federal regulation of information privacy law are stronger than Professor Schwartz suggests.

AUTHOR. Professor of Law and Notre Dame Presidential Fellow, Notre Dame Law School. I thank A.J. Bellia, Susan Freiwald, Nicole Garnett, John Nagle, and Paul Schwartz for helpful comments, and research librarian Dwight King and law student Jeffery Houin for excellent research assistance.

FEATURE CONTENTS

INTRODUCTION

In early 2007, as mega-retailer TJX began disclosing details of a massive network security breach involving at least 45.7 million credit card accounts,[1] members of Congress introduced an array of bills promising strong and comprehensive federal protection of personal data.[2] Although the 110th Congress failed to adopt any significant data privacy legislation, let alone any deserving the labels "strong" or "comprehensive," data security breaches will keep information privacy issues on federal legislative and regulatory agendas for the foreseeable future.

Paul Schwartz's provocative essay suggests that Congress should not seek to adopt a comprehensive federal information privacy law.[3] The positive case for federalization, he argues, is weak: state-level regulation of data privacy is unlikely to lead to the sort of "race to the bottom" that often justifies federal regulation in other areas, such as environmental law.[4] Moreover, a comprehensive information privacy law brings the danger of "ossification."[5] Particularly if such a law is broadly preemptive of state law efforts, we will lose the benefit of state experimentation with innovative privacy law protections.[6]

Schwartz's ultimate conclusion appears to be a narrow one. He argues that it would be unwise for Congress to impose unitary federal information privacy rules that both block more stringent state law rules and eliminate the sector-specific distinctions that now exist in federal law.[7] Although I agree with that

---

1. *See, e.g.*, Ross Kerber, *Court Filing in TJX Breach Doubles Toll*, BOSTON GLOBE, Oct. 24, 2007, at A1 (noting discrepancy between TJX's estimate that 45.7 million accounts were affected and banks' estimate that 94 million accounts were affected).

2. *See, e.g.*, 153 CONG. REC. S1628 (daily ed. Feb. 6, 2007) (statement of Sen. Leahy). The various bills include the following: Privacy and Cybercrime Enforcement Act of 2007, H.R. 4175, 110th Cong. (2007); Social Security Account Number Protection Act, S. 1208, 110th Cong. (2007); Personal Data Protection Act of 2007, S. 1202, 110th Cong. (2007); Identity Theft Prevention Act, S. 1178, 110th Cong. (2007); Data Security Act of 2007, H.R. 1685, 110th Cong. (2007); Data Accountability and Trust Act, H.R. 958, 110th Cong. (2007); Personal Data Privacy and Security Act of 2007, S. 495, 110th Cong. (2007); and Notification of Risk to Personal Data Act of 2007, S. 239, 110th Cong. (2007).

3. Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 902 (2009).

4. *Id.* at 940.

5. *Id.* at 928.

6. *Id.* at 930.

7. *Id.* at 904 (noting that companies have advocated creation of "a single federal law for the private sector that would impose uniform standards"); *id.* at 930 (expressing concern about a law that would "block new approaches to information privacy in federal and state sectoral laws").

narrow conclusion, it rests on descriptive and theoretical premises that have far broader implications for federal regulation of information privacy. If adoption of a unitary and truly comprehensive privacy statute is (as I would contend) unlikely, then we are left with difficult questions about what the relationship between federal and state law should be and whether there is any role for a non-sector-specific federal approach to information privacy. Because I disagree with some of the descriptive and theoretical points that drive Schwartz's analysis, my views on these questions differ from his in significant ways. In particular, the case for federal regulation of data privacy is stronger than Schwartz suggests, even when federal regulation would preempt state law in favor of a unitary federal standard. In addition, I view carefully crafted minimum privacy standards that cut across sectoral lines as unproblematic, so long as such standards permit stronger sector-specific approaches.

My analysis proceeds as follows. In Part I, I first seek to separate the "vertical" and "horizontal" strands of Schwartz's claims—that is, respectively, those arguments focusing on the federal-state balance in information privacy regulation and those arguments focusing on the putative scope of a federal statute in relation to sectoral federal privacy laws. I then briefly discuss the horizontal issues to identify and put to one side my narrow disagreement with Schwartz's approach on these questions.

Parts II through IV focus on the vertical dimensions of information privacy law and explore the key premises, explicit and implicit, upon which Schwartz's opposition to a federal information privacy law rests. I begin in Part II with the descriptive claims. Schwartz views states as "especially important laboratories for innovations in information privacy law,"[8] and that view supports his normative claim that Congress should not adopt a broadly preemptive information privacy law.[9] While I agree with much of his descriptive account, I suggest that it may overstate the role of states as engines of experimentation and change. I then turn in Part III to theories about the proper allocation of regulatory authority between state and federal authorities. Like many scholars who consider federalism questions in other areas of the law, Schwartz seems sympathetic to theories of competitive federalism. Such theories assume that allowing states and localities to compete for citizens' loyalty by experimenting with different policy approaches will generate better regulatory outcomes. This approach and other closely related efficiency-based approaches to allocating regulatory authority are widespread in existing federalism scholarship. Even if we accept these efficiency-based perspectives, however, the case for

8. *Id.* at 916.

9. *See id.* at 930 (noting the benefits of experimentation).

federalization of information privacy law is stronger than Schwartz suggests. Finally, in Part IV, I move beyond the efficiency-based perspectives. Such perspectives, I argue, cannot explain or justify a number of federal information privacy statutes that are better understood as efforts to articulate and federalize privacy expectations. We should not lightly disable the federal government from playing that role.

I. THE VERTICAL AND HORIZONTAL DIMENSIONS OF INFORMATION PRIVACY REGULATION

Schwartz argues that it would be a "mistake" for the United States to adopt "a comprehensive or omnibus federal privacy law for the private sector."[10] Parsing this claim proves more difficult than it first appears, for there are at least three categories of arguments that one opposing such a privacy law might raise. First, one might claim that any regulatory intervention—state or federal—is unnecessary or even counterproductive in light of the possibilities for market-based responses to privacy and security breaches.[11] Schwartz does not appear to make this claim, and indeed in other contexts has expressed skepticism about the adequacy of market responses to data privacy threats.[12] Second, one might focus on the vertical aspects of federal information privacy regulation. One might accept the need for action by legislatures or regulatory agencies but conclude that state regulation is preferable to federal regulation; or one might argue that even though federal intervention itself may be appropriate, such regulation becomes problematic if it broadly preempts state law. Schwartz focuses heavily on these vertical dimensions of information privacy law. Although he specifically opposes a comprehensive and strongly preemptive federal statute, some of his arguments call into question federal regulations that are not strongly preemptive of state approaches and federal regulations that target specific sectors.[13]

Third, one might focus on the horizontal features of federal regulation—that is, the interplay of any federal information privacy law with other

10. *Id.* at 904.

11. *See, e.g.*, Richard A. Epstein & Thomas P. Brown, *Cybersecurity in the Payment Card Industry*, 75 U. CHI. L. REV. 203 (2008) (arguing that regulators should not preempt efforts of private actors to distribute losses arising from payment card fraud).

12. *See, e.g.*, Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913, 927-28 (2007) (noting that companies may not take adequate data security precautions because they fail to fully bear the costs of data breaches or precisely calibrate the costs and benefits of investing in data security).

13. *See infra* notes 101-104 and accompanying text.

sector-specific federal rules. One might argue that a comprehensive approach to regulating the collection, storage, and use of data across varied industries is inappropriate, even if sector-specific deviations from those rules survive. Or one could argue that a comprehensive approach is not generally problematic, but becomes so if it displaces sector-specific rules. Here, Schwartz appears to be unenthusiastic about any form of comprehensive regulation,[14] but especially opposes regulation that displaces existing sectoral laws.[15]

In my view, Schwartz's claims about the vertical dimensions of information privacy offer the most significant challenge to current and future regulations. Federalism issues are often overlooked in debates over what the privacy law landscape should look like. I devote most of the remainder of this Essay to these issues. Before turning to them, however, I note my overall agreement with much of Schwartz's discussion of the horizontal dimensions of information privacy regulation, as well as a narrow point of disagreement.

I agree with Schwartz that a horizontally preemptive statute—that is, one that eliminates any sector-specific privacy approaches—would be problematic (although the possibility of such a statute being adopted seems rather remote). First, this approach fails to acknowledge that information privacy interests vary depending on the type of information at issue. Citizens have different interests in shielding information depending on how sensitive it is: one has a different interest in protecting information about one's health than one has in protecting information about one's shoe purchases. Second, as discussed in Part III, at least in theory one of the benefits of having multiple regulatory regimes—whether by state or by sector—is that it permits experimentation with various regulatory options. Passage of a horizontally preemptive statute does not eliminate the opportunity for sectoral experimentation, because the obstacles to a subsequent Congress's enactment of a sector-specific regulation are political rather than structural. Eliminating sector-specific distinctions, however, does cut existing experiments short.

My disagreement relates to the question whether it is appropriate for Congress to adopt any baseline federal information privacy protections while preserving sectoral protections that exceed the baseline, or to adopt protections where there are gaps in sector-specific protection. Schwartz acknowledges the possibility of such baseline or interstitial regulation and considers some of its advantages, but he fears that adopting a federal baseline violates a principle of

14. Schwartz, *supra* note 3, at 928 (noting that "the case for and against a federal omnibus law proves close").

15. *Id.* at 930.

"regulatory parsimony."[16] Schwartz writes approvingly of Congress's caution in information privacy regulation in the 1970s, when Congress opted not to enact "a broad regulation of information use that would include the private and public sectors in one fell swoop."[17] To this objection about regulatory parsimony we might also add another objection that Schwartz raises against regulations that are both comprehensive and strongly preemptive—that such regulations will lead to "ossification."[18] Schwartz fears that broad federal data privacy legislation would be unamendable. The law's broad scope might make it less likely that Congress would want to revisit it and unravel the compromises it may reflect, even in response to significant changes in technology.

