THE YALE LAW JOURNAL

PAUL M. SCHWARTZ

Preemption and Privacy

ABSTRACT. A broad coalition, including companies formerly opposed to the enactment of privacy statutes, has now formed behind the idea of a national information privacy law. Among the benefits that proponents attribute to such a law is that it would harmonize the U.S. regulatory approach with that of the European Union and possibly minimize international regulatory conflicts about privacy. This Essay argues, however, that it would be a mistake for the United States to enact a comprehensive or omnibus federal privacy law for the private sector that preempts sectoral privacy law. In a sectoral approach, a privacy statute regulates only a specific context of information use. An omnibus federal privacy law would be a dubious proposition because of its impact on experimentation in federal and state sectoral laws, and the consequences of ossification in the statute itself. In contrast to its skepticism about a federal omnibus statute, this Essay views federal sectoral laws as a promising regulatory instrument. The critical question is the optimal nature of a dual federal-state system for information privacy law, and this Essay analyzes three aspects of this topic. First, there are general circumstances under which federal sectoral consolidation of state law can bring benefits. Second, the choice between federal ceilings and floors is far from the only preemptive decision that regulators face. Finally, there are second-best solutions that become important should Congress choose to engage in broad sectoral preemption.

AUTHOR. Professor of Law, University of California, Berkeley, School of Law; Director, Berkeley Center for Law and Technology. For helpful suggestions, I thank Michelle Wilde Anderson, Holly Doremus, Ira Ellman, Daniel Farber, Malcolm Feeley, Robert Gellman, Andrew Guzman, Patrick Hanlon, Kate Heinzelman, Chris Hoofnagle, Ian Kerr, Ira Rubinstein, James Rule, Pamela Samuelson, Jason Schultz, Spiros Simitis, David Sklansky, Daniel Solove, Sarah Song, Stephen Sugarman, and William Treanor.

FEATURE CONTENTS

INTRODUCTION

In March 2007, Bill Gates, Microsoft Chairman, called for the enactment of a comprehensive federal privacy law.[1] His voice became one of many asking Congress to take broad and preemptive action to regulate the collection, storage, and transfer of information across the private sector. A patchwork of information privacy laws now exists in the United States, and it is one with federal and state elements. In the view of Gates and many others, it would be preferable to create a single federal law for the private sector that would impose uniform standards.

A broad coalition, including companies formerly opposed to enactment of privacy statutes, has now formed in support of a national information privacy law. Businesses that have signed on to this policy include Microsoft, Google, eBay, Intel, Oracle, Sun Microsystems, Hewlett-Packard, and Procter & Gamble.[2] The Center for Democracy and Technology, a privacy advocacy group, is coordinating this drive for a nationwide privacy law.[3] Among the benefits that proponents attribute to such a law is that it would harmonize the U.S. regulatory approach with that of the European Union (EU), and possibly minimize international regulatory conflicts about privacy.

This Essay argues, however, that it would be a mistake for the United States to enact a comprehensive or omnibus federal privacy law for the private sector that preempts sectoral privacy law. An omnibus statute establishes regulatory standards for a large field, which can, in many countries, sweep in the entire public and private sectors. In contrast, a sectoral law has jurisdiction over a specific context of information use. As an example, the Video Privacy Protection Act of 1988 establishes rules for the use of video rental information,[4]

---

1. *See* Anne Broache, *Gates Urges Federal Data Privacy Law*, CNET NEWS, Mar. 8, 2007, http://www.news.com/2100-1014_3-6165395.html; Grant Gross, *Microsoft's Bill Gates Wants New Privacy Law*, CIO, Mar. 7, 2007, http://www.cio.com/article/29936/Microsoft_s_Bill_Gates_Wants_New_Privacy_Law. The Microsoft support for a federal privacy law did not begin, however, in 2007, but 2005. A white paper by Brad Smith, Microsoft's General Counsel, provides the most detailed explanation of the company's position. *See* Brad Smith, Senior Vice President, Gen. Counsel, Microsoft Corp., Protecting Consumers and the Marketplace: The Need for Federal Privacy Legislation (Nov. 2005), http://www.microsoft.com/presspass/download/features/2005/PrivacyLegislationCallWP.doc [hereinafter Microsoft White Paper].

2. *See* Riva Richmond, *Business Group Calls for Privacy Law*, WALL ST. J., June 21, 2006, at B2; Erika Morphy, *Tech Giants Form Consumer Privacy Rights Forum*, TECHNEWSWORLD, June 21, 2006, http://www.technewsworld.com/story/51272.html.

3. Morphy, *supra* note 2.

4. *See infra* text accompanying notes 34-39.

and the Fair Credit Reporting Act contains rules for the use of credit reports.[5] The EU has long adopted omnibus information privacy laws; the United States has chosen sectoral laws for its private sector.

This Essay traces the history of information privacy law in Part I, discusses different aspects of a federal omnibus privacy law in Part II, and explores the jurisprudence of sectoral law in Part III. Throughout all Parts, it examines privacy statutes from different sectors in the United States, including laws regulating credit information, financial data, and video rentals. It also considers laws in areas other than privacy, such as environmental and labor law, and looks at comparative examples with a special focus on the EU and Canada.

A comparative element of Part I demonstrates American exceptionalism. From the start, U.S. information privacy law has taken a sectoral approach while European information privacy law has centered on omnibus laws. Yet these differences are best explained by a modest historical account of initial choices, path dependency, and the influence within the EU of a longstanding project to harmonize law within different member states. Omnibus privacy laws cannot be said to be fundamentally incompatible with a federal government.

In Part II, this Essay first considers the case for and against a federal omnibus law that functions only as a gap-filler. Such a statute would provide general standards to be used in areas in which no sectoral law exists, or when there is silence or ambiguity in such a law. The case for such an omnibus law is a close one. This kind of omnibus law proves, however, at best a long shot for enactment. Congress is far more likely to enact an omnibus law with strong preemptive language built around regulatory ceilings. Industry has indicated its support for only such a statute, and it may be in a position to derail any other legislation.[6] Yet such a law would be a dubious proposition due to its impact on experimentation in federal and state sectoral laws, and the consequences of ossification in the statute itself.

In contrast, and as Part III examines, federal sectoral statutes have more promise for information privacy. Sectoral laws are also likely to be a future privacy growth field. Due to a regulatory dynamic that scholars have termed "defensive preemption," businesses often may react to statutory innovations at

---

5. See *infra* text accompanying notes 79-86 for a discussion of the Fair Credit Reporting Act in the context of its amendment by the Fair and Accurate Credit Transactions Act.

6. The Microsoft White Paper indicates the importance of preemption from the perspective of a leading industry participant in this debate. *See* Microsoft White Paper, *supra* note 1, at 4-5. On the presence of numerous veto points for federal legislation in the United States, see ABRAHAM L. NEWMAN, PROTECTORS OF PRIVACY 60 (2008).

the state level by seeking legislation at the federal level.[7] The critical question is the optimal nature of a dual federal-state system for information privacy law, and this Essay concludes by considering three aspects of this question.

First, there are certain general circumstances under which federal sectoral consolidation of state law can bring benefits. These include the avoidance of inconsistent regulations in areas with high costs and little policy payoff, and the establishment of "field definitions" that can lower compliance costs. Second, the choice between federal ceilings and floors is far from the only preemptive decision that regulators face. In particular, the toolkit of privacy federalism should not be limited to the standard concept of "subject matter" preemption. As this Essay argues, privacy federalism can also include ceilings that extend only to the "conduct" regulated and not the entire subject matter of the regulation. As an example of such conduct preemption, I will discuss the Fair and Accurate Credit Transactions Act (FACTA), an important 2003 amendment to the Fair Credit Reporting Act.[8] Another important aspect of the toolkit of privacy federalism is a sharing of enforcement authority among federal and state regulators.

As a final aspect of its consideration of an optimal dual federal-state system for information privacy, this Essay develops a number of second-best solutions. These policy safeguards are important because Congress may engage at times in broader sectoral preemption than is fully merited. In such circumstances, important policy safeguards to consider include a "plus one" strategy, under which Congress allows at least a single state to retain higher standards or to develop standards different from the federal one. Another policy safeguard would be to subject preemption clauses in federal privacy legislation to a ten-year sunset.

I. THE PAST AND PRESENT OF INFORMATION PRIVACY LAW

This Part looks at the emergence of modern information privacy law and its reliance on Fair Information Practices (FIPs). It then traces the development of omnibus and sectoral privacy laws in the United States and analyzes differences in the regulatory paths for information privacy in the United States and the European Union.

7. See *infra* text accompanying notes 166-167 for a discussion of defensive preemption.

8. 15 U.S.C. §§ 1681-1681x (Supp. V 2005).

A. The Roots of Privacy Law

The roots of modern information privacy law are found in state common law, and, specifically, in the tort right of privacy. The genesis of this aspect of privacy law was the publication in 1890 of *The Right to Privacy* by Samuel Warren and Louis Brandeis.[9] Over the course of the twentieth century, and under the helpful influence of William Prosser, author of the relevant sections of the *Restatement (Second) of Torts*, nearly all states have recognized some branches of the tort right of privacy.[10] The process of adoption of the privacy tort was long, but its acceptance is now nearly universal. In 1998, one of the last three holdouts, Minnesota, adopted the tort of invasion of privacy in *Lake v. Wal-Mart Stores, Inc.*[11]

Tort privacy relies on litigation by injured parties and decisionmaking by juries. In Robert Post's seminal formulation, tort privacy is centered on civility norms that maintain and structure communal life.[12] It creates a legal process for negotiation of limits both on the community's access to personal information and on the individual's desire for zones without community scrutiny. Tort privacy's centrality to the law of information privacy has also waned over time. As Post rightfully observes, tort privacy is under stress today for two reasons. First, society's need for accountability has placed new emphasis on the community's access to information.[13] Second, the rise of an "instrumental world of large surveillance organizations" is in basic tension with the underlying logic of civility norms.[14] These large surveillance organizations are only one aspect, albeit an important one, of the information age, which is marked by computerized data processing, innovative means for collecting and sharing personal information, and detailed data trails left by all individuals in their daily lives.

The law's chief reaction to these new developments has not been through tort law, but FIPs.[15] This legal response, which began in the United States and

---

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

10. For a detailed overview of the privacy tort and its development, see DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 77-231 (3d ed. 2009).

11. 582 N.W.2d 231 (Minn. 1998).

12. Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CAL. L. REV. 957 (1989).

13. *See id.* at 1010.

14. *Id.* at 1009. Daniel Solove also has developed proposals to revitalize the tort right of privacy for the information age. *See* DANIEL J. SOLOVE, THE FUTURE OF REPUTATION 113-24 (2007).

15. Paul M. Schwartz, *Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy-Control, and Fair Information Practices*, 2000 WIS. L. REV. 743, 779-81 [hereinafter Schwartz, *Lessig's*

Western Europe in the 1970s, defines obligations for bureaucratic organizations that process personal information. The basic toolkit of FIPs includes the following: (1) limits on information use; (2) limits on data collection, also termed data minimization; (3) limits on disclosure of personal information; (4) collection and use only of information that is accurate, relevant, and up-to-date (data quality principle); (5) notice, access, and correction rights for the individual; (6) the creation of processing systems that the concerned individual can understand (transparent processing systems); and (7) security for personal data.[16]

No single privacy statute contains all these rules in the same fashion or form. As a critical matter, the precise content of the rules will be different based on the context of data processing, the nature of the information collected, and the specific regulatory and organizational environment in which the rules are formulated. Of particular note is the enforcement of FIPs. Depending on the form that FIPs take, the law can include some combination of enforcement and oversight through a private right of action and governmental enforcement. Public entities involved in the process of FIPs include the Federal Trade Commission, various federal regulators of financial institutions, Privacy Act officers, and state attorneys general.

B. Omnibus and Sectoral Privacy Laws: U.S. and European Regulatory Paths

The world's first comprehensive information privacy statute was a state law; the Hessian Parliament enacted this statute in Wiesbaden, Germany, on September 30, 1970.[17] In the accepted terminology, this statute is an "omnibus law." It establishes regulatory standards for a broad area—namely the state and local governments of Hessen. This law was followed by those of other German states, which then influenced the form and content of a federal omnibus law, the Federal German Data Protection Act (Bundesdatenschutzgesetz, or

Code]; *see* Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1614 (1999) (fair information practices "are the building blocks of modern information privacy law").

16. The expression of FIPs in different laws, regulations, and proposals varies in details, sometimes crucially. For my own attempts to summarize these standards, see Schwartz, *Lessig's Code*, *supra* note 15, at 779-80; and Paul M. Schwartz & William M. Treanor, Review Essay, *The New Privacy*, 101 MICH. L. REV. 2163, 2181 (2003).

