Memorandum

To: LEO Workshop Members, Yale Law School
From: Paul M. Schwartz, Jefferson E. Peyser Professor of Law, Berkeley Law School
Re: "Information Privacy Federalism," LEO Talk, Yale Law School (November 20, 2014)
Date: November 15, 2014

As a basis for my presentation on November 20, I will be using my chapter, *The Value of Privacy Federalism*. This Memorandum will sketch out some larger goals of my "Information Privacy Federalism" project. In particular, there is a need for development of a robust normative theory of how differently situated governmental units, at both the federal and state levels, can contribute to the development of information privacy law.[1] Associated with this issue is the question of the proper role of courts, legislators, administrative agencies and other governmental entities.

In this Memorandum, I wish to describe the gap in information privacy scholarship regarding federalism, provide a sketch of how information privacy law functions at the federal and state levels, and suggest that collective action explanations may not get us very far towards a normative theory of information privacy federalism. There is also a comparative dimension to this project, and I address that briefly in a final section.

I. Information Privacy Law Scholarship: "Mind the Gap"

Information privacy scholarship in the U.S. largely ignores federal-state issues. Much privacy scholarship simply focuses on federal law; this work is frequently organized around specific statutes, such as Anita Allen's exploration of whether the Children's Online Privacy Protection Act is excessively paternalistic.[2] Similar statutory-driven analysis exists around such federal laws as the Fair Credit Reporting Act (FCRA), the Gramm-Leach-Bliley (GLB) Act, the Video Privacy Protection Act, and the Health Insurance Portability and Accountability Act (HIPAA).

Other privacy scholarship focuses on how the law regulates new technologies and associated services. One recent strand of such scholarship looks at Big Data and its

[1] For my previous work in this area, see Paul M. Schwartz, *Preemption and Privacy*, 118 Yale L.J. 902 (2009).
[2] Anita Allen, *Coercing Privacy*, 40 William & Mary L. Rev. 723 (1999).

manifestations.[3] Here, authors typically analyze how both federal and state law respond to this new technology. The characteristic finding is one of legal inadequacy. These diverse strands of scholarship share at further trait: a manifest lack of interest in how federal and state entities work together to create and administer information privacy law.

A focus on federalism can add to the analysis of even pathbreaking information privacy scholarship. Consider the recent work of Daniel Solove and Woodrow Hartzog regarding the role of the FTC.[4] Solove and Hartzog argue that the FTC creates "the primary regulation" for privacy in the United States through its settlement orders. As they state, these orders represent "the broadest and most influential force on information privacy in the United States." In my view, however, "the broadest and most influential force" for U.S. information privacy law is not the FTC, but the synergy resulting from the combination of federal and state law as well as of federal and state regulators. The lack of even a basic model that depicts the interplay of these joint regulatory forces is a central current gap in information privacy scholarship.

II. Information Privacy Federalism: Some Examples

In contrast to information privacy scholars, federalism scholars have deepened our understanding of the shifting parameters between the federal government and the states. Two examples will suffice. Judith Resnick has described the ongoing renegotiations of domains of authority by different regulators, state and federal, "as conflicts emerge about the import of rights and the content of jurisdictional allocations."[5] Cristina Rodríguez has emphasized the value of "decentralized ferment" in the national debate about immigration and other contested areas and depicted its value in managing social conflict across policy domains.[6]

At a minimum, the scholarship of information privacy requires a thick descriptive account of these federal and state law processes. Information privacy scholarship has ignored how federal and state law work together and the consequences of the existing "decentralized ferment." Yet, there are many examples of existing information privacy federalism. A descriptive account should consider statutory structures, overlapping administrative powers, and areas of exclusive state regulation.

---

[3] Scott Peppet, *Unraveling Privacy*, 105 Northwestern L. Rev. 1153 (2011); Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. Rev. 1701 (2010); Paul Ohm, *The Underwhelming Benefits of Big Data*, 161 U. Penn. L. Rev. Online 339 (2013).

[4] Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 Columbia L. Rev. 583 (2013).

[5] Judith Resnik, *Federalism(s)' Forms and Norms*, in Federalism and Subsidiarity: Nomos LV 363 (James Fleming & Jacob T. Levy, eds. 2014).

[6] Cristina Rodríguez, *Negotiating Conflict Through Federalism*, 123 Yale L.J. 2095, 2100 (2014).