I do not understand Schwartz's regulatory parsimony principle simply to reflect skepticism about the appropriateness of governmental rather than market-based responses to information privacy problems. Rather, I understand it to reflect a preference for a nuanced rather than one-size-fits-all approach. Of course, the Federal Trade Commission (FTC) already has made a substantial move down the path of baseline regulation in critically important areas of information privacy, including the creation of data security standards, through use of its authority to regulate unfair trade practices.[19] One could reasonably argue that congressional attention to this question would be preferable to the FTC's broad interpretation of its authority. And baseline or interstitial regulation, whether by statutory or administrative action, is not inconsistent with more nuanced sector-specific regulation. On the merits, moreover, substantial consolidation in information privacy regulation would be a welcome development. As Schwartz acknowledges, technological convergence itself provides a compelling reason for consolidation.[20] More generally, information privacy law is replete with distinctions that are formal rather than functional. To take one example, consider the Video Privacy Protection Act of 1988 (VPPA), which prohibits one who rents, sells, or delivers "prerecorded video cassette tapes or similar audio visual materials" from disclosing information on what materials a customer has acquired.[21] A different statute, the Cable Communications Policy Act of 1984, governs a cable operator's disclosure of cable viewing records—records that are functionally similar to

16. *Id.* at 913, 928.

17. *Id.* at 913.

18. *Id.* at 928.

19. *See infra* notes 79-80 and accompanying text.

20. Schwartz, *supra* note 3, at 923-24.

21. 18 U.S.C. § 2710 (2000).

those covered by the VPPA.[22] The extent to which the VPPA covers information on what video content a user views at sites such as YouTube is already controversial.[23] And it is unclear how, if at all, the VPPA might apply to a third party such as TiVo, which does not provide video content but which has access to some of a subscriber's recording and viewing information by virtue of the services associated with use of its digital video recorder. Consider also the disparate statutory protection of wire communications in the Wiretap Act and of electronic communications in the Electronic Communications Privacy Act of 1986 (ECPA) amendments to that statute,[24] and the disparate statutory protection of electronic communications in transit and electronic communications in storage.[25]

---

22. 47 U.S.C. § 551(c) (2000 & Supp. V 2005) (prohibiting cable operators from disclosing "personally identifiable information concerning any subscriber," subject to certain exceptions).

23. *See* Viacom Int'l Inc. v. YouTube, Inc., No. 07-CV-2103, 2008 WL 2627388, at *5 (S.D.N.Y. July 2, 2008). In this case, Viacom sought to compel YouTube and its parent corporation, Google, to disclose information about the YouTube service, including information from YouTube's "logging" database. That database contained information on how often particular videos were viewed, as well as the unique login IDs of the users who watched them and the Internet protocol (IP) addresses of the users' computers. YouTube and Google claimed that the VPPA barred them from disclosing the information, but the court dismissed the VPPA's applicability. The court may have misread the statute to cover only video tapes. *See id.* at *5 n.5. The court also characterized the privacy claims as "speculative," in part because the login IDs are pseudonymous and IP addresses, without more information, cannot identify specific users. *Id.* at *5. The parties later reached an agreement allowing YouTube to mask user information with anonymous but unique codes before disclosing the relevant records to Viacom. *See* Viacom Int'l Inc. v. YouTube, Inc., No. 07-CV-2103 (S.D.N.Y. July 17, 2008) (stipulation regarding July 1, 2008 opinion and order).

24. *Compare, e.g.*, 18 U.S.C.A. § 2516(1) (2000 & West Supp. 2008) (enumerating specific federal felonies and requiring approval of high-level Justice Department officials for authorization of order intercepting wire communications), *with* 18 U.S.C. § 2516(3) (2000) (omitting such requirements for authorization of an order intercepting electronic communications). Additionally, see 18 U.S.C. §§ 2515, 2518(10) (2000), which bar the use in evidence of wire communications, but not electronic communications, obtained in violation of the Wiretap Act or an order issued under it. For further discussion, see Patricia L. Bellia, *Surveillance Law Through Cyberlaw's Lens*, 72 GEO. WASH. L. REV. 1375, 1392-93 (2004).

25. For example, for government officials to acquire electronic communications in transit in connection with a criminal investigation, they must satisfy the Wiretap Act's stringent requirements. *See* 18 U.S.C. § 2518. They can compel the production of electronic communications from a third-party service provider on a lesser showing. *See* 18 U.S.C. § 2703 (2000 & Supp. V 2005). For discussion of these different requirements, see Patricia L. Bellia, *The Memory Gap in Surveillance Law*, 75 U. CHI. L. REV. 137, 153-59 (2007). For an argument that the acquisition of stored communications should be subject to stringent requirements akin to those in the Wiretap Act, see Susan Freiwald, *First Principles of*

As for ossification, I do not view that phenomenon as being unique to broad federal statutes. ECPA, for example, proved remarkably resistant to amendment until after the September 11 attacks, despite the fact that it is sector-specific.[26] In any event, the possibility of ossification provides a reason to ensure, as a matter of institutional design, that ossification will be less likely, not necessarily a reason to abandon a comprehensive approach. The need for a legislature to revisit a statute may depend on the mechanisms the statute provides for the law to develop. To take an example from the surveillance statutes, the inclusion of a statutory suppression mechanism in the Wiretap Act[27] has led to vastly greater development of the law under that statute than under the Stored Communications Act, which lacks a statutory suppression mechanism.[28] Similarly, a statute creating private rights of action may allow for greater development than one that does not.

In short, while I agree with Schwartz that a federal statute that not only provides baseline privacy protections but that also eliminates existing sector-specific protections would be unwise, I am less worried about the baseline or interstitial approach merely because it is broad. Such a law may be problematic from the perspective of federalism, but not from the perspective of scope. To examine this question from another angle, I am not sure that Schwartz would oppose a baseline *state* statute on the ground that its broad scope would induce ossification. If I am right, then we can narrow our focus to the vertical issues that Schwartz's essay ably raises.

II. STATE-FEDERAL DYNAMICS IN INFORMATION PRIVACY LAW

I first consider Schwartz's descriptive account of the relationship between state and federal information privacy regulations. Although I do not fully explore the rich detail of the state-federal mix here, it is important to probe a claim that is at the heart of Schwartz's account: that states are privacy "innovators." As discussed in the next Part, theories of competitive federalism

---

Communications Privacy, 2007 STAN. TECH. L. REV. 3, http://stlr.stanford.edu/pdf/freiwald-first-principles.pdf.

26. *See, e.g.*, Patricia L. Bellia, Institutional Design in Communications Surveillance Law (Oct. 1, 2008) (unpublished manuscript, on file with author).

27. 18 U.S.C. § 2518(10)(a) (2000).

28. *See id.* § 2708 (providing that "[t]he remedies and sanctions described in this chapter," which do not include a suppression remedy, "are the only judicial remedies and sanctions for nonconstitutional violations of this chapter"); *see also* Orin S. Kerr, *Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law*, 54 HASTINGS L.J. 805 (2003).

assume that leaving states free to regulate information privacy will generate a market for regulation in which states experiment with various policies in order to satisfy citizens' preferences.[29] Evidence of state innovation in privacy law might buttress that normative approach and also demonstrate the high costs of a strongly preemptive statute.

The mere existence of a range of state regulations, however, is not enough to show the kind or degree of innovation necessary to support that claim, because focusing on state *outputs* tends to minimize the important judicial, federal, and other *inputs* that can profoundly influence state law. Judicial rulings, for example, can provide the impetus for federal and state statutory changes by exposing areas of underregulation. One example of this phenomenon, discussed in greater detail below, involves the adoption of federal and then state wiretapping laws in the wake of the Supreme Court's Fourth Amendment rulings in *Berger v. New York*[30] and *Katz v. United States*.[31] Although state wiretapping laws are widespread, the reactive nature of much of this legislation detracts from the image of states as innovators.

In other words, if we are to assess the role of states as privacy law innovators, we must consider the interplay of state and federal developments, and we must consider both legislative and nonlegislative fora. To facilitate that analysis, I discuss three regulatory patterns illustrating the dynamic relationship between state and federal law. I focus in particular on the adoption of various federal information privacy laws and consider the actions of states leading up to or following the federal action.[32] I do not purport to analyze systematically the reality of states as privacy law innovators. My analysis, for instance, leaves to one side both state activity that does not prompt or follow corresponding federal activity, as well as privacy gaps that neither state law nor federal law has filled. But simply probing the dynamic relationship between

---

29. *See infra* notes 89-91 and accompanying text.

30. 388 U.S. 41 (1967).

31. 389 U.S. 347 (1967).

32. A few caveats are appropriate. First, I do not claim that all federal and state privacy regulation fits within the three patterns I identify. The patterns I identify are simply useful to illustrate the interplay between state and federal law. Second, I do not contend that we can or should view all portions of any given federal statute as illustrating a single pathway to federalization. Different segments of the same statute may reflect different responses to state law. Third, in categorizing privacy statutes, I seek to describe the effect of congressional action rather than what motivates it. That is, my argument is not intended to demonstrate that we can attribute to Congress as a whole, or to any particular legislator, the motivation to follow a particular privacy path. I do use standard tools of statutory interpretation (including some forms of legislative history) to discern the meaning of particular statutes, but I make no specific claims about congressional motivation.

state and federal privacy laws, as I do here, reveals that federal nonregulation might not necessarily result in the kind and degree of generative state privacy experimentation that Schwartz appears to contemplate. I will return to the patterns discussed here when I take up the affirmative case for federalization—and its limits.

A. Quasi-Constitutional Provisions

In casting states as information privacy innovators, Schwartz focuses mainly on legislative accomplishments, such as state statutes requiring notification of data security breaches, statutes restricting the use of social security numbers, and so on.[33] Privacy law's story, of course, begins with the common law. Samuel Warren and Louis Brandeis's influential article, *The Right to Privacy*,[34] spawned hundreds of state law cases recognizing privacy torts that scholar William Prosser subsequently classified into four branches—intrusion upon seclusion, public disclosure of private facts, false light, and appropriation of name or likeness.[35] Schwartz's focus on legislative developments acknowledges that courts have not readily adapted any of these branches to activities involving the collection, storage, or transfer of personal data.