17. For a masterful account of these developments, see Spiros Simitis, *Einleitung* [*Introduction*], *in* NOMOS KOMMENTAR ZUM BUNDESDATENSCHUTZGESETZ [COMMENTARY ON THE FEDERAL PRIVACY LAW] 61, 62-63 (Spiros Simitis ed., 6th ed. 2006).

BDSG).[18] The term, "data protection," is the standard nomenclature in Europe for information privacy. The 1977 BDSG establishes standards for information processing by public and private entities alike.

The German preference for anchoring data protection law in omnibus privacy statutes is typical of European data protection law. The European Union's adoption in 1995 of the Data Protection Directive has played a key role in this process.[19] The Data Protection Directive envisions that all EU member states follow its requirements by "transposing" them into national law.[20] It leaves the choice of specific legal instruments to each member state, and, at least theoretically, an EU member state could choose to enact a combination of sectoral laws to comply with the Directive.[21] Yet all member states have enacted omnibus laws to transpose the Directive into national law. As Ulrich Dammann notes, the universal favoring of omnibus laws in the EU is unsurprising because the Directive requires a transposition in "its entire range of application."[22] A choice of sectoral laws would place a burden on each member state to enact "a multitude of sectoral regulations."[23] Moreover, each member state was faced with the relatively short deadline of three years that the Directive established for compliance with its standards.[24] Enacting a complete range of sectoral laws in this framework would have been a more than heroic endeavor. Even with omnibus statutes as the chosen method of regulation, only four member states were able to meet the established deadline, and the European Commission even initiated legal action in 1999 due to this

18. Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung (Bundesdatenschutzgesetz) [Federal Data Protection Act], Jan. 27, 1977, BGBl. I at 201, Jan. 14, 2003, BGBl. I at 66, last amended by Gesetz, Aug. 22, 2006, BGBl. I at 1970.

19. Council Directive 95/46, 1995 O.J. (L 281) 31 [hereinafter Data Protection Directive]. For background on the Directive, see Paul M. Schwartz, *European Data Protection Law and Restrictions on International Data Flows*, 80 IOWA L. REV. 471, 480-83 (1995).

20. Data Protection Directive, *supra* note 19, recital 69, at 37.

21. Recital 23 of the Directive leaves the choice of regulatory instruments open to the EU member state. It states, "Whereas Member States are empowered to ensure the implementation of the protection of individuals both by means of a general law on the protection of individuals as regards the processing of personal data and by sectorial laws such as those relating, for example, to statistical institutes." *Id.* recital 23, at 33. This language probably is best read as permitting a combination of omnibus and sectoral laws by member states.

22. Ulrich Dammann, *in* EG-DATENSCHUTZRICHTLINIE: KOMMENTAR [COMMENTARY ON EUROPEAN COMMUNITY DATA PROTECTION DIRECTIVE] 133 (Ulrich Dammann & Spiros Simitis eds., 1997).

23. *Id.*

24. Data Protection Directive, *supra* note 19, art. 32, at 49.

delay in the European Court of Justice against France, Germany, Ireland, Luxemburg, and the Netherlands.[25]

The Directive's requirement that national laws reflect its principles has followed the EU in its eastward expansion. The typical omnibus statute also allows for further specification of regulatory norms through sectoral regulations. For example, the BDSG explicitly provides within its first section that federal sectoral laws take precedent over its provisions.[26] And there has been no shortage of sectoral laws in EU member states.

In the United States, by contrast, FIPs have generally developed through laws that regulate information use exclusively on a sector-by-sector basis. The one partial exception in the United States is the Privacy Act of 1974,[27] which is an omnibus law for the public sector, albeit a narrow one. The Privacy Act only regulates certain kinds of federal agencies, and only certain kinds of information use.[28] This Essay discusses the Privacy Act and its genesis in more detail below.

The divergent evolution of U.S. and European law raises the question of why these legal systems took different paths at the fork in the regulatory road. The puzzle is all the more intriguing because an omnibus bill for the private and public sectors, Senate Bill 3418 (S. 3418), was on the table, however briefly, during the formative period in the United States for information privacy. As originally introduced by Senator Samuel Ervin on May 1, 1974, S. 3418 had a broad jurisdictional sweep. It would have established requirements for "[a]ny Federal agency, State or local government, or any other organization maintaining an information system that includes personal information."[29] Before turning to analysis of the divergent regulatory paths in the United States and Europe, I discuss the road not taken by Congress. S. 3418 can also

25. *See* COMM'N OF THE EUROPEAN CMTYS., FIRST REPORT ON THE IMPLEMENTATION OF THE DATA PROTECTION DIRECTIVE (95/46/EC), at 3 n.1 (2003), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52003DC0265:EN:NOT.

26. "In so far as other legal provisions of the federal government are applicable to personal data . . . such provisions shall take precedence over the provisions of this Act." Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung (Bundesdatenschutzgesetz) [Federal Data Protection Act], Jan. 27, 1977, BGBl. I at 201, last amended by Gesetz, Aug. 22, 2006, BGBl. I at 1046, § 1(3).

27. Privacy Act of 1974, 5 U.S.C. § 552a (2000).

28. Regarding the important limitations of the Privacy Act to only "federal agencies" and its narrow definition of "record," see PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW 92 n.4 (1996); and U.S. DEP'T OF JUSTICE, PRIVACY ACT OVERVIEW, MAY 2004 EDITION: DEFINITIONS (2004), *available at* http://www.usdoj.gov/oip/1974definitions.htm.

29. S. 3418, 93d Cong. § 201(a) (1974).

help illustrate differences between an omnibus bill and a sectoral law, whether in the United States or Europe.

The core of any omnibus bill is a reliance on general clauses; these provisions establish FIPs that are of necessity broadly worded because they cannot be directed to a specific area of information processing. As an initial example, S. 3418 would have required public and private entities to "collect, maintain, use, and disseminate only personal information necessary to accomplish a proper purpose of the organization."[30] In the taxonomy of FIPs, which Section I.A discussed above, this language establishes a disclosure limitation. The bill would also have required organizations to "maintain information in the system with accuracy, completeness, timeliness, and pertinence as necessary to assure fairness in determinations relating to a data subject"[31]—a data quality requirement. As a final example, the bill would have placed restrictions on onward transfers. S. 3418 would prohibit the regulated entities from making a "dissemination" of information without meeting certain requirements, such as "including limitations on access thereto, and . . . determining that the conditions of transfer provide substantial assurance that those requirements and limitations will be observed."[32] In other words, the organization transferring personal data would be obliged to determine that the entity receiving the information followed FIPs, including drawing a line against further transfers.

From a contemporary perspective, one of the most interesting aspects of the proposed bill from 1974 is that it would have conditioned international transfers of information on either subject consent or equivalent protections abroad for the personal data. This proposed requirement of "equivalency" would have exceeded the protections later found in the European Data Protection Directive, which was enacted in 1995 and took effect in 1998. The Directive calls only for "adequate" protection before an organization, public or private, in an EU member state is permitted to transfer personal information to an organization in a third-party nation, such as the United States.[33] Yet, taken as a whole, the general clauses of S. 3418 would have proven similar to those in a typical, modern omnibus European data protection law.

In contrast to these omnibus privacy laws, a sectoral approach is necessarily more narrowly tailored and its terms, by their nature, are more specific. The

30. *Id.* § 201(a)(1).

31. *Id.* § 201(a)(4).

32. *Id.* § 201(a)(5).

33. Data Protection Directive, *supra* note 19, art. 25(1), at 45; *see* Schwartz, *supra* note 19, at 483-88.

U.S. Video Privacy Protection Act of 1988 (VPPA) provides a good example.[34] Its jurisdictional sweep is limited to a "video tape service provider," which is defined in technology-neutral terms.[35] As a result, the law has been easily extended to DVDs. The VPPA contains FIPs, but these are necessarily tailored to the specific context of the "rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials."[36] A description of its customization will provide a useful illustration of the basics of a sectoral information privacy statute.

As an initial example of this tailoring, the VPPA first forbids video tape service providers from disclosing personal information about their customers. It then provides a series of disclosure exceptions centered on the context of video rentals and sales. Thus, it allows disclosures "incident to the ordinary course of business of the video tape service provider."[37] The VPPA also permits disclosure of a limited subset of information, namely of the names and addresses of consumers, but only if an opt-out, or a chance to refuse this disclosure, is first offered to the consumer and the disclosure "does not identify the title, description, or subject matter of any video tapes."[38] A further exception for a different subset of information allows disclosure of the subject matter of videos, but limited to circumstances when "the disclosure is for the exclusive use of marketing goods and services directly to the consumer."[39] The idea here is that consumers will be able to make their wishes known to video providers if they do not wish to receive such marketing information.

I now return to the question of why the United States and Europe have taken divergent paths. The United States continues to lack an omnibus bill that covers the private sector and has, at best, only a relatively limited omnibus bill for part of the public sector. In contrast, as new countries have joined the EU, they have commenced their regulation of information privacy with omnibus laws and have supplemented these statutes with sectoral ones. In my view, the continuing differences can best be explained by a modest account that looks at (1) initial choices followed by path dependency, and (2) the usefulness of omnibus laws in multination systems that wish to harmonize their regulations.

---

34. 18 U.S.C. § 2710 (2000).

35. *Id.* § 2710(a)(4).

36. *Id.*

37. *Id.* § 2710(b)(2)(E).

38. *Id.* § 2710(b)(2)(D)(ii).

39. *Id.*

1. *The U.S. Path*

The original form of S. 3418 was quickly abandoned in favor of a scaled-back statute—the Privacy Act, which only regulates federal agencies. The Senate report on S. 3418 indicates legislators' concerns regarding an overly broad statutory response and their doubts as to whether the private sector even posed much of a threat to privacy beyond credit reporting.[40] Furthermore, Congress had reason at the time to believe that its enactment of the Fair Credit Reporting Act in 1970 had responded to the threats to privacy posed by credit reporting. Priscilla Regan notes that congressmen also wondered during the debate over S. 3418 if an omnibus law for the private sector represented "an impossible task; too many factors had to be taken into account to devise a policy that protected individuals and did not unreasonably burden organizations, while also allowing for government oversight."[41]

Thus, there was considerable caution in the United States in the 1970s against a broad regulation of information use that would include the private and public sectors in one fell swoop. This orientation demonstrates an ideology that I term "regulatory parsimony." As the medical profession expresses the idea, "above all, do no harm."[42] The same perspective is demonstrated in aspects of the Privacy Act of 1974, which, though a kind of omnibus bill for the public sector, is more limited than the typical omnibus EU law for the public sector.

---

40. STAFF OF S. COMM. ON GOV'T OPERATIONS & H. COMM. ON GOV'T OPERATIONS, 94TH CONG., LEGISLATIVE HISTORY OF THE PRIVACY ACT OF 1974, S. 3418 (PUBLIC LAW 93-579): SOURCE BOOK ON PRIVACY 172 (Comm. Print 1976) [hereinafter PRIVACY SOURCEBOOK]. The Senate Committee on Government Operations in its report on the bill observed that it was persuaded to "delay a decision on total application by considerations of time and investigative resources for developing a full hearing record and for drafting the needed complex legislative solution for information abuses in the private sector, beyond those presently covered by the Fair Credit Reporting Act and its pending amendments." *Id.* As Priscilla Regan in her account of this period writes, "A major argument for removing the private sector from the purview of the 1974 legislation was that there was little concrete evidence of abuses in private sector personal information practices." PRISCILLA REGAN, LEGISLATING PRIVACY 78 (1995).

41. REGAN, *supra* note 40, at 78.

42. For a discussion of the origins of this phrase, see Cedric M. Smith, *Origin and Uses of* Primum Non Nocere—*Above All, Do No Harm!*, 45 J. CLINICAL PHARMACOLOGY 371 (2005).

2. *The EU Path*

Multiple factors contributed to the rise of the omnibus model in the EU. For one thing, the EU nations that enacted this kind of information privacy statute viewed preventive action to be more important than the risks of legislating under uncertainty. Instead of the parsimony principle used in the United States, the European nations were acting on a "precautionary principle." As Cass Sunstein, a critic of this concept, has explained, the idea is that it is wiser to act to prevent harm than to require unambiguous evidence to support a regulatory measure.[43]

Regarding the decision to enact omnibus laws from the first era of data protection law in Europe, Spiros Simitis observes that the European lawmaker began with the idea that it was necessary to analyze problems that cut across individual contexts of processing and for which, therefore, a uniform solution expressed in a single statute should be developed.[44] At the same time, the European legislator was also confronted with a considerable challenge because data processing was in its infancy and, therefore, the subject of regulation lacked clear contours.[45]

Despite uncertainty, European lawmakers decided to enact omnibus data protection statutes. Abraham Newman has identified different historically contingent factors that smoothed the path to enactment of data protection statutes in the 1970s in France and Germany,[46] two leaders in information privacy law. For example, Newman shows how French industry's potential opposition to the proposed French data protection legislation was muted by the past nationalization of many affected companies and the centralization of these industries, which minimized the impact of the statute.[47] As a further example, in Germany, a pro-privacy alliance benefited at the critical point in the late 1970s from a "particular alignment of political actors at that time [who] neutralized key barriers to the passage of the policy."[48]

After the initial choice in key European nations to enact omnibus laws, the EU's "harmonizing" project in the field of data protection exercised a strong

---

43. *See* CASS R. SUNSTEIN, LAWS OF FEAR: BEYOND THE PRECAUTIONARY PRINCIPLE 23-25 (2005).