Focusing exclusively on legislative developments, however, risks overstating the role of states, for it minimizes the role of courts in generating legislative change. Courts can expose constitutional, statutory, and common law privacy gaps and identify the constitutional standards to which legislation must conform. Indeed, some of our most significant federal information privacy statutes attempt to implement or recalibrate the balance that courts have arrived at in applying the Fourth Amendment to the conduct of government agents. When a court applies the Fourth Amendment to government conduct affecting information privacy, the Supreme Court's broad interpretation of the Commerce Clause gives Congress considerable leeway to respond by implementing or ratcheting up the judicial standard.[36] In other

33. Schwartz, *supra* note 3, at 917.

34. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

35. *See* RESTATEMENT (SECOND) OF TORTS §§ 652B-E (1977); William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 389 (1960).

36. *See, e.g.*, Gonzales v. Raich, 545 U.S. 1, 22 (2005) (framing the relevant inquiry as whether Congress has a "rational basis" for concluding that the regulated activities, taken in the aggregate, affect interstate commerce). In many cases, Congress has explicitly linked the scope of particular privacy statutes to interstate commerce. *See, e.g.*, 18 U.S.C. § 2510(1) (2000) (defining "wire communication"); *id.* § 2510(12) (defining "electronic

words, the Commerce Clause permits Congress to reinforce a judicial decision that Congress believes adequately protects privacy or to overcome a decision that Congress believes does not, and thereby create a quasi-constitutional form of criminal procedure.

The Federal Wiretap Act,[37] for example, responded to a pair of cases the Supreme Court decided in 1967. In *Katz*, the Court held that government agents' use of an electronic device to overhear a suspect's conversation is a "search" for purposes of the Fourth Amendment and therefore cannot proceed without a warrant.[38] During the preceding term, in *Berger*, the Court had invalidated a New York statute authorizing wiretapping by local law enforcement officials.[39] Taken together, *Katz* and *Berger* rendered government officials' use of wiretapping and eavesdropping techniques illegal unless officials satisfied the Fourth Amendment requirements the Court identified. The Wiretap Act was Congress's response; Congress set by statute the hurdles for investigators to clear to obtain a judicial order authorizing electronic surveillance.[40]

---

communication"); *id.* § 2710(a)(4) (defining "video tape service provider"); 42 U.S.C. § 2000aa(a) (regulating officials' seizure of work product materials held by one who intends to disseminate a publication "in or affecting interstate or foreign commerce"). Even where it does not, Congress can conclude that personal data is itself a subject of interstate commerce. *See* Reno v. Condon, 528 U.S. 141, 148 (2000) (accepting the claim that "the personal, identifying information that the [Driver's Privacy Protection Act] regulates is a thing in interstate commerce, and that the sale or release of that information in interstate commerce is therefore a proper subject of congressional regulation" (internal quotation marks omitted)). For an unusually candid acknowledgment of the limits of Congress's power to protect privacy using its Commerce Clause powers, see S. REP. NO. 90-1097, at 92 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2180, which noted that "the extent of the constitutional power of Congress to prohibit [the interception of oral communications] is less clear than in the case of interception of wire communications."

37. Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, tit. III, 82 Stat. 197, 211 (codified as amended at 18 U.S.C.A. §§ 2510-2522 (West 2000 & Supp. 2008)).

38. 389 U.S. 347 (1967).

39. 388 U.S. 41 (1967).

40. *See* 18 U.S.C. § 2518 (2000). The Foreign Intelligence Surveillance Act of 1978 (FISA), Pub. L. No. 95-511 (codified as amended at 50 U.S.C.A. §§ 1801-1811 (West 2003 & Supp. 2008)), provides a second example of Congress's attempt to translate the Supreme Court's reasoning into an information privacy statute. In 1972, in *United States v. U.S. District Court*, 407 U.S. 297 (1972), the Supreme Court held that the Fourth Amendment barred government agents from conducting warrantless electronic surveillance to safeguard national security, at least when the target was a domestic group lacking any connection to a foreign power. *Id.* at 320. Although the Court found the agents' conduct unconstitutional, the Court acknowledged that Congress could tailor specific statutory requirements to the peculiarities of national security surveillance without violating the Fourth Amendment. *Id.* at 322-24. Congress never took up the Supreme Court's invitation to create distinct

In addition to implementing judicial rulings that limit official conduct, Congress can itself limit official conduct when courts do not. Consider, for example, Congress's response to a series of Supreme Court decisions in the late 1970s. In *United States v. Miller*, the Court ruled that, for purposes of the Fourth Amendment, a depositor has no expectation of privacy in information and documents he furnishes to his bank to complete his financial transactions, and that government agents therefore could compel production of such items without a warrant.[41] In the Right to Financial Privacy Act of 1978, Congress generally required that federal agents either use a warrant to gather information from a target's financial institution or provide the target with notice and an opportunity to contest a subpoena.[42] Similarly, after the Court concluded in the 1978 case of *Zurcher v. Stanford Daily* that the Fourth and First Amendments permitted government agents to search the offices of a student newspaper for evidence of criminal activity, even though there was no evidence that members of the newspaper staff were themselves involved in that activity,[43] Congress passed the Privacy Protection Act of 1980 (PPA).[44] The statute prohibited government agents, federal and state alike, from searching or seizing work product and other documentary materials held by a person "reasonably believed to have a purpose to disseminate" information to the public, unless the agents could establish probable cause to believe that the publisher committed the criminal offense to which the materials relate.[45] In effect, the PPA requires government agents to obtain documentary material by subpoena, which the publisher can challenge in court and with which the publisher can comply without government officials intruding on the premises. Finally, after the Court ruled in *Smith v. Maryland* that government officials' use of a "pen register" to detect the number of an outgoing call was not a search under the Fourth Amendment,[46] Congress set minimum standards for officials' use of those and similar devices. More specifically, a portion of the Electronic Communications Privacy Act of 1986 (ECPA) imposed procedural standards for the use of pen registers as well as "trap and trace devices" (which are devices to detect the number of an incoming call), requiring officials to

standards for national security surveillance of domestic targets, but it adopted in FISA a special framework for surveillance of foreign powers or agents of foreign powers.

41. 425 U.S. 435 (1976).

42. 12 U.S.C. § 3402.

43. 436 U.S. 547 (1978).

44. 42 U.S.C. § 2000aa.

45. *Id.*

46. 442 U.S. 735 (1979).

certify to a judge that the information in question is relevant to an ongoing investigation.[47]

In short, a number of federal information privacy statutes directly respond to judicial rulings on the contours of permissible official conduct.[48] It is perhaps unsurprising to find the federal government imposing standards for federal agents' conduct, for that seems a uniquely federal role. Several of the statutes described above, however, set standards for state officials' conduct, both where courts have concluded that the Constitution itself imposes some minimum requirements (as in the case of wiretapping and eavesdropping) and where courts have concluded that the Constitution imposes no such requirements (as in the case of the Privacy Protection Act and the pen register and trap and trace device statute). After Congress acted, a number of states adopted their own laws regulating similar conduct. In design and detail, many of the statutes are strikingly similar to the federal laws. Consider, for example, the number of state laws closely patterned after the Federal Wiretap Act[49] and

---

47. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, §§ 301-302, 100 Stat. 1848, 1868-72 (codified as amended at 18 U.S.C. §§ 3121-3127 (2000 & Supp. V 2005)).

48. There is, of course, much more to some of these statutes: in both the Wiretap Act and the pen register and trap and trace statute, Congress also regulated private parties' access to the information in question. *See, e.g.*, 18 U.S.C. § 2511(1) (2000); 18 U.S.C. § 3121 (2000 & Supp. V 2005). The portions of the statutes restricting official conduct, however, essentially implement or substitute for constitutional requirements.

49. *See, e.g.*, ARIZ. REV. STAT. ANN. §§ 13-3001, -3005 to -3012 (2001 & Supp. 2008); DEL. CODE ANN. tit. 11, §§ 2401-2412 (2007); D.C. CODE ANN. §§ 23-541 to -556 (LexisNexis 2001 & Supp. 2008); FLA. STAT. ANN. §§ 934.02-.10 (West 2006); HAW. REV. STAT. ANN. §§ 803-41 to -49 (LexisNexis 2007); IDAHO CODE ANN. §§ 18-6701 to -6709 (2004); IOWA CODE ANN. §§ 808B.1-.8 (West 2003); KAN. STAT. ANN. §§ 22-2514 to -2518 (2007); LA. REV. STAT. ANN. §§ 15:1301-:1312.1 (West 2005 & Supp. 2008); MD. CODE ANN., CTS. & JUD. PROC. §§ 10-401 to -411 (LexisNexis 2006); MASS. ANN. LAWS ch. 272, § 99 (LexisNexis 2000 & Supp. 2008); MINN. STAT. ANN. §§ 626A.01-.20 (West 2003 & Supp. 2009); MISS. CODE ANN. §§ 41-29-501 to -536 (2005); MO. ANN. STAT. §§ 542.400-.422 (West 2002 & Supp. 2008); NEB. REV. STAT. §§ 86-271 to -295 (2008); NEV. REV. STAT. ANN. §§ 179.410-.515, 200.610-.690 (LexisNexis 2006); N.H. REV. STAT. ANN. §§ 570-A:1 to :11 (LexisNexis 2003 & Supp. 2008); N.J. STAT. ANN. §§ 2A:156A-1 to -26 (West 1985 & Supp. 2008); N.D. CENT. CODE §§ 12.1-15-02 to -04 (1997); OHIO REV. CODE ANN. §§ 2933.51-.66 (LexisNexis 2006); OKLA. STAT. ANN. tit. 13, §§ 176.1-.14 (West 2002 & Supp. 2008); OR. REV. STAT. §§ 133.721-.739 (2007); 18 PA. CONS. STAT. §§ 5701-5728 (2000 & Supp. 2008); R.I. GEN. LAWS §§ 12-5.1-1 to -16 (2002); S.C. CODE ANN. §§ 17-30-15 to -145 (Supp. 2007); TENN. CODE ANN. §§ 39-13-601 to -603, 40-6-301 to -310 (2003); TEX. PENAL CODE ANN. § 16.02 (Vernon Supp. 2008); TEX. CODE CRIM. PROC. ANN. art. 18.20 (Vernon Supp. 2008); UTAH CODE ANN. §§ 77-23a-1 to -11 (2008); VA. CODE ANN. §§ 19.2-61 to -70 (2008); W. VA. CODE §§ 62-1D-2 to -16 (2005 & Supp. 2008); WIS. STAT. ANN. §§ 968.27-.33 (West 2007); WYO. STAT. ANN. §§ 7-3-701 to -712 (2007).

the pen register and trap and trace device statute.[50] It is difficult to see such statutes as reflecting significant state innovation and leadership in information privacy law. That is not to say that the state statutes are identical to one another or to the federal statutes. In authorizing electronic surveillance activities by their own officials, for example, states had the opportunity to choose for which offenses these investigative tools should be available, and in fact there is a fair amount of variety among the state statutes on this question.[51] Overall, however, the examples above tend to demonstrate the importance of federal leadership in information privacy problems, with the adoption of a federal statute creating the momentum for adoption of state law. Because it is hard to imagine what the state legislative landscape would have looked like in the absence of the significant judicial and federal changes, it is hard to see state statutes adopted in the wake of the federal statutes as important examples of independent state innovation.

B. "Federal-First" Regulatory Responses

If the conduct of government officials is not at issue, neither the Federal Constitution nor most state constitutions provide the backdrop for regulation of data privacy.[52] Instead, that backdrop includes private arrangements (backed by the threat of judicial enforcement) and common law rules. When these mechanisms are inadequate to address particular information privacy

---

50. *See, e.g.*, ARIZ. REV. STAT. ANN. § 13-3017; DEL. CODE ANN. tit. 11, §§ 2430-2434; FLA. STAT. ANN. §§ 934.31-.34; HAW. REV. STAT. ANN. §§ 803-44.5 to -44.6; IDAHO CODE ANN. §§ 18-6720 to -6722; IOWA CODE ANN. §§ 808B.10-.12; KAN. STAT. ANN. §§ 22-2525 to -2527; LA. REV. STAT. ANN. §§ 15:1313-:1316; MD. CODE ANN., CTS. & JUD. PROC. §§ 10-401 to -05; MINN. STAT. ANN. §§ 626A.35-.37; MONT. CODE ANN. §§ 46-4-402 to -403 (2007); NEB. REV. STAT. §§ 86-298 to -2100 (2008); N.H. REV. STAT. ANN. §§ 570-B:2 to :5; N.Y. CRIM. PROC. LAW §§ 705.00-.35 (McKinney 2008); N.D. CENT. CODE §§ 29-29.3-02 to -05 (1997); OHIO REV. CODE ANN. §§ 2933.76-.77; OKLA. STAT. ANN. tit. 13, §§ 177.1-.5; R.I. GEN. LAWS §§ 12-5.2-1 to -5; S.C. CODE ANN. §§ 17-29-10 to -50 (2003); S.D. CODIFIED LAWS §§ 23A-35A-22 to -30 (2004); UTAH CODE ANN. §§ 77-23a-13 to -15; VA. CODE ANN. §§ 19.2-70.1 to -70.2; W. VA. CODE § 62-1D-10; WYO. STAT. ANN. §§ 7-3-801 to -806.

51. For examples of the various approaches taken in the state wiretapping and eavesdropping statutes, see FLA. STAT. ANN. § 934.07; HAW. REV. STAT. ANN. § 803-44; IOWA CODE ANN. § 808B.3; KAN. STAT. ANN. § 22-2515; LA. REV. STAT. ANN. § 15:1308; MD. CODE ANN., CTS. & JUD. PROC. § 10-406; MINN. STAT. ANN. § 626A.05; OKLA. STAT. ANN. tit. 13, § 176.7; OR. REV. STAT. § 133.724; 18 PA. CONS. STAT. § 5708; S.C. CODE ANN. § 17-30-70; UTAH CODE ANN. § 77-23a-8; VA. CODE ANN. § 19.2-66; W. VA. CODE § 62-1D-8 (2005); WIS. STAT. ANN. § 968.28; and WYO. STAT. ANN. § 7-3-705.

52. But see the California Constitution, which does contain an explicit right of privacy. CAL. CONST. art. 1, § 1.

problems, the response can presumably begin at the state level or at the federal level. Here I consider "federal-first responses," through which Congress regulates information privacy in the absence of substantial state legislative or regulatory activity.

Portions of ECPA provide an example. The first title of ECPA grafted protections against the interception of electronic communications onto the Federal Wiretap Act, which until then had covered only the interception of wire and oral communications.[53] The second title of ECPA, often referred to as the Stored Communications Act (SCA), established independent protections for stored wire and electronic communications.[54] Both segments filled information privacy law gaps that state law largely did not address. The hearings preceding adoption of ECPA brought to light concerns that existing law—state and federal—did not adequately protect electronic communications, as well as concerns that the successful development and adoption of new communications technologies depended upon public perceptions that electronic communications were secure from private and governmental interception.[55] Although numerous states had adopted or updated state wiretap acts in the wake of the Federal Wiretap Act's passage, many of the statutes, like the Wiretap Act, covered the use of a device to intercept wire and oral communications. By 1986, Congress had already adopted a federal anti-hacking statute,[56] but participants in the debates over ECPA did not perceive it or its emerging state analogues to adequately cover the interception of electronic communications or the acquisition of stored electronic communications from a service provider's system.[57] Congress passed ECPA before states could fill the perceived gaps.

---

53. *See* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, § 101, 100 Stat. 1848, 1848-53.

54. *See id.* § 201, 100 Stat. at 1860, 1860-73.

55. *See, e.g.*, S. REP. NO. 99-541, at 5 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3559; H.R. REP. NO. 99-647, at 18-19 (1986).

56. Congress passed the initial federal anti-hacking statute in 1984. *See* Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, 98 Stat. 2190. As initially enacted, the statute protected only a narrow range of computers. *Id.* § 2102, 98 Stat. at 2190-91 (covering computers containing national security information, computers containing financial data, and computers operated by or on behalf of the government).

57. Congress considered a major amendment to the federal anti-hacking statute at the same time that it considered ECPA, and the relationship between the statutes was a subject of concern in the hearings on ECPA. *Electronic Communication Privacy: Hearing on S. 1667 Before the Subcomm. on Patents, Copyrights and Trademarks of the S. Comm. on the Judiciary*, 99th Cong. 94-95 (1987) [hereinafter *Senate ECPA Hearing*]; *Electronic Communications Privacy Act: Hearings on H.R. 3378 Before the Subcomm. on Courts, Civil Liberties, and the*

There are other significant examples of Congress stepping into perceived information privacy gaps. When Congress considered whether to repeal the Glass-Steagall Act provisions precluding banks from offering investment, commercial banking, and insurance services, consumer groups urged that allowing financial institutions to combine these functions would expose customers' personal information. Although state law presumably could have responded to this problem, at least in part, the Gramm-Leach-Bliley package tied the Glass-Steagall Act's repeal to new protections regarding the sharing of information by financial institutions.[58] Congress has also acted in the face of certain highly publicized privacy breaches. In 1988, for example, Congress passed the VPPA, which limited government and private access to video rental and purchase records.[59] The Senate Report accompanying the proposed legislation focused on media coverage of the video rental records of Judge Robert H. Bork during his failed confirmation hearings.[60] Similarly, the Driver's Privacy Protection Act of 1994[61] (DPPA) responded to a series of high-profile incidents in which state agencies' release of drivers' personal information led to crime or harassment. Most notable among these incidents was the murder of actress Rebecca Schaeffer, whose stalker had obtained her address through a private investigator's request to the California Department of Motor Vehicles.[62]

As in the case of the quasi-constitutional statutes, when Congress fills a perceived information privacy gap before states do so and Congress does not preempt state legislation, states can adopt their own laws regulating similar

Administration of Justice of the H. Comm. on the Judiciary, 99th Cong. 22-23, 90 (1986). ECPA evolved to protect communications in connection with the transmission process rather than general hacking activities. *See, e.g.*, *Senate ECPA Hearing*, *supra*, app. 156 & n.* (summarizing changes between versions of ECPA and indicating that ECPA was intended to cover storage of communications in connection with the communications process, so as to eliminate overlap with hacking statutes).

58. Gramm-Leach-Bliley Act, Pub. L. No. 106-102, tit. V, 113 Stat. 1338 (1999) (codified as amended at 15 U.S.C. §§ 6801-09 (2000 & Supp. V 2005)).

59. Video Privacy Protection Act of 1988, Pub. L. No. 100-618, 102 Stat. 3195 (codified at 18 U.S.C. § 2710).

60. S. REP. NO. 100-599, at 5 (1988) (noting that a Washington newspaper published a profile of Judge Bork based on the titles of the 146 movies his family rented from a local video store).

61. Driver's Privacy Protection Act of 1994, Pub. L. No. 103-322, § 300,001, 108 Stat. 1796, 2099 (codified as amended at 18 U.S.C. § 2721).

62. *See, e.g.*, 140 CONG. REC. 7924 (1994) (statement of Rep. Moran); 139 CONG. REC. 29,466 (1993) (statement of Sen. Boxer).

conduct. States, for example, have adopted statutes analogous to the SCA,[63] the VPPA,[64] and the DPPA,[65] as well as statutes mirroring some aspects of the Gramm-Leach-Bliley Act.[66] Again, however, the existence of these state statutes does not necessarily provide strong evidence of independent state innovation, for in many instances the state statutes appear to stem from the momentum of and share the design of the federal rules. To be sure, there is some diversity among state approaches. In my view, what is striking is that so many of the state statutes share a large federal statutory core, subtracting only one or two options from the federal menu.