44. Simitis, *supra* note 17, at 68.

45. *Id.*

46. NEWMAN, *supra* note 6, at 60-69.

47. *Id.* at 62. The impact was muted because in France, "[b]anks did not need to exchange intense amounts of information because they had relatively large, national customer pools and access to a wide range of information about those customers." *Id.*

48. *Id.* at 63-64.

influence on other nations. This term of European Community law refers to formal attempts to increase the similarity of legal measures in member states. As Joachim Jacob, the Federal Data Protection Commissioner of Germany, observed, "the European Community is also becoming an information and data community."[49] European integration increased the sharing of data among EU Member Nations and created new demands for personal information. Due to this data sharing throughout the EU, nations with privacy statutes had incentives to advocate equivalent safeguards in all member states. Without such shared levels of protection, previous efforts within individual nations to ensure privacy for their citizens' data would be for naught. The information could easily be transferred to other member states with weaker levels of data protection.

The resulting policy response was the movement to harmonize privacy law throughout the EU. Through the Data Protection Directive, the EU obliged lagging nations within its ranks to protect personal information and to follow the omnibus approach.[50] Moreover, as Newman has observed, the national data protection commissioners, already in place by the 1980s, played an important transgovernmental role in shaping the Directive and expanding privacy protection in Europe.[51] National privacy regulators worked so that their national legislation would be "exported upward regionally."[52] The benefit of an omnibus law for this project is that it provides a relatively limited series of benchmarks and sets them within a single statute. In contrast, an exclusively sectoral approach would lead to far greater complexity in assessing the "equivalency" of data protection for each of the now twenty-seven EU member states.

These differences in the regulatory form of information privacy do not demonstrate that an omnibus system would be incompatible with U.S. federalism. Indeed, omnibus laws are far from incompatible with this principle of governmental organization. Germany—one of the EU leaders in data protection law—has a federal system of government. Outside of the EU, Canada—a country with a federal form of government—enacted an omnibus

49. 14. TÄTIGKEITSBERICHT DES BUNDESBEAUFTRAGTEN FÜR DEN DATENSCHUTZ GEMÄß ABS. 1 DES BUNDESDATENSCHUTZGESETZES [REPORT OF THE COMMISSIONER FOR DATA PROTECTION IN ACCORDANCE WITH ABS. 1 OF THE FEDERAL DATA PROTECTION ACT] 12 (1993).

50. For a discussion of the influence of the European pressure on Margaret Thatcher's Tory government and how it led to the U.K. data protection law, see COLIN J. BENNETT, REGULATING PRIVACY 91 (1992).

51. NEWMAN, *supra* note 6, at 75. For an early discussion of the important role of the data protection commissioners in the EU, see Schwartz, *supra* note 19, at 492-95.

52. NEWMAN, *supra* note 6, at 3, 97-98.

privacy law for the private sector in 2000. Omnibus laws function no better or worse in Germany and Canada than in nonfederal countries, such as France or the United Kingdom. I am also skeptical about the role that cultural differences regarding information privacy in Europe and the United States play with regard to the resulting choices of respective regulatory forms.[53] This comparative topic must be reserved, however, for another day.

C. Recent Federal and State Trends and the Role of Preemption

This Essay's brief history of information privacy in U.S. law has traced its roots from tort law to the start of the modern era. It also has drawn on comparative examples to illustrate U.S. regulatory exceptionalism centered on its lack of an omnibus statute for the private sector. To bring this account up to the present, this Essay returns to the formative decade for information privacy law in the United States—the 1970s. During this period, the U.S. Congress enacted Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (the Wiretap Act), the Fair Credit Reporting Act in 1970, the Family Educational Rights and Privacy Act of 1974, and the Right to Financial Privacy Act of 1978.[54] All of these laws are sector-specific except for the Privacy Act of 1974.

Against this background, the states in the United States have been especially important laboratories for innovations in information privacy law. As noted, the state tradition begins with the recognition of privacy torts throughout the twentieth century. Other innovations followed. Already in 1977, the blue ribbon Privacy Protection Study Commission commented on "the significant increase in State regulatory efforts to protect the interests of the individual in records kept about him . . . [which had] already led a number of

53. James Whitman provides the richest argument for the influences of cultural differences in the differing approaches to information privacy in Europe and the United States. James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1163 (2004). For an interpretation of differences in EU and U.S. information privacy law that stresses the influence of historically contingent events, see NEWMAN, *supra* note 6, at 52-54. For a discussion that stresses both historically contingent factors and cultural ones in shaping European privacy law, see Francesca Bignami, *European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining*, 48 B.C. L. REV. 609, 684-88 (2007).

54. Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3401-3422 (2000); Fair Credit Reporting Act of 1970, 15 U.S.C. §§ 1681a-1681x; Wiretap Act, 18 U.S.C. §§ 2510-2522; Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g.

States to try out innovative protections, particularly in their regulation of private-sector organizations."[55]

State privacy law has started the twenty-first century with renewed activity. The influence of state privacy law has been felt in three ways. First, states have often been the first to identify areas of regulatory significance and to take action. Laws requiring data security breach notifications began with California's Senate Bill 1386 (S.B. 1386) in 2002.[56] Another forty-four states, Puerto Rico, the Virgin Islands, and the District of Columbia have enacted similar statutes.[57] This activity can be contrasted with a lack of any federal response in this policy area. Congress remains unable to agree on a data breach notification bill—a perfect illustration, as noted earlier, of the slow trajectory of federal privacy legislation. As examples from a different area of privacy law, New York and Connecticut are now considering bills that would set limits on companies that track consumers across websites to deliver targeted advertisements based on their behavior.[58]

Second, states have provided innovative approaches. Such innovations are illustrated in the preceding paragraph. As a further example, states have taken legislative action to restrict the use of social security numbers.[59] They also have granted consumers who are victims of identity theft the ability to place freezes on their credit reports, and have obliged businesses to supply these victims with the relevant records of transactions associated with their stolen identity.[60] Moreover, state law preceded federal law in granting identity theft victims a right to free copies of their credit reports.[61]

---

55. PRIVACY PROTECTION STUDY COMM'N, PERSONAL PRIVACY IN AN INFORMATION SOCIETY 491 (1977).

56. CAL. CIV. CODE §§ 1798.29, 1798.82 (West Supp. 2009); *see also* Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913, 915 (2007).

57. Nat'l Conference of State Legislatures, State Security Breach Notification Laws, http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm (last visited Feb. 9, 2009).

58. For the Connecticut bill, see H.B. 5765, Gen. Assem., Feb. Sess. (Conn. 2008). In New York, there have been bills introduced in the Senate and House. *See* Assem. B. 9275, 2007 Leg., 230th Sess. (N.Y. 2007); S. 6441, 2007 Leg., 230th Sess. (N.Y. 2007).

59. National Conference of State Legislatures, Financial Privacy, http://www.ncsl.org/programs/lis/privacy/financeprivacy.htm (last visited Feb. 9, 2009).

60. Consumer Union, State Security Freeze Laws, http://www.consumersunion.org/campaigns/learn_more/003484indiv.html (last visited Dec. 1, 2008). For an example of a state law requirement requiring the disclosure of transaction information to a victim of ID theft, see CAL. PENAL CODE § 530.8 (West Supp. 2009).

61. The applicable states are Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, and Vermont. COLO. REV. STAT. §§ 12-14.3-104 to -105 (2008); GA. CODE. ANN. § 10-1-393(29)(C) (2000); ME. REV. STAT. ANN. tit. 10, §§ 1315-1316 (1997 & Supp. 2008); MD.

Third, states have created an opportunity for simultaneous experiments with different policies. As Malcolm Feeley and Edward Rubin dryly observe of the general idea of states-as-laboratories, these experiments are "desirable, presumably . . . not because of an abiding national commitment to pure research but because the variations may ultimately provide information about a range of alternative government policies and enable the nation to choose the most desirable one."[62] Justice Louis Brandeis famously pointed to this benefit of state regulation and also identified the ability of these "novel social and economic experiments" to take place, at least some of the time, "without risk to the rest of the country."[63] As an illustration of these simultaneous policy solutions, data breach notification statutes vary in their notification "triggers"—that is, the standard under which a company must share information about a data security incident.[64]

As Patricia Bellia correctly observes in her contribution to this Feature, there also have been important federal statutory contributions to this area as well as federal and state judicial inputs. Bellia points to the rich interplay between federal and state regulatory responses and provides a nuanced description of this process.[65] Yet this federal-state dialogue does not refute the notion that states have been significant innovators in this area. At the same time, certain kinds of federal choices are best seen as examples of predetermined (and sometimes useful) inputs to the privacy landscape and not as illustrations of "federal leadership in information privacy problems."[66]

In particular, a host of Bellia's examples drawn from the federal law of surveillance falls into this category of assigned tasks. After all, it is uniquely the

---

CODE ANN., COM. LAW §§ 14-1206 to -1209 (LexisNexis 2005); MASS. ANN. LAWS ch. 93, §§ 58-59 (LexisNexis 2006 & Supp. 2008); N.J. STAT. ANN. §§ 56:11-34 to -37 (West 2001 & Supp. 2008); VT. STAT. ANN. tit. 9, § 2480(b)-(c) (2006). Federal law permits these states to continue to determine how many free credit reports each year that their residents can receive. 15 U.S.C. § 1681t(b)(4) (Supp. V 2005). The result of these federal and state laws is that residents of these states each year can receive one free credit report under federal law and one free credit report under state law, or, in the case of the Georgia statute, two free reports.

62. MALCOLM M. FEELEY & EDWARD RUBIN, FEDERALISM: POLITICAL IDENTITY AND TRAGIC COMPROMISE 26 (2008).

63. New State Ice Co. v. Liebmann, 285 U.S. 262, 311 (1932) (Brandeis, J., dissenting) ("It is one of the happy incidents of the federal system that a single courageous state may, if its citizens choose, serve as a laboratory; and try novel social and economic experiments without risk to the rest of the country.").

64. Schwartz & Janger, *supra* note 56, at 960-70.

65. Patricia L. Bellia, *Federalization in Information Privacy Law*, 118 YALE L.J. 868 (2009).

66. *Id.* at 882.

task of the federal government to develop rules for federal law enforcement. Many of these federal inputs to the privacy landscape in the area of telecommunications surveillance have been notably unsuccessful.[67] Admittedly, the regulatory questions are thorny.[68] For instance, Congress has bungled even a relatively easy task—the creation and maintenance of a system for systematic collection of telecommunications surveillance statistics.[69]

As for preemption, federal statutes have taken varied approaches to state experimentation in the information privacy area. Some federal laws only establish a "floor"—that is, a minimum standard that states may exceed. As an example, consider the Video Privacy Protection Act of 1988 (VPPA), which regulates how video stores collect and share rental information.[70] The VPPA requires states to follow its list of prohibited disclosures but permits additional state safeguards, including reductions to its lists of permitted disclosures of rental information.[71] At least thirteen states have enacted their own video privacy statutes.[72]

The Wiretap Act provides another classic example of a federal privacy "floor." This federal statute permits the recording of telephone conversations by private parties if one party to the conversation has consented.[73] It also allows

---

67. For different critical perspectives, see CHRISTOPHER SLOBOGIN, PRIVACY AT RISK 181 (2007); Susan Freiwald, *Uncertain Privacy: Communication Attributes After the Digital Telephony Act*, 69 S. CAL. L. REV. 949 (1996); Paul M. Schwartz, *Reviving Telecommunications Surveillance Law*, 75 U. CHI. L. REV. 287 (2008); and Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1264, 1292-98 (2004). Although not a critic in general of federal surveillance law, Orin Kerr has expressed strong criticisms of one branch of this law, the Stored Communications Act. Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1233-43 (2004).

68. As a single example, classic statutory assumptions in the Foreign Intelligence Surveillance Act regarding the location of the subject of surveillance have been undercut by modern telecommunications surveillance. *See* Orin S. Kerr, *Updating the Foreign Intelligence Surveillance Act*, 75 U. CHI. L. REV. 225 (2008).