To take the example of the DPPA, some states have adopted statutes that tweak the federal rules so as to provide greater privacy protection. The federal statute outlines fourteen categories of permitted disclosures by state motor vehicle departments of personally identifiable information from motor vehicle

---

63. *See, e.g.*, DEL. CODE ANN. tit. 11, §§ 2421-2427 (2007); FLA. STAT. ANN. § 934.21 (West 2006); HAW. REV. STAT. ANN. §§ 803-47.5 to -47.8 (LexisNexis 2007); MD. CODE ANN., CTS. & JUD. PROC. §§ 10-4A-01 to -08 (LexisNexis 2007); MINN. STAT. ANN. §§ 626A.26-.34 (West 2003); N.J. STAT. ANN. §§ 2A:156A-27 to -34 (West 1985 & Supp. 2008); TEX. PENAL CODE ANN. § 16.04 (Vernon 2003).

64. For statutes tracking the structure of the VPPA, see MINN. STAT. ANN. §§ 325I.01-325I.03 (West 2004); N.Y. GEN. BUS. LAW §§ 671-675 (McKinney 1996); and TENN. CODE ANN. §§ 47-18-2201 to -2205 (2001). *See also* MASS. GEN. LAWS ANN. ch. 93, § 106 (West 2006) (tying lawfulness of release of certain information to categories in the Federal VPPA). A handful of states considered video rental privacy bills at the same time as Congress and enacted those measures slightly before Congress did. *See* Act To Add Section 1799.3 to the Civil Code, Relative to Business Records, Sept. 20, 1988, ch. 1050, 1988 Cal. Stat. 3405 (codified at CAL. CIV. CODE ANN. § 1799.3 (West 1998)); Act Concerning Video Tape Distributors, May 27, 1988, ch. 631, 1988 Md. Laws 4221 (codified at MD. CODE ANN., CRIM. LAW § 3-907 (LexisNexis 2002)); Act Relating to Criminal Offenses—Unlawful Dissemination of Records, May 27, 1988, ch. 94, 1988 R.I. Pub. Laws 255 (codified at R.I. GEN. LAWS § 11-18-32 (2002)).

65. For statutes tracking the structure of the DPPA (albeit with some important differences in coverage discussed below), see ALASKA STAT. § 28.10.505 (2008); ARIZ. REV. STAT. ANN. § 28-455 (Supp. 2008); CONN. GEN. STAT. ANN. § 14.10 (West Supp. 2008); DEL. CODE ANN. tit. 21, § 305 (2005); FLA. STAT. ANN. § 119.0712(2) (West 2008); IND. CODE ANN. § 9-14-3.5-1 to -15 (LexisNexis 2004 & Supp. 2008); MD. CODE ANN., STATE. GOV'T § 10-616(p) (LexisNexis Supp. 2008); MO. ANN. STAT. § 32.091 (West Supp. 2009); MONT. CODE ANN. §§ 61-11-501 to -516 (2007); NEB. REV. STAT. § 60-2901 to -2912 (2004); N.H. REV. STAT. ANN. § 260:14 (LexisNexis Supp. 2008); N.J. STAT. ANN. §§ 39:2-3.3 to -3.7 (West 2002 & Supp. 2008); N.C. GEN. STAT. § 20-43.1 (2007); N.D. CENT. CODE § 39-33-01 to -10 (2008); OHIO REV. CODE ANN. § 4501.27 (LexisNexis 2008); OKLA. STAT. ANN. tit. 4, § 1109 (West 2003); OR. REV. STAT. §§ 802.175-.191 (2007); R.I. GEN. LAWS § 27-49-3.1 (2008); S.D. CODIFIED LAWS § 32-5-143 to -151 (2004); TENN. CODE ANN. §§ 55-15-107 to -25-102 (2004 & Supp. 2007); and TEX. TRANSP. CODE ANN. §§ 730.001-.016 (Vernon 1999 & Supp. 2008).

66. *See, e.g.*, CAL. FIN. CODE §§ 4050-4060 (West 1999 & Supp. 2009).

records.[67] By permitting but not requiring such disclosures, the DPPA essentially leaves in state hands the choice whether to allow all categories of disclosure that the federal law permits. Some state statutes track the DPPA but omit or alter a category. The Federal DPPA, for example, allows state motor vehicle departments to disclose personal information "[f]or use by any licensed private investigative agency or licensed security service for any purpose permitted under this subsection."[68] Some states disallow or limit disclosures to private investigators.[69] Other states disallow or narrow disclosures that federal law conditions on the express consent of the subject of the motor vehicle record.[70] Similarly, there are state statutes pursuing the general approach of the VPPA but omitting certain categories of disclosures that federal law would permit. While the federal statute permits law enforcement officials to compel production of video rental records after obtaining a court order issued upon a showing of relevance to any criminal investigation, the Tennessee analogue requires a warrant or an actual criminal proceeding.[71] Unlike the federal statute, the New York analogue does not permit disclosure of customer names and addresses for marketing purposes.[72]

In short, although there are a wide array of state statutes protecting the privacy of video rental records and motor vehicle records, many of these statutes are prompted by and retain the basic structure of federal law, while reflecting some narrowing of the options that federal law leaves open. On one view, the statutes demonstrate some degree of state experimentation; on another, they demonstrate a surprising lack of it. Moreover, although diversity in state approaches can be valuable in and of itself, the competitive federalism model seems to expect something more—that such diversity will in turn generate further changes in state and federal law. Assessing whether state law has had this generative power would require an empirical assessment that is beyond the scope of this Essay. For now, the point is simply that the mere existence of varied state approaches layered over a federal approach does not,

---

67. 18 U.S.C. § 2721(b) (2000).

68. *Id.* § 2721(b)(8).

69. *See* ALASKA STAT. § 28.10.505(d)(2); CONN. GEN. STAT. § 14.10(f)(2); N.J. STAT. ANN. § 39:2-3.4(c)(3).

70. *Compare, e.g.*, 18 U.S.C. § 2721(b)(11), (12), *with* N.C. GEN. STAT. § 20-43.1(b) (disallowing disclosures permitted by § 2721(b)(11)), *and* MONT. CODE ANN. § 61-11-509 (omitting authority to disclose information for bulk distribution), *and* N.J. STAT. ANN. § 39:2-3.4(c)(11) (limiting disclosures for marketing).

71. TENN. CODE ANN. § 47-18-2204(b)(1)(B), (C) (2001).

72. *Compare* 18 U.S.C. § 2710(b)(2), *with* N.Y. GEN. BUS. LAW § 673 (McKinney 1996 & Supp. 2009).

without more, provide strong evidence of state privacy innovation unprompted by federal initiatives.

C. Federal Provisions Reacting to State Regulatory Activities

A third pattern involves the adoption of federal law after substantial state legislative or regulatory activity has already occurred. In other words, the move away from the default of private arrangements and state common law is first made by the states themselves, and federal action responds to that shift. Although not a traditional privacy statute, the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act) provides one example.[73] By the time Congress passed the statute, many states had adopted statutes restricting spam e-mail or, through state agencies, had applied unfair trade practice laws to deceptive forms of spam.[74] Congress took an approach similar to that of many state regulations, by restricting commercial e-mail sent with the intent to deceive or mislead recipients.[75] Congress included a provision preempting any state regulation "that expressly regulates the use of electronic mail to send commercial messages, except to the extent that [the regulation] prohibits falsity or deception in any portion of a commercial electronic mail message or information attached thereto."[76] More recently, in the wake of highly publicized security breaches, states have imposed notification requirements on companies that experience a data security breach. California was the first state to adopt such a requirement in 2002,[77] and forty-four states have since followed suit.[78] Although Congress has not yet passed data breach notification requirements, several of the federal bills proposed in the wake of the TJX data spill would do so. There are also signs that the FTC is more aggressively targeting data security breaches, in effect

---

73. Pub. L. No. 108-187, 117 Stat. 2699 (codified at 15 U.S.C. §§ 7701-7713 (Supp. V 2005)). Although the CAN-SPAM Act is not centrally concerned with the collection, storage, and use of personal information, some commentators treat it as a "privacy" statute because receiving spam is in some sense itself an invasion of privacy or because the statute embodies the fair information practice strategy of allowing consumers to opt out in some circumstances.

74. For a summary of state legislation, see SpamLaws.com, State Laws, http://spamlaws.com/state/index.shtml (last visited Feb. 10, 2009).

75. *See* 15 U.S.C. § 7704.

76. *Id.* § 7707(b)(1).

77. *See* CAL. CIV. CODE § 1798.29 (West 1998 & Supp. 2009).

78. *See* National Conference of State Legislatures, State Security Breach Notification Laws, http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm (last visited Dec. 16, 2008).

developing common law data security standards at the federal level.[79] Whether the FTC's action responds to or anticipates state action or reflects concerted shifts in federal policy is unclear.[80]

---

79. The FTC has privacy enforcement authority under a number of specific statutes, including protections concerning financial privacy, *see* 15 U.S.C. § 6805 (2000) (granting the FTC authority to enforce Gramm-Leach-Bliley Act requirements as to financial institutions not subject to the jurisdiction of other federal agencies or state insurance authorities), the privacy of credit information, *see* 15 U.S.C. § 1681s (2000 & Supp. V 2005), and the privacy of personally identifiable information relating to children, *see* 15 U.S.C. §§ 6501-6502 (2000). In other cases, however, the FTC has taken an increasingly broad view of its role under section 5 of the Federal Trade Commission Act, which empowers the FTC to investigate "unfair or deceptive acts or practices in or affecting commerce." 15 U.S.C.A. § 45 (West 1997 & Supp. 2008).

Beginning in the late 1990s, the FTC filed complaints against various companies' privacy practices on the ground that the companies had violated their own privacy policies – for example, by breaching promises not to share personally identifiable information with third parties, *see, e.g.*, Complaint, FTC v. Toysmart.com, LLC, No. 00-11341-RGS, 2003 WL 34016434 (D. Mass. July 21, 2000), *available at* http://www.ftc.gov/os/2000/07/toysmartcomplaint.htm, or by breaching promises to safeguard customers' information, *see, e.g.*, Complaint at 3, *In re* Eli Lilly & Co., No. C-4047, 2001 WL 1712505 (Fed. Trade Comm'n May 8, 2002), *available at* http://www.ftc.gov/os/2002/05/elilillycmp.htm (claiming that Eli Lilly and Co. had represented "that it employs measures and takes steps . . . to maintain and protect the privacy and confidentiality of personal information" but that in fact such representations are false and misleading). The FTC treated breaches of privacy policies as unfair and deceptive trade practices under section 5 of the FTCA.

More recently, however, the FTC has interpreted section 5 as directly obligating companies to safeguard such information, whether or not the company's privacy policy promises that the company will do so. In a complaint involving the TJX data security breach, for example, the FTC claimed that TJX's failure to employ "reasonable and appropriate security measures to protect personal information caused or is likely to cause substantial injury to consumers that is not offset by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers" – the FTC interpretation of unfairness that Congress codified in 1994. *See* Complaint at 3, *In re* The TJX Cos., Inc., No. 072-3055, 2008 WL 903808 (Fed. Trade Comm'n Mar. 27, 2008), *available at* http://www.ftc.gov/os/caselist/0723055/080327complaint.pdf. *Compare id.*, *with* Federal Trade Commission Act Amendments of 1994, § 9, Pub. L. No. 103-312, 108 Stat. 1691, 1695 (codified at 15 U.S.C. § 45(n) (2000)). The FTC did not allege that TJX violated its own policies or that it violated any specific FTC rules; rather, the FTC apparently viewed the failure to protect data as an unfair trade practice in and of itself.

80. The FTC's role in enforcing privacy policies is controversial, and many commentators have argued that the FTC has been and will continue to be ineffective as a privacy regulator. *See, e.g.*, Joel R. Reidenberg, *Privacy Wrongs in Search of Remedies*, 54 HASTINGS L.J. 877 (2003); Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1637-39 (1999). When the FTC first began investigating privacy practices in the late 1990s, some states acted more aggressively under "little FTC Acts" (that is, state statutes paralleling the FTCA). For example, the FTC closed an investigation of DoubleClick without charges, *see* Letter from Joel Winston, Acting Assoc. Dir., Div. of Fin. Practices, Bureau of Consumer

State-level privacy initiatives are likely to have the most influence on the shape of federal law when they fill an information privacy gap rather than following federal action. State laws can provide possible models for federal regulation. When Congress reacts to substantial state regulatory activity rather than itself seeking to fill a privacy gap, however, stronger preemption may be quite tempting. A federal statute can consolidate regulatory gains made by the states by adopting a rule that has proven successful at the state level. If the goal is to mimic a successful state regulatory experience, those involved in the legislative process may perceive strong preemption to be costless, because in theory Congress is adopting the "best" rule from among a range of rules already in operation (and the successful state regulatory experience may have made other states less likely to impose greater standards in any event). In other cases, preemption will be a key component, if not the chief goal, of the legislation, where Congress seeks to smooth out regulatory unevenness among the states.

D. Summary

The discussion above permits some preliminary observations about federal information privacy regulation, theories of competitive federalism, and preemption. First, although it would be foolish to deny that states are quite active in privacy regulation, the volume of state regulation, without more, does not provide strong evidence of competitive federalism at work or of the costs of preemption. In some cases, as with quasi-constitutional provisions regulating official conduct and other cases involving federal-first responses, states simply mimic or expand upon existing federal regulation, and state regulation is largely attributable to the momentum of federal regulation. Second, we should hesitate to generalize about the inappropriateness of strong preemption. In

---

Prot., Federal Trade Comm'n, to Christine Varney, Counsel for DoubleClick Inc. (Jan. 22, 2001), http://www.ftc.gov/os/closings/staff/doubleclick.pdf, whereas a coalition of state attorneys general prompted DoubleClick to change its privacy policies, *see In re* DoubleClick: Agreement Between the Attorneys General of the States of Arizona, California, Connecticut, Massachusetts, Michigan, New Jersey, New Mexico, New York, Vermont, and Washington and DoubleClick Inc. (Aug. 26, 2002), http://www.oag.state.ny.us/media_center/2002/aug/aug26a_02_attach.pdf; Press Release, N.Y. State Att'y Gen., Major Online Advertiser Agrees to Privacy Standards for Online Tracking (Aug. 26, 2002), http://www.oag.state.ny.us/media_center/2002/aug/aug26a_02.html. Despite the fact that state attorneys general have aggressively targeted companies' privacy practices in the past, there is little evidence that states are interpreting their own laws governing unfair and deceptive practices to cover inadequate security standards. Accordingly, one could argue that the FTC's approach does reflect a concerted shift in federal policy. On the other hand, the FTC may be acting in anticipation of aggressive state approaches.

some cases, strong preemption may simply be the natural outgrowth of the process of innovation, as Congress seeks to temper perceived overregulation by states. In other cases, when states follow Congress's lead in implementing judicial decisions or responding to perceived privacy gaps, strong preemption in theory forecloses states from experimenting with more stringent privacy rules. Whether foreclosing state experimentation is good or bad policy, however, depends not only on the lost benefits of state experimentation—benefits that may be limited when states simply build upon judicial or federal responses to perceived underregulation—but also on what might be gained by a unitary federal approach. The benefits of a unitary approach, if any, will be context-specific, depending, for example, on the extent to which one state's policy interferes with another's. The point for now is simply that we cannot move from the fact of state regulation to a normative prescription for state regulation. The existence of substantial state regulation of information privacy does not confirm that competitive federalism is thriving—nor does the fact that states are often followers of federal action suggest that it is not.

III. INFORMATION PRIVACY REGULATION AND FEDERALISM THEORY

I now consider more fully Schwartz's normative claims about the relative roles of the states and the federal government in regulating information privacy. Schwartz's view that it would be a mistake for Congress to adopt a comprehensive information privacy regulation is not simply a reaction to the possible breadth of such a statute. At bottom, that view rests upon the premise that leaving the lion's share of information privacy regulation in state hands is preferable to federal intervention. Nor can a preference for state regulation simply relate to the predicted substance of state versus federal regulations; as Schwartz recognizes, we cannot predict that different levels of government will consistently adopt positions that favor or disfavor privacy interests.[81]

What, then, are the more general principles about the allocation of state and federal regulatory authority that should shape information privacy regulation? Other areas of the law, perhaps most notably environmental law, feature robust scholarly debates over the appropriate mix of federal, state, and local regulation. Although Schwartz does not fully engage this literature, he appears to be sympathetic to at least one of its dominant premises—the presumption of "decentralization," which holds that regulation should occur at the state level unless a compelling basis for federal intervention exists. Scholars

81. Schwartz, *supra* note 3, at 938 ("One cannot be confident in a given policy result reached by reliance on a federal as opposed to state regulatory process, or vice versa.").

in other areas of the law tend to evaluate justifications for deviating from this presumption through the lens of efficiency.[82] Schwartz does not explicitly adopt this approach, but the concept of competitive federalism on which he relies links back to this literature. As I will argue, even under efficiency-based approaches, there are strong justifications for federal intervention in information privacy regulation. My purpose in considering information privacy regulation through the lens of efficiency is not to embrace this methodology to the exclusion of others; as discussed in the next Part, efficiency-based approaches cannot explain or justify a range of federal information privacy statutes. Rather, it is to establish that even from this limiting perspective, the predicates for federal intervention are met.

Scholars defend the presumption of decentralization that provides the starting point for many discussions of federalism on a number of overlapping grounds. Many scholars argue that the Constitution itself encodes such a presumption[83] or that such a presumption can be derived from the principle of "subsidiarity"—that is, the principle that regulation should occur at the lowest level of government capable of appropriately addressing a particular problem—and the values of autonomy and self-determination that it supports.[84] Others link such a presumption to regulatory efficiency, by suggesting that state experimentation with innovative regulatory approaches will lead to better outcomes,[85] or that the presumption helps to ensure an equivalence between the scope of a problem and the jurisdiction of the institution addressing it.[86] I leave the first two grounds to one side, except to say that, in my view, they cannot fully justify a presumption of decentralization. The enumeration of federal powers and reservation of powers to the states, without more, does not help to identify the circumstances in which Congress should forestall use of the

---

82. For examples of this approach in environmental law scholarship, see Jonathan H. Adler, *Jurisdictional Mismatch in Environmental Federalism*, 14 N.Y.U. ENVTL. L.J. 130, 134-35 (2005); Richard L. Revesz, *The Race to the Bottom and Federal Environmental Regulation: A Response to Critics*, 82 MINN. L. REV. 535, 536-38 (1997); and Richard B. Stewart, *Pyramids of Sacrifice? Problems of Federalism in Mandating State Implementation of National Environmental Policy*, 86 YALE L.J. 1196, 1211-22 (1977). *See also* C. Boyden Gray, *Regulation and Federalism*, 1 YALE J. ON REG. 93, 93 (1983) (describing the presumption of decentralization as a "basic precept" of the Reagan Administration's approach to regulation).

83. *See* Adler, *supra* note 82, at 134; Revesz, *supra* note 82, at 536.

84. *See* Adler, *supra* note 82, at 134; *see also* George A. Bermann, *Taking Subsidiarity Seriously: Federalism in the European Community and the United States*, 94 COLUM. L. REV. 331, 338-39 (1994) (discussing the connection between the presumption of decentralization and subsidiarity).

85. *See infra* text accompanying notes 89-91.