69. Schwartz, *supra* note 67, at 287.

70. 18 U.S.C. § 2710 (2000).

71. *Id.* § 2710(f).

72. *See* CAL. CIV. CODE § 1799.3 (Deering 2005); CONN. GEN. STAT. § 53-450 (2007); DEL. CODE ANN. tit. 11, § 925 (2008); IOWA CODE § 727.11 (2003); LA. REV. STAT. ANN. § 37:1748 (2007); MD. CODE ANN., CRIM. LAW § 3-907 (LexisNexis 2002); MASS. GEN. LAWS ch. 93, § 106 (2006); MICH. COMP. LAWS ANN. §§ 445.1711-.1715 (West 2002); MINN. STAT. ANN. § 325I.02-.03 (West 2004); N.H. REV. STAT. ANN. § 351-A:1 (2008); N.Y. GEN. BUS. LAW §§ 670-675 (McKinney 1996); R.I. GEN. LAWS § 11-18-32 (2002); TENN. CODE ANN. §§ 47-18-2201 to -2205 (2002).

73. 18 U.S.C. § 2511(2).

states to enact more restrictive laws.[74] As the Wiretap Act's legislative history notes, "The proposed provision envisions that States would be free to adopt more restrictive legislation, or no legislation at all, but not less restrictive legislation."[75] Twelve states have enacted "all party" consent statutes.[76] Under these laws, all parties to a phone call must agree to have their telephone call recorded.

Another federal law with a similar approach to state regulation is the Gramm-Leach-Bliley Act (GLB Act), Title V of which regulates the personal information processing of financial institutions. This statute also sets a federal "floor" for privacy.[77] For example, the GLB Act allows states to set higher privacy standards regarding how financial institutions share personal information with outside organizations (termed "non-affiliated entities" in the statute).[78]

Federal privacy legislation has also preempted state legislation with the effect of weakening existing state standards. A statute from 2003, FACTA, which amends the Fair Credit Reporting Act, contains examples of such a downward revision.[79] To be sure, FACTA also has positive aspects. For example, it seeks to improve the accuracy of credit reports. Thus, it requires each national credit bureau to provide upon request a free report to consumers and to provide credit scores to consumers for a fee.[80] FACTA also takes a number of steps to heighten data security. For example, it mandates credit card truncation on receipts provided to consumers—a requirement that courts have found to apply not only to printed receipts in real space, but also to receipts for online purchases that are displayed electronically.[81] FACTA also forbids printing a credit card expiration date on a receipt.[82] Moreover, FACTA institutes strict data disposal rules that reach "any person that maintains or

74. *See* People v. Conklin, 522 P.2d 1049, 1057 (Cal. 1974).

75. S. REP. NO. 1097, at 98 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2187.

76. Reporters Committee for Freedom of the Press, Can We Tape?, http://www.rcfp.org/taping/index.html (last visited Dec. 1, 2008).

77. 15 U.S.C. § 6807.

78. For an analysis, see Edward J. Janger & Paul M. Schwartz, *The Gramm-Leach-Bliley Act, Information Privacy, and the Limits of Default Rules*, 86 MINN. L. REV. 1219, 1241-46, 1257-59 (2002).

79. 15 U.S.C. §§ 1681-1681x (Supp. V 2005).

80. *Id.* §§ 1681g(a), 1681j(a).

81. *Id.* § 1681c(g). For these cases, see Grabein v. 1-800-Flowers.com, Inc., No. 07-22235-CIV, 2008 U.S. Dist. LEXIS 11757 (S.D. Fla. Jan. 29, 2008); Vasquez-Torres v. Stubhub, Inc., No. CV 07-1328, 2007 U.S. Dist. LEXIS 63719 (C.D. Cal. July 2, 2007).

82. 15 U.S.C. § 1681c(g)(1).

otherwise possesses consumer information."[83] It requires covered entities that hold customer accounts to implement programs to respond to so-called "Red Flags" that signal possible ID theft.[84]

These meritorious aspects of FACTA are accompanied, however, by a number of ceilings that restrict the ability of states to offer greater protections to consumers. Before FACTA, the Fair Credit Reporting Act contained a list of limited preemptions for certain specified "subject matters," and these preemptions were set to expire in 2004.[85] In FACTA, Congress made permanent all existing preemptions in the Fair Credit Reporting Act, and added a list of new and permanent preemptions. In so doing, it reversed some existing state safeguards.[86] As Part III explains, however, FACTA also makes an important innovation to the jurisprudence of preemption by limiting some of its ceiling preemptions to a narrow category of "required conduct" rather than the broader category of "subject matter."[87]

Here, then, is the landscape against which Bill Gates and others have called for a federal omnibus statute for privacy—and one with strong preemption requirements. Industry in the United States also has made clear that strong ceiling preemption is an essential condition of its support for any comprehensive legislation. As a Microsoft white paper from 2005 states, "federal privacy legislation should pre-empt state laws that impose requirements for the collection, use, disclosure and storage of personal information."[88] Any single drop of preemption language in a federal statute is, moreover, likely to go a long way. In recent litigation concerning other areas of law, the Supreme Court has demonstrated a willingness in the face of statutory

---

83. *Id.* § 1681w(a)(1).

84. *Id.* § 1681m(e). A Red Flag is a pattern, or activity that might indicate identity theft, and the law and applicable guidelines require covered companies that have consumer information to implement identity theft programs to respond to Red Flags. *Id.*

85. *See, e.g.*, *id.* §§ 1681h(e), 1681t(b).

86. For example, FACTA reversed one aspect of California's Senate Bill 1 (S.B. 1), which required customers to be permitted to "opt-out," or indicate their refusal to information sharing before an organization could share such personal information with their affiliates. *Id.* § 1681a(d)(1). For case law finding that FACTA's preemption voids some but not all of S.B. 1's affiliate sharing provisions, see *American Bankers Ass'n v. Lockyer*, 541 F.3d 1214 (9th Cir. 2008).

87. 15 U.S.C. §§ 1681c-1, 1681t(b)(5) (Supp. V 2005).

88. Microsoft White Paper, *supra* note 1, at 4.

ambiguity to identify a congressional intent to occupy a regulatory field and impose a "ceiling."[89]

II. A FEDERAL OMNIBUS PRIVACY LAW: STRENGTHS AND WEAKNESSES

Overall, the approach in the United States to information privacy law in the private sector has been through sector-specific laws containing FIPs, which have been enacted by federal and state lawmakers. As I mentioned at the start of this Essay, Bill Gates and others support the creation of a federal omnibus law. Here there are two distinct issues, which I will treat sequentially. First, there is the issue of the general choice between an omnibus versus sectoral means of regulating information privacy law. The second issue, preemption, concerns how such a law would interact with state laws.

In this Part, while considering the possible merits of a federal omnibus law, I focus on the instrumental and normative implications for information privacy on the distribution of lawmaking authority among the federal government and the states. Thus, I assume that such legislation is constitutionally permissible. The scope of the Commerce Clause is broad, and the Supreme Court is likely to uphold a federal omnibus privacy law.[90] An omnibus privacy law might also have consequences for the overall distribution of political power between the federal government and the states. Rather than considering this larger federalism issue, however, I concentrate on the consequences for information privacy law of a federal omnibus law.

A. Federal Versus State Regulation of Information Privacy

Imagine enactment of a law that would provide general standards to be used when there was no sectoral law, or when there was silence or an

89. *Compare* Watters v. Wachovia Bank, N.A., 127 S. Ct. 1559 (2007) (noting that under the National Bank Act, a national bank's mortgage business, including its operating subsidiaries in the states, is subject exclusively to regulation by the Federal Office of the Comptroller of the Currency), *with id.* at 1573 (Stevens, J., dissenting) (noting an "absence of relevant statutory authority" permitting "the laws of a sovereign State" to "yield to federal power" in the regulation of the business activities of mortgage brokers and lenders).

90. *See* Reno v. Condon, 528 U.S. 141 (2000). In *Reno*, the Supreme Court held in a unanimous decision that Congress had power to regulate the conditions under which states and private parties could use, share, and sell drivers' motor vehicle registration information. *Id.* The Supreme Court has considerable leeway to decide that personal information itself is a subject of interstate commerce, and to find that even intrastate information markets can have an impact on interstate commerce. *See* Gonzales v. Raich, 545 U.S. 1, 26 (2005).

ambiguity in a sectoral law. In this Section, I consider precisely such an omnibus privacy statute, which would function as a gap-filler. What would be the results of such a statute? The consequences would prove to be both positive and negative. First, an omnibus law would overcome the inability of sectoral laws, whether federal or state, to respond adequately to telecommunications convergence. Second, omnibus laws would level the regulatory playing field where sectoral laws can place unequal burdens on industries in closely related areas. Finally, an omnibus law might help convince the EU of the adequacy of U.S. privacy law and thereby assist in smoothing data flows to this country. As for the negative results, these are the costs of an extra layer of regulation, namely, the harms from disregard of the "parsimony principle"—which is a warning against taking broad action under uncertainty—and the risk of an omnibus law's obsolescence.

1. Positive Results

Convergence is the idea that different kinds of telecommunications media are coming together in ways and with consequences that are often unexpected. In *Technologies of Freedom*, Ithiel de Sola Pool made an early and influential description of how convergence was affecting one area of telecommunications. As Pool noted in 1983, "Cable television systems no longer just distribute broadcast programs but also transmit data among business offices and sell alarm services, movies, news, and educational courses."[91] Such convergence is a result of the ease with which digital data can be shared, combined, and transmitted. Beyond such multifunctionality, convergence is also taking place because of the invention of new devices, applications, and software technologies.

In the face of convergence, sectoral laws run up against limits. I have already examined the VPPA and noted that it smoothly made the transition from the videocassette era to DVDs. It is now in the process of confronting the era of movies rented and watched online as well as YouTube and similar Internet sites, such as blogs with embedded vlogs. The statute's transition concerning traditional movies accessed online should be unproblematic, but more open questions are likely to confront the VPPA if it is to be applied to digital media that no longer seem to fit the regulatory paradigm from 1988 of "prerecorded video cassette tape[s] or similar audio visual materials."[92]

---

91. ITHIEL DE SOLA POOL, TECHNOLOGIES OF FREEDOM 27 (1983).

92. 18 U.S.C. § 2710(a)(4) (2000).

As another example of sectoral laws confronting convergence, the Children's Online Privacy Protection Act of 1998 (COPPA) regulates the use of children's personal information on the Internet. COPPA assigns enforcement power to the FTC, and this agency has already demonstrated through enforcement actions that COPPA applies to social networking sites that knowingly collect personal information from children without following the statute's requirements.[93] Yet COPPA does not regulate the new digital platforms that are independent of the Internet; it only applies to a "website or online service."[94] Moreover, scattered FTC enforcement actions pursuant to its general statutory authority neither provide comprehensive privacy protections nor completely close gaps in legal coverage.[95]

There is another problem that can follow from telecommunications convergence. A sectoral law might create competitive disadvantages for companies that fall under it and a corresponding subsidy to those outside of its reach. As an example, COPPA is a sectoral law that might bring comparative advantages to an industry that wishes to market to children on new digital platforms that fall outside its jurisdictional sweep.[96] As a further example, federal law regulates the use by telephone companies of a certain kind of customer information, which is termed "Customer Proprietary Network Information" (CPNI).[97] Yet Internet companies do not face analogous

---

93. 15 U.S.C. §§ 6501-6506. The two enforcement actions in question were settled in 2006 and 2008 respectively. United States v. Xanga.com, Inc., No. 06 Civ. 6853 (S.D.N.Y. filed Sept. 12, 2006), *available at* http://www.ftc.gov/os/caselist/0623073/xangaconsentdecree_image.pdf; United States v. Industrious Kid, Inc., No. 08-0639 (N.D. Cal. filed Jan. 30, 2008), *available at* http://www.ftc.gov/os/caselist/0723082/080730cons.pdf.

94. 15 U.S.C. § 6502(b)(1)(A).

95. *See generally* SOLOVE & SCHWARTZ, *supra* note 10, at 803 (describing FTC enforcement actions pursuant to COPPA).

96. There has been a dramatic increase in the marketing of food products, frequently unhealthy ones, to children on just such digital platforms. JEFF CHESTER & KATHRYN MONTGOMERY, INTERACTIVE FOOD & BEVERAGE MARKETING: TARGETING CHILDREN AND YOUTH IN THE DIGITAL AGE 13-18 (2007). At the same time, there also has been an increase in the ability of advertisers to track consumers on the Internet and elsewhere and collect personal information about them. JEFF CHESTER, DIGITAL DESTINY 128-38 (2007).