86. *See infra* text accompanying notes 93-96.

powers it does possess. Similarly, the principle of subsidiarity, at least as developed in Catholic social thought,[87] does not automatically presume the superiority of decisionmaking at a lower level of a hierarchy. Rather, it suggests that regulation at the lower level is preferable *if* such regulation has the capacity to accomplish the desired objectives,[88] which thus requires some metric for deciding whether state regulation is adequate.

The efficiency-related justifications figure prominently in the federalism literature in other areas of the law, and it is worth exploring them in greater detail. Theories of competitive federalism hold that, as a matter of policy, if not as a matter of constitutional law, decentralized decisionmaking generally will yield better decisions.[89] Theorists view state and local governments as competitors in the market for a mobile citizenry. If mobile citizens can choose the jurisdiction that best suits their needs, state and local governments will have incentives to satisfy citizens' preferences.[90] The Supreme Court's classic statement of the values of federalism in *Gregory v. Ashcroft* focuses in part on the benefits of market responsiveness:

> The federalist structure of joint sovereigns preserves to the people numerous advantages. It assures a decentralized government that will be more sensitive to the diverse needs of a heterogeneous society; it increases opportunity for citizen involvement in democratic processes; it allows for more innovation and experimentation in government; and it makes government more responsive by putting the States in

87. *See, e.g.*, Pope Leo XIII, *Rerum Novarum: Encyclical of Pope Leo XIII on Capital and Labor* (May 15, 1891), *in* 2 THE PAPAL ENCYCLICALS 1878-1903, at 241, 250-51 para. 36 (Claudia Carlen ed., 1990); Pope Pius XI, *Quadragesimo Anno: Encyclical of Pope Pius XI on Reconstruction of the Social Order* (May 15, 1931), *in* 3 THE PAPAL ENCYCLICALS 1903-1939, *supra*, at 428 paras. 79-80.

88. *See* sources cited *supra* note 87; *see also* JOHN FINNIS, NATURAL LAW AND NATURAL RIGHTS 147 (1980).

89. *See, e.g.*, Michael W. McConnell, *Federalism: Evaluating the Founders' Design*, 54 U. CHI. L. REV. 1484, 1499 (1987); Deborah Jones Merritt, *The Guarantee Clause and State Autonomy: Federalism for a Third Century*, 88 COLUM. L. REV. 1, 9 (1988). This argument builds upon Justice Brandeis's observation that a federal system permits states to "try novel social and economic experiments without risk to the rest of the country." New State Ice Co. v. Liebmann, 285 U.S. 262, 311 (1932) (Brandeis, J., dissenting).

90. The classic treatment is Charles M. Tiebout, *A Pure Theory of Local Expenditures*, 64 J. POL. ECON. 416 (1956). For more recent discussions, see, for example, McConnell, *supra* note 89, at 1498-99; and Barry R. Weingast, *The Economic Role of Political Institutions: Market-Preserving Federalism and Economic Development*, 11 J.L. ECON. & ORG. 1, 5-6 (1995).

competition for a mobile citizenry.[91]

As noted earlier, Schwartz extensively discusses the perceived virtues of state experimentation in privacy regulation; his descriptive claims serve in part to buttress a normative claim about the benefits of competitive federalism.[92]

Theories about competitive federalism represent only one of the efficiency-related justifications for a presumption of decentralization. Claims about the systemic benefits of state experimentation necessarily depend on the view that, individually, states can adequately address particular regulatory challenges. Of course, that will not always be the case. Many scholars approaching federalism questions from the perspective of efficiency would allocate regulatory authority by determining which level of government has a jurisdictional reach that most closely matches the scope of the problem to be addressed, on the theory that efficient regulation occurs only when the regulating entity can fully internalize the costs and benefits of its policies.[93] In environmental law scholarship, then, debates over when federal intervention should occur are often debates over application of this matching principle, with scholars identifying the circumstances in which states can and cannot internalize the costs or benefits of a particular policy. In addition, some scholars who advocate a matching principle to guide the allocation of regulatory responsibilities recognize that federal regulation may be appropriate for some purely intrastate problems, as where competition for mobile industries[94] or special interest distortions[95] will lead to overly lax standards, although these theoretical bases for recognizing a failure in the market for regulation are more controversial.[96]

---

91. 501 U.S. 452, 458 (1991).

92. *See* Schwartz, *supra* note 3, at 916-18, 929-30.

93. *See, e.g.*, HENRY N. BUTLER & JONATHAN R. MACEY, USING FEDERALISM TO IMPROVE ENVIRONMENTAL POLICY 1-3 (1996); Adler, *supra* note 82, at 133; Henry N. Butler & Jonathan R. Macey, *Externalities and the Matching Principle: The Case for Reallocating Environmental Regulatory Authority*, 14 YALE L. & POL'Y REV. 23, 25 (1996); Daniel C. Esty, *Revitalizing Environmental Federalism*, 95 MICH. L. REV. 570, 587 (1996).

94. *See, e.g.*, Stewart, *supra* note 82, at 1212 ("Given the mobility of industry and commerce, any individual state or community may rationally decline unilaterally to adopt high environmental standards that entail substantial costs for industry and obstacles to economic development for fear that the resulting environmental gains will be more than offset by movement of capital to other areas with lower standards.").

95. *See* Esty, *supra* note 93, at 597-99.

96. The debate over whether competition for mobile industries causes a "race to the bottom" is particularly robust. *Compare, e.g.*, Revesz, *supra* note 82, *and* Richard L. Revesz, *Rehabilitating Interstate Competition: Rethinking the "Race-to-the-Bottom" Rationale for Federal Environmental Regulation*, 67 N.Y.U. L. REV. 1210 (1992), *with* Kirsten H. Engel, *State*

Although the matching principle will usually point toward regulation at the subfederal level, sometimes it will point to federal intervention. One example involves the existence of a physical externality, such as air or water pollution, that spills over from one jurisdiction to another.[97] The state in which the polluting factory is located does not fully experience the costs of the pollution or the benefits of limiting it. Because local decisionmakers cannot fully internalize the benefits of regulatory action and the costs of regulatory inaction, their regulations will be too lax.

How do these principles apply to information privacy regulation? The consequences of an information privacy breach obviously do not correspond to particular physical jurisdictions, and one could argue that data "spills" are analogous to the sort of cross-border pollution that justifies federal regulation. The fact that states can regulate data processors' transactions with their own citizens is likely to temper the problem of underregulation, since states will internalize the benefits of their policies. Such regulation creates a different problem, however—that of inconsistent regulations generating compliance burdens for companies. It is possible for companies to respond by customizing digital databases of personal information. Whether federal intervention to eliminate such inconsistencies is justified depends on the significance of the costs of customization—including not only that of coding the personal information of clients in particular states so that use of the data is consistent with the applicable legal rules, but also that of determining which clients reside in which states.

Moreover, an externality can exist whenever a state's regulation projects significantly beyond its borders, regardless of whether the regulation directly conflicts with another state's regulation. Consider, for example, the status of California's motor vehicle emissions standards before Congress gave the federal government regulatory authority over air pollution and preempted all state standards but California's.[98] If California adopts the nation's highest

---

Environmental Standard-Setting: Is There a "Race" and Is It "to-the-Bottom"?, 48 HASTINGS L.J. 271 (1997), *and* Esty, *supra* note 93, *and* Joshua D. Sarnoff, *The Continuing Imperative (but Only from a National Perspective) for Federal Environmental Protection*, 7 DUKE ENVTL. L. & POL'Y F. 225 (1997). On the public choice issues, see Richard L. Revesz, *Federalism and Environmental Regulation: A Public Choice Analysis*, 115 HARV. L. REV. 553 (2001).

97. *See* Stewart, *supra* note 82, at 1215.

98. *See* Air Quality Act of 1967, Pub. L. No. 90-148, § 208, 81 Stat. 485, 499 (codified as amended at 42 U.S.C. § 7543(b)(1) (2000)); Motor Vehicle Air Pollution Control Act, Pub. L. No. 89-272, § 202(a), 79 Stat. 992, 992 (1965). The 1965 statute set a regulatory floor for emissions standards; the 1967 statute gave federal standards preemptive effect over states that had not yet adopted standards. More specifically, the preemption provision allowed any state that adopted emission control standards before March 30, 1966, to seek a waiver of

emissions standards, automobile manufacturers that wish to serve the California market are forced to produce a car that is compliant with California's standards. If manufacturers cannot cheaply produce different cars for different markets, then California's standard becomes a national standard. Because the manufacturer passes the costs of meeting higher emissions standards to all customers nationwide, California residents bear only a fraction of the actual cost of the regulation. California's Online Privacy Protection Act, which took effect in 2004, presents a similar phenomenon. The statute requires website operators that collect personally identifiable information from California residents to "conspicuously post" online privacy policies identifying the categories of information the operator collects and the third parties with whom it will share the information.[99] Any website seeking to serve a national market will meet the general requirements of the California standard. The standard becomes a national, though not a federally adopted, standard, and it may create externalities even if no other state adopts a conflicting rule. The effect of California's regulation—if not the very goal—is to raise the website's costs. Customers nationwide bear these costs, regardless of whether non-California residents value privacy at the same level as California residents do.

Of course, there is an important distinction between California's emissions standards and its online privacy requirements. The former has a federal imprimatur that the latter lacks. By permitting California to maintain higher-than-federal motor vehicle emissions standards,[100] Congress effectively accepted that others value clean air as highly as Californians do. In the absence of federal regulation, the signals that Californians' privacy preferences should predominate are much weaker. At most, those signals consist of the absence of a congressional response displacing those rules, and possibly courts' failure to displace the regulation under the dormant Commerce Clause.

To be clear, my argument is not that regulation of privacy policies must be taken up at the federal level. Congress may conclude that California's standards are perfectly adequate as a national standard, or that they are so weak as to reflect already widespread best practices among website operators and therefore impose minimal compliance costs. My argument is simply that the nationwide projection of California's regulation provides a sound theoretical basis for federal involvement even from an efficiency-based perspective.