97. CPNI consists of personal customer information relating to the "quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier." 47 U.S.C. § 222(h)(1)(A). As the D.C. Circuit explains, CPNI "encompasses customers' particular calling plans and special features, the pricing and terms of their contracts for those services, and details about who they call and when." Nat'l Cable & Telecomms. Ass'n v. FCC, No. 07-0312, 2009 WL 348811, at *1 (D.C. Cir. Feb. 13, 2009). The D.C. Circuit has upheld the FCC's requirement that carriers obtain opt-in consent from a customer before sharing

restrictions on their use of similar customer data. CPNI regulations do not affect how Google uses customer information gathered through its search function, online calendar service, or e-mail service, Gmail. As explained below, however, the flip side of responding to convergence through an omnibus law is that this statute over time may itself become inflexible or ossified.

Finally, an omnibus federal privacy law might lessen the burden of the European regulatory hand on U.S. companies. Here, the Microsoft white paper notes, "[a] U.S. privacy law that is largely compatible with those of other countries would not only help reduce the complexity and cost of compliance, but also promote international business. Such legislation may help reduce barriers to data flowing into the United States."[98] The argument here is that a federal omnibus privacy law would do much, by its form alone, to smooth over differences concerning the critical issue—namely, the EU's regulation of personal data flows into the United States.

The EU Data Protection Directive requires that member states have equivalent data protection law. This requirement has exerted a force for harmonization around omnibus laws in the European Union. As a further requirement in the Directive, member states are only permitted to transfer personal data to nonmember states that have "an adequate level of protection."[99] As already noted, Senator Ervin wanted the United States to refuse to allow transfers of the personal information of U.S. citizens abroad without guarantees that the standards of S. 3418 would be met.[100] The idea of a data embargo on privacy grounds can be said, therefore, to have been first expressed in a U.S. Senate bill in 1974. Yet it was the EU that included a provision that required limits on data exports on privacy grounds in its information privacy laws.

It is hard to know whether the EU might conclude that an omnibus law in the United States adds something substantive to the current mix of information privacy safeguards in this country. Considering its ongoing scrutiny of substantive privacy practices in the United States, the EU may not reverse its "inadequacy" finding for U.S. law, or become more sympathetic to its privacy regime based simply on the form of American legislation. In 1999, the Working Party of EU Data Protection Commissioners found that U.S.

---

personal information with a carrier's joint venture partner or independent contractor in order to market communication-related services to that customer. *Id.* at *7.

98. Microsoft White Paper, *supra* note 1, at 5.

99. Data Protection Directive, *supra* note 19, art. 25(1), at 46.

100. *See supra* text accompanying note 29.

privacy law did not meet the adequacy standard.[101] Article 29 of the Data Protection Directive establishes this group; it is composed of a representative of the supervisory authorities in each Member State and a representative of the European Commission. Among the Working Party's tasks is providing the Commission with opinions on the level of data protection in third countries.[102] Pursuant to this authority, the Working Party stated that the "current patchwork of narrowly focused sectoral laws and voluntary self-regulation" in the United States is not adequate.[103]

Over time, the separate and collective responses by the U.S. government and the EU have provided U.S. businesses with myriad ways to comply with the adequacy requirement. These include (1) a negotiated "Safe Harbor" for companies that follow a set of preapproved regulations that meet the adequacy standard, (2) two sets of EU-approved model contractual clauses for use by American businesses, and (3) a newly streamlined process for approval of Binding Corporate Rules by European Data Protection Commissioners.[104] In addition, there has been an increasingly dense net of sectoral legal protection in the United States. Nonetheless, an omnibus law might add something and, thereby, help smooth the flow of personal information from the EU to the United States. In general, observers expect similar results from systems that share similar organizational forms.[105] Thus, if U.S. law adopted the same form as found throughout the EU, EU regulators might conclude that U.S. information privacy law provided as much protection as their own systems. On the other hand, the EU has already devoted significant resources to assessing information privacy in specific sectors in the United States and may continue with this mode of analysis.

Regarding the weight of the EU's regulatory hand, the United States might secure greater benefits through creation of a federal information privacy agency than adoption of a federal omnibus law. The Data Protection Directive requires

---

101. WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA, OPINION 1/99 at 2 (1999), http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1999/wp15en.pdf [hereinafter WORKING PARTY].

102. Data Protection Directive, *supra* note 19, art. 30, at 48.

103. WORKING PARTY, *supra* note 101, at 2.

104. SOLOVE & SCHWARTZ, *supra* note 10, at 1079-80.

105. As a specific example of this phenomenon, the European Commission in 2003 formally found Argentina to have adequate data protection. Its decision was influenced by Argentina's omnibus law. *See* Press Release, European Union, Data Protection: Commission Recognises That Argentina Provides Adequate Protection for Personal Data (July 2, 2003), http://europa.eu/rapid/pressReleasesAction.do?reference=IP/03/932.

such an independent organization in all EU member states.[106] The EU also has created a Data Protection Supervisor to ensure EU institutions process personal data lawfully, advise EU institutions on all issues with data protection dimensions, and cooperate with other data protection authorities.[107] Canada, Australia, Hong Kong, and Israel are only a few of the other countries that have a national data protection commission.[108] The lack of such an entity in the United States has harmed the continuity of its international privacy policy entrepreneurship. As Newman concludes, the lack of such a regulatory entity in the United States "has unintentionally undermined the power resources available to the United States to promote its interests globally."[109] In 2003, Robert Gellman made a similar point: "In essence, with the international critical mass of data protection agencies that now exists, a country without an agency is at an disadvantage."[110]

2. Negative Results

There are three potential problems with a federal omnibus law. These are (1) the costs of an extra layer of regulation, (2) the harms from disregard of the parsimony principle, and (3) the danger of ossification in the federal omnibus law itself. Under federal omnibus legislation, regulated entities would bear the cost of compliance with not only any sector regulation, federal or state, but also the federal omnibus law as it applies to their activities. To some extent FTC enforcement actions are already partial gap-fillers in regulatory coverage, and thereby increase the costs of compliance for private organizations that process personal information.[111] Yet the existing FTC privacy principles are far from comprehensive, and a federal omnibus law will, therefore, add in some fashion

---

106. Data Protection Directive, *supra* note 19, art. 28, at 47.

107. The EU Data Protection Supervisor was created in 2000. Regulation 45/2001, art. 41, 2001 O.J. (L 8/1) 1. For the home page of the European Data Protection Supervisor, see European Data Protection Supervisor, http://www.edps.europa.eu/EDPSWEB/edps/site/mySite/pid/15 (last visited Feb. 9, 2009).

108. For a listing of these agencies, see European Commission, National Data Protection Commissioners, http://ec.europa.eu/justice_home/fsj/privacy/nationalcomm/index_en.htm (last visited Feb. 9, 2009).

109. NEWMAN, *supra* note 6, at 155; *see* Schwartz, *supra* note 19, at 494 (arguing that the lack of an information privacy agency in the United States "handicaps its participation" in important international debates).

110. Robert Gellman, *A Better Way To Approach Privacy Policy in the United States: Establish a Non-Regulatory Privacy Protection Board*, 54 HASTINGS L.J. 1183, 1187 (2003).

111. *See supra* text accompanying note 95.

to the regulatory weight. At the same time, by leveling the privacy regulatory field, an omnibus law would also ameliorate inconsistencies that flow from convergence.

As for the parsimony principle, it warns against taking action—and especially broad action—under conditions of uncertainty. This principle was at work in 1974 during the debate about S. 3418 and then the Privacy Act. An analogy can also be drawn from environmental law. In this area, Congress has not enacted a federal gap-filling statute modeled on nuisance law. Instead, federal environmental law emerged in targeted areas—through sectoral regulations, as it were—as represented by the Clean Air Act, the Clean Water Act, the Endangered Species Act, and so on. Nuisance law is left as a gap-filler on the state level, where it is left to develop and be applied in a fashion that is attuned to local conditions, including aggregate local policy preferences.

Finally, a federal omnibus law might be difficult to amend. This flaw in a potential omnibus privacy law can be usefully compared to this flaw in the labor law context. Cynthia Estlund has demonstrated how an "ossification" of American labor law has taken place and contributed significantly to its ineffectuality.[112] By ossification, Estlund means a lack of meaningful changes over time within and without the National Labor Relations Act (NLRA) in response to new conditions. As part of her account, she describes the negative consequences of the federal labor statute's broad preemption of state and local law.

The risk of ossification following enactment of a federal omnibus privacy law is also great. Such an omnibus law, like the NLRA, would be difficult to amend—industry, privacy advocates, and other parties may be able to muster enough congressional support to block any significant changes to it.[113] Yet technological change will wreak havoc over time with such a statute's regulatory assumptions, both explicit and implicit. This example illustrates the negative side of the promise of an omnibus law in responding to telecommunications convergence.

In sum, with the issue of preemption off the table, the case for and against a federal omnibus law proves close. As a political reality, however, the issue of preemption cannot be bracketed from the discussion. Without strong preemptive language built around regulatory ceilings, an omnibus privacy bill would face considerable hurdles to enactment. The business coalition in favor

---

112. Cynthia L. Estlund, *The Ossification of American Labor Law*, 102 COLUM. L. REV. 1527, 1574 (2002) (offering an especially perceptive account of the way that labor law preemption doctrine has come "untethered from its statutory moorings").

113. *See generally* NEWMAN, *supra* note 6, at 60 (discussing "several institutional veto points" in the federal legislative system, which makes it easy to block legislation).

of the omnibus privacy bill has indicated its strong support for such preemption. As Meg Whitman, President and CEO of eBay, testified before Congress, "Legislation without preemption would make the current situation possibly worse, not better, by creating additional uncertainty and compliance burdens."[114] Indeed, the private sector alliance for privacy legislation is likely to prefer no federal privacy law to one that defers to stronger state privacy laws. Hence, I now turn to the critical issue of the merits of an omnibus privacy law that preempts stronger state privacy statutes.

B. Federal Omnibus Privacy Preemption of State Laws

The standard federalism terminology presents three preemptive possibilities. These are express, field, or conflict preemption.[115] In the area of information privacy, a federal omnibus statute can be expected to involve only conflict preemption.

First, an omnibus privacy law is unlikely to contain an express clause that allows it to preempt *all* state sectoral privacy law. Regulatory chaos would result as hundreds, perhaps even thousands, of more specific state laws fell by the wayside, and courts were obliged to determine how to apply the general provisions of a federal omnibus law to specific situations.

Second, and as a related point, an omnibus privacy law is unlikely to occupy an entire subfield of privacy regulation. After all, such a statute is by definition a general one, and information privacy, moreover, is a subject that touches on many areas. Unlike classic areas for field preemption, such as nuclear safety or alien registration, the federal interest in the regulation of information privacy is not so compelling as to displace all state concerns and state laws on the subject.[116]

Under conflict preemption, a federal law blocks a state statute that frustrates its ends. One can imagine, for example, that a federal omnibus law might cap damages for statutory violations. It might forbid private rights of

---

114. *Privacy in the Commercial World II: Hearing Before the Subcomm. on Commerce, Trade, and Consumer Protection of the H. Comm. on Energy and Commerce*, 109th Cong. 12-13 (2006) (statement of Meg Whitman, President and CEO, eBay Inc.) [hereinafter *Whitman Statement at Commercial Privacy Hearing*].

115. *See* Richard A. Epstein & Michael S. Greve, *Introduction: Preemption in Context*, *in* FEDERAL PREEMPTION: STATES' POWERS, NATIONAL INTERESTS 1, 1-5 (Richard A. Epstein & Michael S. Greve eds., 2007).

116. *See* Pac. Gas & Elec. Co. v. State Energy Res. Conservation & Dev. Comm'n, 461 U.S. 190, 212-13 (1983); Hines v. Davidowitz, 312 U.S. 52, 67-68 (1941).

action in state law. More generally, an omnibus law might set a series of ceilings above which the states may not regulate.

An omnibus law with such conflict preemption would be a dubious proposition. The two problems with it are its effect on experimentation in federal and state sectoral laws and ossification of the omnibus law itself. The preemptive scope of an omnibus federal privacy law is likely to block new approaches to information privacy in federal and state sectoral laws. Regarding the importance of state law, Martha Derthick has noted, "[s]tate governments are usually first to act in response to new problems or issues, of which many arise in a time of rapid technological and cultural change. It is very rare . . . for the federal government to be the first mover on a domestic question."[117] Such first moves by the states have occurred in the health care area, with state experiments in universal health care insurance, and recently in the reduction of greenhouse gases and other areas of environmental law. This Essay has also examined privacy law innovations in Section I.C.

Note, as well, the healthy choice that both Germany and Canada made to incorporate zones for both federal and state sectoral privacy regulation. In Germany, one such zone reserved for the states is for the protection of the data of insured citizens, including those who receive public support.[118] As Spiros Simitis observes of the shared authority of the federal and state governments in Germany, "[t]he regulation of the processing of personal information is a task that can only be performed by both, and that therefore has from the start demonstrated all the chances and risks of a genuinely federal regulation."[119]

Canada's federal privacy law, the Personal Information Protection and Electronic Documents Act (PIPEDA), regulates the international collection, use, and transfer of personal information. It also regulates the use of personal information by federal organizations and data flows between Canadian provinces. The provinces are generally reserved the right to regulate other use of personal information. As a substantive safeguard, however, PIPEDA requires that a provincial privacy law displace it only when the provincial

---

117. Martha Derthick, *Federalism*, *in* UNDERSTANDING AMERICA: THE ANATOMY OF AN EXCEPTIONAL NATION 121, 140 (Peter H. Schuck & James Q. Wilson eds., 2008).

118. The general German terms for this area of regulation are *Sozialordnung* ("social order"), or *Sozialwesen* ("social welfare"). For examples of the data protection issues in this area, see the recent report of the Berlin Data Protection Commissioner. BERLINER BEAUFTRAGTER, BERICHT DES BERLINER BEAUFTRAGTEN FÜR DATENSCHUTZ UND INFORMATIONSFREIHEIT [REPORT OF THE BERLIN COMMISSIONER FOR DATA PROTECTION AND FREEDOM OF INFORMATION] 123-56 (2007).

119. Spiros Simitis, *Zweck und Andwendungsbereich des Gesetzes* [*Goal and Scope of the Statute*], *in* NOMOS KOMMENTAR ZUM BUNDESDATENSCHUTZGESETZ [COMMENTARY ON THE FEDERAL PRIVACY LAW], *supra* note 17, at 156 (commenting on Section 1 of the BDSG).

regulation is "substantially similar" to it.[120] PIPEDA does not contain an explicit benchmark regarding the meaning of "substantial similarity," but assigns an important task to the national Privacy Commissioner in making this evaluation. In a report to Parliament, Commissioner George Radwanski has stated that, in the view of his office, substantial similarity means "equal or superior to" PIPEDA "in the degree and quality of privacy protection provided."[121] Lest there be any confusion, the Canadian Commissioner added, "The federal law is the threshold or floor."[122] The Ministry of Industry generally appears to take the same approach.[123] In her contribution to this Feature, Bellia also suggests that states will be subject to a number of federal inputs regardless of the formal existence of a federal statute.[124] These influences include judicial decisions interpreting constitutional provisions. As noted earlier, this point is well taken, and I further develop this theme of regulatory experimentation under decentralization in this Essay's next Part, which concerns federal and state sectoral law.

A second problem with a federal omnibus law would be difficulties in amending it. Here, I return to the risk of ossification in any federal omnibus privacy law.[125] Gridlock can also exist, of course, at the federal and state level for sectoral laws, but these challenges are more likely to be overcome. The next Part addresses this issue.

III. SECTORAL PRIVACY LAW: LIFE UNDER DEFENSIVE PREEMPTION

Thus far, this Essay has found a mixed case for a federal omnibus law without preemption, and expressed skepticism about such a statute with conflict preemption, which is the form that it is most likely to take. This Part turns to the issue of sectoral privacy law. In my view, there is a role for federal activity in this area, although one cannot state in advance that a federal sectoral law will necessarily be an improvement on the perhaps less tidy results from various state privacy statutes.

---

120. Personal Information Protection and Electronic Documents Act, 2000 S.C., ch. 5 § 26(2)(b) (Can.); *see* STEPHANIE PERRIN ET AL., THE PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT: AN ANNOTATED GUIDE 119 (2001).

121. PRIVACY COMM'R OF CANADA, REPORT TO PARLIAMENT CONCERNING SUBSTANTIALLY SIMILAR PROVINCIAL LEGISLATION 2 (2002).

122. *Id.*

123. *See infra* text accompanying notes 135-136.

124. *See* Bellia, *supra* note 65, at 875.

125. *See supra* note 112 and accompanying text.

A. Federal or State Sectoral Regulation

Among its problems, a federal omnibus law with conflict preemption would block regulatory experiments in sectoral laws. Yet these disparate statutes often can be improved through a process of ongoing consolidation of their results. As an initial point, I wish to describe this process and explain why this Essay's earlier objections to a federal omnibus law do not apply to sectoral laws, whether state or federal. This Section concludes by discussing why a trend of enacting federal sectoral laws is likely to continue.

States can generate simultaneous experimentation among different policies, but as information is generated about the benefits and costs of these alternatives, the next step, ideally, is a coherent policy implementation of the knowledge gained. In a similar fashion, Feeley and Rubin point to the need to take experimentalism under decentralization seriously.[126] In their view, some degree of centralization is needed to implement the results of experimentalism in a "reasonably effective fashion."[127] It is also important to add that centralizing results from multiple state laboratories of regulation does not necessarily lead to advocacy or creation of federal law.

First, the consolidation process can also take place within states. For example, important California financial privacy regulations originated at the local level, with counties in the Bay Area taking the lead.[128] These laws were then used in drafting S.B. 1, the California financial privacy law. Second, states might organize their own interstate mechanisms for evaluating results of disparate legislation. Possible institutions for such consolidation include the American Law Institute (ALI), the National Conference of Commissioners on Uniform State Law (NCCUSL), and the National Association of Attorneys General (NAAG). The classic example of an ALI process for improving state law is the *Restatement (Second) of Torts*, which sets out Prosser's privacy torts and heavily influences state law.[129] In contrast, NCCUSL and NAAG have not yet been especially influential in privacy law.[130]

---

126. *See* FEELEY & RUBIN, *supra* note 62.

127. *Id.* at 28.

128. Contra Costa County, Cal., Ordinance 2002-30 (Sept. 24, 2002); San Mateo County, Cal., Ordinance 04126 (Aug. 6, 2002).

129. For a selection of cases and a sense of the heavy influence of privacy torts as articulated in the *Restatement (Second) of Torts*, see SOLOVE & SCHWARTZ, *supra* note 10, at 30-140.

130. NAAG PRIVACY SUBCOMMITTEE REPORT: PRIVACY PRINCIPLES AND BACKGROUND, *available at* http://web.archive.org/web/20041216174950/http://www.naag.org/naag/resolutions/subreport.php (last visited Feb. 23, 2009).

What about the consolidation of state legal experiments at the federal level and through sectoral statutes? To a large extent, the arguments *against* a federal omnibus law that includes conflict preemption do not apply to sectoral law. Regarding its impact on state experimentation, a federal sectoral law in the United States is likely to occur subsequently to state sectoral laws because of the slow and sometimes difficult process of enacting federal legislation.[131] Indeed, assuming a similar pace of lawmaking among Congress and the states, there would be a random distribution of final legislative results among all the entities. The consequence would be that one or more of the fifty states would be likely to act before the federal government.

Moreover, in areas in which federal privacy law does not shut the door on further state activity, the states are likely to continue lawmaking. It is not only that state sectoral laws often will precede federal sectoral law in the United States, but also that state lawmakers will act in reaction to federal activity when it occurs, and a process of experimentation, drawing on involvement by advocacy groups and other stakeholders, will continue.[132] In addition, state government involvement in lawmaking increases the number of independent observations and the likelihood of deviations from the mean.[133]

Recent developments in Canadian information privacy law provide an illustration of this point. Important forces behind the enactment of PIPEDA, the federal Canadian privacy law, include the EU Data Protection Directive's "adequacy" standard, Canadian industry's drafting of an information privacy code for itself that it was able to incorporate into PIPEDA, and industry's awareness that it was increasingly subject to a variety of sometimes differing sectoral privacy laws in the provinces.[134] In addition, and as noted above, PIPEDA allows itself to be displaced by provincial laws that are "substantially similar" to it.[135] PIPEDA assigns authority to make this finding to the Governor in Council, legal adjunct to the federal cabinet, with recommendations from

---

131. For one illustration, contrast the quick reaction in Vermont in 1992 to certain credit reporting mistakes in the state the year before, and the slower reaction in Washington, D.C., which ultimately led in 1996 to certain amendments to the Fair Credit Reporting Act. *See* Michael Epshteyn, Note, *The Fair and Accurate Credit Transactions Act of 2003: Will Preemption of State Credit Reporting Laws Harm Consumers?*, 93 GEO. L.J. 1143, 1162-63 (2005).

132. *See* Michael W. McConnell, *Federalism: Evaluating the Founders' Design*, 54 U. CHI. L. REV. 1484, 1498 (1987) (book review) ("Lower levels of government are more likely to depart from established consensus simply because they are smaller and more numerous.").

133. *Id.*

134. PERRIN ET AL., *supra* note 120, at 2-11.

135. *See supra* text accompanying note 120.

the Ministry of Industry and the Privacy Commissioner of Canada.[136] Thus far, this process has led to exemptions for all three of the provinces with omnibus privacy laws for the private sector. These provinces are Quebec, British Columbia, and Alberta. The omnibus privacy law in Quebec was enacted before the PIPEDA, and those in British Columbia and Alberta subsequent to it.[137] A sectoral privacy law for health information in Ontario that came into force in 2004 has also been found to meet PIPEDA's standards, and thus "health information custodians" in that province are exempt from the application of PIPEDA.[138]

PIPEDA offers a path to harmonize different state laws while also leaving room for continuing state government inputs into information privacy lawmaking. By allowing exemptions for "substantially similar" provincial laws, PIPEDA provides incentives for the state to enact omnibus and sectoral laws that follow its approach. More subtly, it also permits a way for innovations at the state level to be incorporated into it. PIPEDA's section 29 calls for a parliamentary review of the Act every five years.[139] In May 2007, a committee of the Canadian House of Commons provided recommendations from the first such statutory review.[140] Perhaps the most striking aspect of this report is the broad consensus about drawing on lessons from provincial laws in considering amendments to and alterations in PIPEDA. As the committee stated, "[W]e heard from privacy advocates, academics, business and industry organizations, as well as from the Federal Privacy Commissioner, that reference should be made to these provincial laws when making changes to PIPEDA."[141] Special attention in the ensuing recommendations was paid to the private sector data protection laws of Alberta and British Columbia.[142] These were considered to

136. Personal Information Protection and Electronic Documents Act: Process for the Determination of "Substantially Similar" Provincial Legislation by the Governor in Council, C. Gaz., pt. I, at 3618-22 (Sept. 22, 2001) (Can.); PRIVACY COMM'R OF CANADA, *supra* note 121, at 1-2.

137. BARBARA MCISAAC, RICK SHIELDS & KRIS KLEIN, THE LAW OF PRIVACY IN CANADA 4-27 (rev. ed. 2006); STANDING COMM. ON ACCESS TO INFO., PRIVACY AND ETHICS, STATUTORY REVIEW OF PIPEDA 3 (2007) [hereinafter STANDING COMM. REPORT].

138. MCISSAC ET AL., *supra* note 137, at 4-27 to 4-28.

139. Personal Information Protection and Electronic Documents Act, 2000 S.C., ch. 5 § 29 (Can.).

140. STANDING COMM. REPORT, *supra* note 137.

141. *Id.* at 1.

142. *Id.* at 47-51.

be important as "second generation" statutes that had been enacted subsequently to PIPEDA as well as the Quebec statute.[143]

In the United States, interplay between federal and state governments as well as with other entities is already observable in environmental law. As scholars in this field have explored, this interplay can take a number of forms. For example, Ann Carlson talks about "iterative federalism," in which the federal government allows one state, in the role of a "super-regulator" to have special power.[144] I return to this idea below. More broadly, Jody Freeman and Daniel Farber have developed a "modular" conception of environmental regulation based on their examination of the CalFed Bay Delta program.[145] In modular environmental regulation, decisionmakers at the federal and state levels share power through a mix of formal and informal tools for implementation of policy goals.

Although rare for the federal government to be a first mover on a domestic privacy issue, as Bellia indicates, such behavior can occur.[146] As an example in the privacy area, the VPPA demonstrates Congress's quick action after the publication of information about Judge Robert Bork's video rental records. This example provides an interesting case study of a privacy horror story with a uniquely federal aspect as well as a historical moment when preemption was not on the radar of the concerned industry.

Immediately before the passage of the VPPA, Judge Bork had been mired in controversial congressional confirmation hearings regarding his ultimately unsuccessful nomination for the Supreme Court. Ironically enough, one of the issues during the confirmation hearings had been the extent of Judge Bork's view of the constitutional dimensions of privacy.[147] There was bipartisan

---

143. *Id.* at 1.

144. Ann E. Carlson, *Iterative Federalism and Climate Change*, 103 NW. U. L. REV. (forthcoming June 2009) (manuscript at 12, on file with author).