---

preemption and impose more stringent standards. 42 U.S.C. § 7543(b)(1). California was the only state that met this criterion. *See, e.g.*, Motor & Equip. Mfrs. Ass'n v. EPA, 627 F.2d 1095, 1100 n.1 (D.C. Cir. 1979). The 1977 amendments to the Clean Air Act permitted other states to impose California standards as well. *See* 42 U.S.C. § 7507.

99. Online Privacy Protection Act of 2003, CAL. BUS. & PROF. CODE §§ 22575-22579 (West 2008).

100. *See* 42 U.S.C. § 7543(b)(1); *supra* note 98.

IV. THE FEDERAL ROLE IN INFORMATION PRIVACY REGULATION

The discussion in Part III of efficiency-based approaches both supplies one missing link in Schwartz's argument and reveals some tension in it. The missing link in Schwartz's argument relates to his willingness to accept a range of information privacy regulation despite the federalism concerns he raises with a comprehensive and strongly preemptive statute. Schwartz has no difficulty with sector-specific federal statutes that set a floor and permit stricter state regulations. Although he objects to a comprehensive regulation that would set a unitary federal standard and preclude stricter state regulations—a phenomenon that others (perhaps inaptly) term ceiling preemption[101]—he is apparently willing to accept some sector-specific regulations that set unitary federal standards. And although he is lukewarm about interstitial or baseline federal regulation, his objections relate to horizontal issues of scope rather than vertical issues of federalism.

If the presumption of decentralization is an appropriate analytical starting point, then we must ask what justifies even floor-preemptive sectoral statutes. The jurisdictional mismatches that would otherwise exist with respect to a variety of information privacy problems provide one justification. Were it otherwise, scholars applying a presumption of decentralization would have to call not only for Congress not to enact a comprehensive statute, but also for it to repeal a number of other information privacy laws. Schwartz does not advocate that course.

The tension arises because—from the perspective of competitive federalism that Schwartz appears to embrace—nothing distinguishes a collection of sector-specific laws from a more comprehensive one covering the same ground. As discussed in Part II, for example, it is not the case that a sectoral law typically follows state experimentation while a comprehensive one would precede it. Of course, Schwartz's argument not only distinguishes sectoral laws from comprehensive ones, it also distinguishes floor-preemptive laws from ones that establish unitary federal standards. The theory of competitive federalism he embraces does provide some support for the distinction between

101. Scholars use the term "floor preemption" to refer to the preemption of state regulations weaker than those in the federal statutes: state regulations can exist above the federal floor or not at all. The term "ceiling preemption" would accurately describe a federal statute that set a maximum standard but allowed weaker state regulations. Some scholars use the term ceiling preemption instead to describe a unitary federal standard that displaces all state regulation. *See* William W. Buzbee, *Asymmetrical Regulation: Risk, Preemption, and the Floor/Ceiling Distinction*, 82 N.Y.U. L. REV. 1547, 1549-55 (2007) (distinguishing floor, ceiling, and "unitary federal choice" preemption).

floor-preemptive regulations and unitary federal standards. Floor-preemptive federal statutes permit the continued state experimentation and diversity that the theory envisions[102] and thus build in the possibility of error correction, by allowing states to demonstrate in concrete ways the workability or desirability of higher standards.[103] Imposing a unitary federal standard, in contrast, disables states from demonstrating that federal standards are either too high or too low. But the theory of competitive federalism is incomplete. Even this theory presupposes that diversity and experimentalism must sometimes give way to uniformity or other federal values—the question is in what circumstances. Yet the competitive federalism approach does not help us to identify these circumstances; the theory is premised upon the existence of a market for state and local regulation but it does not supply a means to measure market failure. In other words, the competitive federalism model suggests a preference for floor-preemptive statutes over strongly preemptive ones, but it neither suggests that this preference should be absolute nor identifies when it should not apply. And from the vantage point of the matching principle, floor-preemptive regulations are just as problematic as unitary federal standards. Just as a too-lax state regulation denies cost-bearers beyond the state's boundaries access to a desired public good, a too-strict federal regulation forces those in jurisdictions that might choose to forgo a public good to pay for it.[104]

Information privacy law presents another challenge for the presumption of decentralization and for efficiency-based theories about the allocation of state and federal authority. Even if the matching principle can justify some sector-specific statutes, there are a number of federal statutes that are difficult to justify on such a theory. The VPPA[105] and the DPPA[106] provide good examples.

---

102. Such claims (along with claims about state autonomy) underlie scholars' objections to strong preemption but acceptance of federal regulation in a range of contexts. *See, e.g.*, Erwin Chemerinsky, *Empowering States: The Need To Limit Federal Preemption*, 33 PEPP. L. REV. 69, 74-75 (2005); Robert A. Schapiro, *Justice Stevens's Theory of Interactive Federalism*, 74 FORDHAM L. REV. 2133, 2135 (2006).

103. Of course, floor preemption limits the marketplace for regulation by permitting only one form of experimentation—experimentation "up" from the federal standard. Since a floor preemption provision is most likely to appear in a statute responding to perceived underregulation by states, this limitation is significant: floor preemption allows states to demonstrate that the federal statute, though it responds to underregulation, in fact still underregulates, but it does not allow states to demonstrate the presumptively more likely phenomenon of federal overregulation.

104. *See* Esty, *supra* note 93, at 589 (describing nationally specified drinking-water pollution controls as an example of this sort of "internality").

105. 18 U.S.C. § 2710.

106. *Id.* § 2721.

When Congress passed the VPPA and the DPPA, states presumably could have regulated the brick-and-mortar video rental stores and motor vehicle departments within their jurisdictions without projecting those regulations in a way that affected activities elsewhere. The regulations would have applied to in-state entities and in most cases would have protected state residents.[107]

In my view, the reason that such statutes are difficult to justify under dominant efficiency-based federalism theories is that they reflect a fundamentally different conception of the federal role in privacy regulation. It is useful to ask why any government regulation of information privacy is justified in the first place. There are a number of reasons why market forces will not produce an optimal level of privacy protection. For one thing, many privacy harms are difficult to value. While it may be possible to value material harms flowing from a security breach that ultimately leads to identity theft, it is more difficult to value the sort of dignitary harms that flow from, for example, the release of sensitive medical data or even the release of preference-revealing information.[108] In addition, both in the short term and in the long term, it will be difficult to predict the consequences of releases of personal data. For example, it is difficult for data subjects to predict how their data will be aggregated or how new technologies will allow it to be manipulated in the future.[109]

The fact that efficiency-based approaches to federal regulation cannot explain or justify a range of federal information privacy statutes does not demonstrate that federal regulation of data privacy is a mistake; rather, it signals the importance of statutes, and in particular the importance of federal statutes, in generating as well as recognizing privacy expectations. To take the VPPA as an example, any harms flowing from the release of the video rental records of Judge Bork's family are difficult to quantify, and similar releases will have different impacts on different individuals. The VPPA reflects an effort to acknowledge and federalize a privacy expectation that video rental records are not a matter of public concern. Similarly, portions of a number of the quasi-constitutional statutes described earlier reflect efforts to articulate and federalize privacy expectations. Matters concerning state investigators' access to journalists' work product, for example, could be dealt with by states' regulation of their own officials. But the PPA recognizes and federalizes an

---

107. The matching principle may provide a better justification for the Federal VPPA now than it did before, since brick-and-mortar video rental stores no longer dominate the video rental and video sale markets.

108. *See, e.g.*, James P. Nehf, *Recognizing the Societal Value in Information Privacy*, 78 WASH. L. REV. 1, 62 (2003).

109. *See, e.g.*, *id.* at 64.

expectation that procedures less intrusive than a search warrant are appropriate, not only for federal officials, but for state officials as well.[110]

Of course, states can and often do seek to perform this same generative role. California appears to take pride in its leadership role on numerous privacy issues. As the analysis in Part II showed, however, there are a number of cases in which federal leadership was crucial to the development of privacy law. Both in the case of quasi-constitutional statutes and in the case of "federal-first" responses to privacy law gaps, we see federal leadership in information privacy laws even where efficiency-based perspectives would suggest that it is inappropriate. When such statutes are not accompanied by strong preemption, there seem to be few risks to them from the perspective of federalism. In theory, they simply place the federal government itself in the marketplace for regulation and allow states to adopt alternative policies. It is possible that even without strong preemption, diverse state offerings will not follow in the wake of the federal statute—that even without preemption, the existence of the federal statute will make diversity in state regulation less likely than it otherwise would have been. Whether the absence of state variation from the federal standard is a problem depends on whether that lack of variation reflects the fact that the federal approach is a good one, or that the federal statute itself induces a failure in the marketplace for regulation.

More is needed, of course, to justify strongly preemptive federal statutes, even when they serve the function of articulating and federalizing privacy norms. The risk here is that diverse state approaches will be foreclosed, thus eliminating one possible avenue for "errors" in the federal approach to become apparent. Of course, maintaining sector-specific variation leaves a different avenue open. In my view, although strongly preemptive data privacy statutes should be rare, they will be justified in some cases. Where substantial state regulation precedes federal regulation, the existence of conflicting schemes may justify preemption. Even where a federal statute responds to constitutional underdevelopment or fills a perceived gap before substantial state regulation can occur, preemption may be justified to prevent such conflicts or to displace a law that has national consequences but that has not been subject to the national political process.

CONCLUSION

I find much common ground with Schwartz's views. First, we agree on the value of experimentation in information privacy law. Second, we agree that a

110. 42 U.S.C. § 2000aa.

data privacy law that is vertically and horizontally preemptive—that not only evens out state disparities, but also that removes sector-specific rules—is undesirable. In my view, however, even within an efficiency-based framework—the framework perhaps least likely to support federal intervention—there are justifications for federal action and in some cases even for strong federal preemption. Strong preemption is unproblematic if the resulting regulation strikes the right privacy balance; the real concern is that federal law will be broadly preemptive and will underregulate. I may share that concern, but I do not view it as a concern about federalism or about the comprehensiveness of federal regulation. I am not confident that we can credit state experimentation with privacy successes or that we can blame federalization for its failures.