145. Jody Freeman & Daniel A. Farber, *Modular Environmental Regulation*, 54 DUKE L.J. 795 (2005).

146. Bellia, *supra* note 65, at 881-86.

147. Judge Bork did not think that the Constitution contained a right to privacy. The confirmation hearings did not, however, turn on whether Congress had a right to legislate in this area. *See Video and Library Privacy Protection Act of 1988: Joint Hearing on H.R. 4947 and S. 2361 Before the Subcomm. on Courts, Civil Liberties and the Administration of Justice of the H. Comm. on the Judiciary and the Subcomm. on Technology and the Law of the S. Comm. on the Judiciary*, 100th Cong. 133-34 (1988) (statement of Sen. Alan K. Simpson) [hereinafter *Video Privacy Hearings*] ("As Judge Bork so articulately pointed out during his hearings, the Congress of the United States does have the power to legislate privacy rights if it wishes."); *id.* at 67 (statement of Janlori Goldman, Staff Attorney, Am. Civil Liberties Union) ("[T]he

agreement, however, regarding the outrageous nature of the violation of Judge Bork's own privacy by a Washington weekly's article on his video rentals. Senator Patrick Leahy expressed this outrage in the hearings on the Act:

> I well remember when Senator Al Simpson came before the committee during the Bork hearings and announced what happened. That committee, as you know, was split between those supporting Judge Bork and those opposed to him. But it was unanimous—the feeling across the committee of outrage—when we learned of the disclosure.[148]

Congress's rapid enactment of the VPPA was an exercise in unanimity at a time when the Bork nomination was dividing it and the nation. As it entered new legislative territory with the VPPA, Congress wisely chose not to preempt future state sectoral laws that offer stronger protections.[149]

From today's perspective, it is interesting to revisit this legislative choice. The legislative history of the VPPA is almost entirely devoid of references to preemption, apart from perfunctory mentions that the law would not preempt stronger state statutes.[150] Most telling, the joint hearing on the statute included no discussion of preemption. To be sure, there were contentious issues aired that day. The joint hearing involved a vigorous discussion of whether or not the proposed statute should include protection for library records, and such coverage, initially included in the House and Senate bills, was dropped from the final Act.[151] Another heated discussion at the hearing concerned the extent to which the Act would change practices of the direct mailing industry.[152] The Act as enacted allows marketing directly to consumers based on general subject matter categories of videos rented, but also requires that consumers be given

majority of Senators who voted against his confirmation cited their concern about the Judge's limited view of the Constitutional right to privacy.").

148. *Id.* at 31 (statement of Sen. Patrick Leahy).

149. 18 U.S.C. § 2710(f) (2000).

150. For such a brief reference, see S. REP. NO. 100-599, at 15 (1988), *reprinted in* 1988 U.S.C.C.A.N. 4342-1, 4342-12.

151. *See id.* at 8, *reprinted in* 1988 U.S.C.C.A.N. 4342-1, 4342-8 (noting that the Subcommittee "was unable to resolve questions regarding the application" of a provision on disclosure of "library borrower records"). For the discussion of the protection of library records at the hearing, see *Video Privacy Hearings*, *supra* note 147, at 34-53.

152. *See Video Privacy Hearings*, *supra* note 147, at 87-114 (statement of Richard A. Barton, Senior Vice President, Direct Mktg. Assoc.).

the chance to prohibit such marketing.[153] It was felt that this approach would be generally consistent with marketing practices at the time.[154]

The hearings also provide hints regarding the grounds for the lack of interest in preemption. As testimony at the hearing indicated, the majority of the video rental industry in 1988 consisted of "small, one-owner operations."[155] Blockbuster and other large chains did not yet exist, and Netflix was not yet even a gleam in the eye of some entrepreneur or venture capitalist. Thus, the then-existing video rental industry, based around mom-and-pop stores, did not view preemption as a significant issue because so many of its retail outlets were in a single location with customers in that same geographic entity.[156] In this regard, the nature of the most affected industry at that time made it easy for Congress to structure this privacy legislation without preemption.

As for ossification, federal sectoral law runs this risk to a considerably lesser extent than an omnibus law. As an example at the federal level, the credit reporting industry is large, but far smaller, of course, than the entire private sector. And the emergence of new factors, such as identity theft, a high public interest in the issue, and a strategic use of sunset provisions in previous legislation, led in 2003 to the enactment of FACTA, which amended the Fair Credit Reporting Act. Many new problems had arisen since the last major amendment of the Fair Credit Reporting Act, which was in 1996.

Two of the most important of these problems concerned the explosion in identity theft and an increase in "risk-based" pricing, which raises or lowers the cost of borrowing based on one's credit score.[157] To help prevent identity theft, FACTA granted consumers the ability to add fraud alerts to their files at national consumer reporting agencies.[158] It also simplified this process by allowing consumers to inform just one agency, which is then required by law

---

153. 18 U.S.C. § 2710(b)(2)(D)(i)-(ii); *see* S. REP. NO. 100-599, *supra* note 150, at 13-14.

154. *See Video Privacy Hearings*, *supra* note 147, at 88-89 (statement of Richard A. Barton, Senior Vice President, Direct Mktg. Assoc.).

155. *Id.* at 125.

156. Indeed, preemption was not even on the radar of the nation's then-largest video retailer, Erol's, which had some multi-state operations. A representative of Erol's testified before Congress strongly in favor of the Video Privacy Protection Act and did not raise the preemption issue. *Id.* at 76-86 (statement of Vans Stevenson, Dir. of Pub. Relations, Erol's, Inc.).

157. *See* Epshteyn, *supra* note 131, at 1154-55 (describing the rise of identity theft after the enactment of the original Fair Credit Reporting Act); Gail Hillebrand, *After the FACTA: State Power To Prevent Identity Theft*, 17 LOY. CONSUMER L. REV. 53, 56-57 (2004) (discussing the use of "risk-based" pricing to determine the "nuances and gradations in price and terms" of consumer credit).

158. 15 U.S.C. § 1681c-1(a) (Supp. V 2005).

to inform the other credit reporting agencies.[159] As noted above, moreover, FACTA also requires the FTC and banking agencies to issue so-called "Red Flag" rules.[160] As a final example regarding identity theft, businesses are to truncate credit and debit card numbers on electronically printed receipts and are forbidden from printing the card's expiration date on a receipt.[161] A receipt with such information on it represented one stop shopping for an identity thief.

As for the "risk-based" provision of credit, FACTA requires notice to the consumer when material terms of credit are less favorable than the most favorable terms available to a "substantial proportion" of consumers.[162] This information allows the consumer to know that she is receiving terms that are less favorable than those offered to others. It will thereby motivate investigations of accuracy in credit scoring. And FACTA also permits consumers to receive a free credit report as well as their credit score "for a reasonable fee."[163] Here, too, the idea is to increase the transparency for consumers of the credit industry.

Overall, federal sectoral law can have the potential to build on the results of state law. The devil is in the details, however, and one cannot state at an abstract level that a federal sectoral law is necessarily preferable to the messier universe of different and unconsolidated state sectoral statutes. Whether one is a privacy advocate or skeptic, history teaches that the federal government and the states may switch back and forth in their concern for and level of attention to this issue. As Lynn Baker and Ernest Young warn concerning institutional aspects of federalism, it is risky to make structural decisions about allocating power "based on predictions that any particular group will continue to dominate a particular portion of the government for long."[164] One cannot be confident in a given policy result reached by reliance on a federal as opposed to state regulatory process, or vice versa.[165] Change will be a constant with ongoing shifts in alignments, whether among branches of the federal government, or between the federal and state levels. Amidst the change, one

---

159. *Id.* § 1681c-1(e).

160. *See supra* text accompanying note 84.

161. 15 U.S.C. § 1681c(g).

162. *Id.* § 1681m(h).

163. *Id.* §§ 1681j(a), 1681g(a); *see* Hillebrand, *supra* note 157, at 65-66.

164. Lynn A. Baker & Ernest A. Young, *Federalism and the Double Standard of Judicial Review*, 51 DUKE L.J. 75, 151-52 (2001).

165. Even though Baker and Young favor state lawmaking, they also concede that "increased diversity [in legislation] among the states is not always a good thing." *Id.* at 155.

contribution that scholars can nonetheless make is to identify at least general circumstances under which federal sectoral law is likely to bring benefits. The next and final Section takes up this task.

An additional point should be made about federal versus state sectoral privacy in the United States regarding a certain reality of regulatory life. Good, bad, or indifferent, sectoral privacy law at the federal level is not only here to stay, it constitutes a future growth field. In a classic paper from 1985, E. Donald Elliott, Bruce Ackerman, and John Millian proposed an evolutionary model of statutory law.[166] In their paradigm, an important middle period in the regulatory lifecycle involves the flight by regulated entities to Washington, D.C., in search of relief. These entities seek to counter organizational successes for advocacy groups at the state level by seeking preemptive lawmaking at the federal level. J.R. DeShazo and Jody Freeman later termed this phenomenon "defensive preemption."[167] As DeShazo and Freeman point out, state-level regulations can unnerve industry and prompt its demand for federal preemptive lawmaking.[168]

This description accurately captures the unfolding dynamic in the policy arena for information privacy. There has been a noticeable lack of gridlock at the state sectoral level. The website of the California Office of Information Security and Privacy Protection displays an impressive list of privacy legislation enacted in 2008 alone or currently pending.[169] Among the recent legislation are statutes that make it a misdemeanor to eavesdrop intentionally on Radio Frequent Identification devices, that increase penalties for hospital employees that snoop through medical records, and that simplify the procedures for consumers to place a security freeze on their credit files.[170] An interesting regulatory lever has been the public's strong interest in privacy. This interest has been reflected in countywide privacy regulations—such as northern California's financial privacy ordinances—and a successful use of a privacy

166. E. Donald Elliott, Bruce A. Ackerman & John C. Millian, *Toward a Theory of Statutory Evolution: The Federalization of Environmental Law*, 1 J.L. ECON. & ORG. 313 (1985).

167. J.R. DeShazo & Jody Freeman, *Timing and Form of Federal Regulation: The Case of Climate Change*, 155 U. PA. L. REV. 1499, 1500 (2007).

168. *See id.* at 1530.

169. California Office of Information Security and Privacy Protection, 2008 Privacy Legislation Enacted, http://www.oispp.ca.gov/consumer_privacy/privacy_leg/leg.asp (last visited Dec. 1, 2008).

170. *Id.*

referendum in North Dakota and the threat of such a referendum in California.[171]

Like environmental law, privacy is also an attractive area for politicians and private advocates seeking a field for policy entrepreneurship. Regarding politicians, Regan in 1995 identified a number of factors that affected the willingness of members of Congress to assume policy leadership in privacy issues. For our purposes, it is of greatest significance that any initial interest and attention is only sustained, in Regan's analysis, when there is continuing visibility for the privacy issue and continuing media interest in it.[172] These conditions are more than present today. Concerning private organizations, Colin Bennett has noted that "the number of groups engaged in privacy advocacy has increased dramatically during the last ten to fifteen years."[173] He also finds that privacy is also now "on the agendas of an increasing number of more established groups."[174] He attributes this increase in advocacy organizations for privacy to the rise of the Internet, the new variety and pervasiveness of technologies of surveillance, and the international nature of flows of personal information.[175]

Thus, gridlock has not kept states from enacting privacy statutes. States are also not competing for business with each other by failing to regulate privacy with sufficient rigor. There certainly has been no race to the bottom, which also has been termed the "race of laxity."[176] In the context of environmental law, there is a rich scholarly debate regarding whether or not states have competed to offer weaker regulatory regimes to curry favor with business.[177] In the area of information privacy, there is scant room for such a debate. Even if there is no indication of a race to the top, states are far from enacting successive waves of information privacy statutes with weaker protections for consumers and more favorable conditions for businesses. In other words, California

---

171. Adam Clymer, *North Dakota Tightens Law on Bank Data and Privacy*, N.Y. TIMES, June 13, 2002, at A28; Jennifer 8. Lee, *California Law Provides More Financial Privacy*, N.Y. TIMES, Aug. 28, 2008, at A24.

172. REGAN, *supra* note 40, at 202-09.

173. COLIN J. BENNETT, THE PRIVACY ADVOCATES 59 (2008).

174. *Id.*

175. *Id.*

176. ZYGMUNT J.B. PLATER ET AL., ENVIRONMENTAL LAW & POLICY 296 (3d ed. 2004).

177. *See, e.g.*, Kirsten H. Engel, *State Environmental Standard-Setting: Is There a "Race" and Is It "to the Bottom"?*, 48 HASTINGS L.J. 271 (1997); Richard L. Revesz, *The Race to the Bottom and Federal Environmental Regulation: A Response to Critics*, 82 MINN. L. REV. 535 (1997); Richard L. Revesz, *Rehabilitating Interstate Competition: Rethinking the "Race-to-the-Bottom" Rationale for Federal Environmental Regulation*, 67 N.Y.U. L. REV. 1210, 1211-12 (1992).

privacy initiatives have not encouraged Nevada or other states, neighboring or otherwise, to enact weaker regulations in the same area. At any rate, state legislative activities will continue and will drive a flight by businesses to Washington for federal solutions. Over the next decade and beyond, continuing waves of state privacy lawmaking will provoke industry activity to seek federal legislation.

B. A Dual Federal-State System for Information Privacy

Due to the regulatory dynamic that this Essay has described, there will be both federal and state privacy legislation in the years to come. As a consequence, there is a need to think critically about life under defensive preemption. In taking such a step, this Essay assesses three aspects of regulatory life under a dual federal-state system for information privacy law. First, there is value in identifying circumstances in which federal consolidation of state law will likely be useful. Second, there is need to consider points beyond the usual debate about floors and ceilings. Third, Congress may prove more enthusiastic regarding broad federal preemption than this Essay generally favors, and in those cases, second-best legislative solutions should accompany preemption.

1. Federal Consolidation

I now consider two ways in which consolidation of different state laws in the area of information privacy would bring benefits: (1) through the avoidance of inconsistent regulations, especially in areas with high costs and little policy payoff, and (2) through the establishment of "field definitions" that can lower compliance costs.

As for avoiding inconsistent regulation, certain regulations entail costs with scant privacy benefits. For example, Massachusetts has a law that blocks breach notices from including information about the breach incident.[178] In their respective statutes, other states require disclosure of precisely such information.[179] In addition, the triggers for notification in different states

178. MASS. GEN. LAWS ch. 93H, § 3 (2007).

179. *Compare id.* ("The notice to be provided to the resident . . . shall not include the nature of the breach or unauthorized acquisition or use or the number of residents of the commonwealth affected by said breach or unauthorized access or use."), *with* N.Y. GEN. BUS. LAW § 899-aa(7) (McKinney 2005) ("[N]otice shall include . . . a description of the categories of information that were, or are reasonably believed to have been, acquired by a person without valid authorization, including specification of which of the elements of

differ—and sometimes in idiosyncratic ways.[180] An obligation to inform a consumer can follow from the acquisition of information by an unauthorized person when there is a breach that poses a significant risk of identity theft, when there has been a reasonable likelihood of illegal use of the information, or when there has been a "material risk of identity theft or other fraud to the resident."[181] The universe of choices might easily be standardized into a menu of three categories with scant loss of substantive regulatory variety.

A second benefit of consolidation concerns basic statutory definitions that mark a given regulatory field. The preemptive power of such a "field definition" prevents states from redefining the scope of a fundamental legislative category. As an example, the Fair Credit Reporting Act contains a detailed definition of "consumer report."[182] Congress was wise to enact such basic subject matter definitions; terms that clearly bound the scope of a regulatory field reduce regulatory transaction costs. Note, however, that as technology and businesses evolve, entire new enterprises and modes of data processing may spring up. In that case, states are free to generate a new category or categories for regulation.

2. *Beyond Ceilings and Floors*

The debate in information privacy law frequently centers on the merits of ceilings versus floors in federal legislation. As an international example, the Canadian Privacy Commissioner indicated his view in 2002 that PIPEDA sets a floor that only permits certification of state laws that offer equivalent or greater privacy protection.[183] The Department of Industry, which also plays an important role in a certification of provincial law as "substantially similar," has issued a notice of its process that indicates a similar view. In particular, the Department requires provincial legislation to incorporate the ten privacy principles of PIPEDA, provide for independent and effective privacy oversight,

personal information and private information were, or are reasonably believed to have been, so acquired.").

180. *See, e.g.*, Schwartz & Janger, *supra* note 56, at 942-43.

181. For a table with a detailed comparison of different state security breach notification laws, see *id.* at 972-84.

182. 15 U.S.C. § 1681a(d) (2000 & Supp. V 2005).

183. *See supra* text accompanying note 121.

and restrict the use of personal information to purposes that are "appropriate or legitimate."[184]

Despite the useful Canadian example, in my view, the debate about ceilings and floors in information privacy law cannot be resolved in advance and at a general level. As William Buzbee notes with a focus on environmental law, "[p]reemption choice . . . must turn largely on the nature of the regulatory task involved."[185] This debate regarding information privacy law also cannot be resolved in advance of a specific regulatory context. Nonetheless, there are important subjects beyond ceiling and floors, and a scholarship of information privacy regulation can contribute to these areas. In this light, I wish to concentrate on two points: the benefits of narrowing ceilings to only the conduct regulated, and sharing of enforcement authority among federal and state regulators.

Even when there is a strong argument for uniformity of regulatory action, and, hence, a federal ceiling, there are merits to narrowing the ceiling to specific conduct rather than the entire subject matter. The benefit of such preemption for conduct is to create an element of certainty for regulators and regulated entities while also leaving open the possibility for future regulatory innovations by the state. FACTA leads the way in showing how to limit a ceiling preemption.

To be sure, FACTA contains numerous examples of subject matter preemption.[186] Yet it also involves some preemption limited to required conduct; this preemption restricts the assignment of federal power to the behavior mandated. For example, as noted above, FACTA requires consumer reporting agencies to place fraud alerts on consumer credit files under certain circumstances.[187] In so doing, FACTA streamlines one area of industry procedures; at the same time, it allows states to engage in further regulation regarding the larger subject area, which is identity theft.

As a further matter, there is a strong argument for sharing enforcement authority among federal and state regulators. As Roderick Hills suggests, "The benefits of federalism in the present and in the future will rest on how the federal and state governments interact, not in how they act in isolation from

---

184. Personal Information Protection and Electronic Documents Act: Process for the Determination of "Substantially Similar" Provincial Legislation by the Governor in Council, C. Gaz., pt. I, at 3621-22 (Sept. 22, 2001) (Can.).

185. William W. Buzbee, *Asymmetrical Regulation: Risk, Preemption, and the Floor/Ceiling Distinction*, 82 N.Y.U. L. REV. 1547, 1602 (2007).

186. 15 U.S.C. § 1681t.

187. *Id.* § 1681c-1. The preemption narrowed to "the conduct required" is codified at 15 U.S.C. § 1681t(b)(5).

each other."[188] FIPs should also take into account such interactions, and hence, demand attention to the conditions of joint federal-state governance. Information privacy standards require contributions by different federal and state government agencies, the private sector, advocacy groups, individual citizens, and the judiciary in ongoing deliberations. FIPs should not end the question of how to regulate a specific area of information privacy, but instead should begin a process of debating privacy norms and negotiating regulatory content.[189]

The problem with a monopoly on enforcement given to federal agencies is that it would assign these organizations too large a role in the regulatory dialogue. Federal preemption of statutory regulatory authority would also burden a handful of federal agencies with an impossibly large regulatory role in light of their limited resources and myriad other responsibilities.[190] In contrast to this view, the industry coalition in favor of federal privacy legislation, in addition to its support for preemption, opposes private rights of action. In her congressional testimony, for example, Meg Whitman termed a private right of action "counterproductive" and warned against companies being "brought to their knees" by class-action lawsuits.[191]

In an absence of private rights of action, however, there is likely to be significant underenforcement of privacy interests. As an illustration, the Federal Trade Commission—which Meg Whitman in her testimony singles out for an enforcement role—includes privacy as only one of its regulatory tasks, along with antitrust, mergers, and consumer protection issues other than privacy. It has already taken on a significant privacy enforcement role under the Children's Online Privacy Protection Act of 1998 as well its own power to stop "unfair or deceptive acts or practices in or affecting commerce."[192] An exclusive statutory grant of additional privacy authority to the FTC is not likely to cause much, if any, additional enforcement.

---

188. Roderick M. Hills, Jr., *Against Preemption: How Federalism Can Improve the National Legislative Process: Cyberspace Filters, Privacy Controls, and Fair Information Practices*, 82 N.Y.U. L. REV. 1, 4 (2007).

189. *See* Schwartz, *Lessig's Code*, *supra* note 15, 781-86.

190. A range of other issues also arise in any division and sharing of power, including the question of choice of judicial fora for hearing claims.

191. *Whitman Statement at Commercial Privacy Hearing*, *supra* note 114, at 13, 37.

192. 15 U.S.C. § 45(a)(1). For a discussion of the FTC's enforcement powers under its enabling act and its use in the context of children's online privacy, see SOLOVE & SCHWARTZ, *supra* note 10, at 777-82, 803.

3. *Second-Best Solutions*

I wish to conclude by acknowledging that Congress may sometimes manifest a taste for broad sectoral preemption.[193] As a second-best solution, this Essay therefore advocates that Congress draw on two additional policy safeguards. First, Congress should consider the usefulness of a unitary sectoral preemption "plus one" strategy. This idea is inspired by the Clean Air Act's regulation of pollution from mobile sources; it sets a federal ceiling, but allows a single state, California, to exceed federal emission standards.[194] Other states are permitted to follow the California approach, but they may not enact customized standards. Carlson terms a state that federal law singles out in such a fashion as a "super-regulator."[195]

If a federal sectoral privacy law chooses the path of broad preemption, Congress should allow at least a single state to keep its higher standards or develop different standards. This state should have bureaucratic expertise in the area, represent a large market in the chosen sector of regulation, and have a citizenry and advocacy organizations involved in the issue. Instead of the "plus one" strategy, however, federal law sometimes simply grandfathers in states with sectoral privacy regulation. For example, FACTA provides exceptions to one of its preemptive ceilings for California and Massachusetts.[196] While the approach rewards the states that beat Congress to the regulatory punch, it cuts off the possibility that other states will be able to make choices in a marketplace of regulatory models.

As a second fallback proposal, preemption clauses in federal privacy legislation should be subject to a ten-year sunset to allow Congress to evaluate information about the successes and failures of federal regulation. There is already a past example of such a sunset in substantive information privacy law. Amendments in 1996 to the Fair Credit Reporting Act contained sunsets for a number of statutory provisions that affected billions of dollars in commercial transactions.[197] With the expiration of these statutory sections imminent, industry was forced to the congressional bargaining table, and at a time when

---

193. Regarding this trend in areas other than information privacy law, see Buzbee, *supra* note 185, at 1552–55.

194. 42 U.S.C. §§ 7507, 7543(e).

195. Carlson, *supra* note 144 (manuscript at 1).

196. 15 U.S.C. § 1681t(b)(1)(F).

197. EVAN HENDRICKS, CREDIT SCORES & CREDIT REPORTS 307–08 (2d ed. 2005). For a skeptical view of the industry's assessment of the cost of letting the preemption of these provisions lapse, noting the historic absence of a single nationwide market for credit reporting, see Epshteyn, *supra* note 131, at 1161.

the public had a growing awareness of the shortcomings of existing regulations and new information about the harms from identity theft and risk-based credit. The result was the enactment of FACTA, which—although imperfect—added important new protections to the Fair Credit Reporting Act. Creating sunsets for preemptions has the additional merit of forcing Congress to reassess the wisdom of its assertion of regulatory primacy. It schedules a revisiting of regulatory choices and thereby creates a safeguard against regulatory ossification.

CONCLUSION

A federal omnibus information privacy law with strong preemption provisions would be an unfortunate development. It would limit further experimentation in federal and state sectoral laws. Such a law also would be difficult to amend, and would, therefore, become outdated as technological changes undermine such a statute's regulatory assumptions.

In contrast, federal sectoral privacy law presents a more complicated situation. One cannot state in advance that a federal sectoral law will necessarily be an improvement on the results of various state privacy statutes. It is clear, nonetheless, that federal sectoral privacy law will be a growth field in the next decades. State innovations in the information privacy field are also likely to provoke industry lobbying for federal responses. There will likely be many attempts, including some successful ones, at defensive preemption in federal sectoral privacy law.

A dual system of federal and state sectoral regulation has both promise and peril. This Essay provides new categories for classifying and encouraging federal and state inputs into information privacy law. Federal consolidation of state privacy laws can provide benefits by avoiding inconsistent regulations, especially in areas with high costs and little positive policy results, and by establishing basic regulatory categories. It is also important to work with concepts beyond the classic preemptive categories of "floors" and "ceilings." One such concept concerns the possibility of limiting ceiling preemption only to certain specific conduct rather than an entire subject matter. In 2003, FACTA demonstrated the feasibility of such an approach to the jurisprudence of preemption.

Even when Congress manifests a preference for broad sectoral preemption, certain second-best solutions are available. The first of these is to adopt a "plus one" strategy. In this approach, states can choose either a federal standard or that of a single state with different standards. A second fallback proposal is to subject preemption clauses in federal information privacy statutes to a ten-year sunset to allow for feedback regarding the performance of federal regulation.

The ultimate task of a dual system for federal and state information privacy law is to develop mechanisms for weeding out policies that fail and for promoting the successes.