A. Statutory Structures

1. *Data Security Breach Notification*. There are many federal and state requirements for data breach notification. In 2003, California became the first state to enact a data security breach notification law. Subsequently, another forty-six states have promulgated such statutes. In April 2014, Kentucky became the most recent state to enact such a law.

Data breach notification law does not merely rest on state law. Federal agencies have created such an obligation for financial institutions, and the HITECH Act imposed one of the entities it regulations. The GLB Act, enacted in 1999, does not explicitly require notification of data security incidents. In 2005, however, regulatory entities with authority under the GLB Act mandated that financial institution's information security programs include "a response program" for security breaches. As part of this response, the "Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice" called for notification for customers of financial institutions when misuse has occurred or is reasonably likely to occur.[7] Further federal regulation in this area came with the enactment of the HITECH Act in 2009, which amended HIPAA, the chief health care privacy law, to require notification in the event of a breach of "protected health information," or PHI. These obligations also extend to "business associates" of the directly regulated entity.

In summary, data breach notification began with the states, but quickly included a federal component. The federal reach is longer than one might initially consider. The GLB Act and HIPAA-HITECH sweep in entities, financial and health care companies, which account for a large percentage of U.S. economic activity. The result is overlap and interplay between state law and federal law that reaches widely both geographically (the many states laws) and in terms of the nation's GDP.

2. *Data Security.* Beyond data breach notification, there are substantive data security requirements set at federal and state levels. First, the GLB Act and HIPAA establish data security requirements for the organizations that fall under their jurisdictions. Second, and more broadly, FTC settlement orders establish data security requirements for commercial entities. These FTC enforcement actions penalize inadequate security even in the absence of breach or leak. As Solove and Hartzog demonstrate, FTC settlements codify FTC-enforced expectations with a resulting broad impact on the law of information privacy. The FTC is far from the only federal entity to enforce substantive requirements for data security. In Fall 2014, the Federal Communications Commission (FCC) announced plans to fine two carriers $10 million for failure to protect the security of personal information that they collected from customers. For the first time, the FCC identified a general duty to reasonably secure personal information in Section 222 of the Communications Act.

State laws also bolster and extend these federal security obligations. Approximately twenty-nine states mandate destruction of personal information in a safe

[7] 71 Federal Register 5779 (2006).

and effective fashion once there is no longer a business-related reason for its retention. Going beyond data disposal, California and Massachusetts require covered organizations to develop, implement and maintain reasonable information security programs. Under the Massachusetts law, an information security program must contain appropriate administrative, technical and physical safeguards, including encryption of personal data stored on laptops or other personal devices. Even if the organization holding the personal information is not itself located in these states, these statutes apply if the data identify residents of Massachusetts or California. Here, too, we see the creation of overlapping obligations. One out of eight residents of the U.S. lives in California, and, hence, businesses must carefully consider not only FTC or FCC data security standards, but also whether they process the personal information of a resident of the Golden State.

3. *Areas of Exclusive State Regulation.* There are also many areas in which only state privacy laws exist. Consider our automobiles, "computers on wheels," which now collect personal information. State laws create privacy rules for Event Data Recordings, which are the "black boxes" located in almost all automobiles. Beyond automobilies, another set of state laws establish privacy rules for the data processing of rental car agencies. State laws regulate the collection of information from Radio Frequency ID devices. State statutes also prohibit on certain use of personal information collected through supermarket club cards. In California, a specific statute, the Song-Beverly Act, regulates the kinds of information that retailers may collect from customers using a credit card.

B. Overlapping Administrative and Enforcement Powers

The rich landscape of federal and state information privacy is also marked by overlapping administration and enforcement. There is a varied structure that enables the kind of "multi-level politics" that Rodríguez has identified as a central element of contemporary federalism.[8] We have already seen examples involving the FTC and FCC in setting requirements for data security. There are also numerous information privacy statutes with shared enforcement by a government agency and state Attorney Generals. These include the CAN-SPAM Act, COPPA, FCRA, HIPAA, and the Telephone Consumer Protection Act. State Attorney Generals also coordinate their actions with each other. The National Association of Attorney Generals is a long-standing focal point for decision-making regarding joint action. As a single illustration of the weighty consequences of this interstate teamwork in enforcement, in November 2013, 37 states and the District of Columbia announced a $17 million settlement of claims against Google for the use of tracking cookies on Apple's Safari browser.

As a further example of the interplay of different governmental agencies, we can consider the GLB Act, an act generally viewed as without shared federal and state enforcement, and HIPPA, one that permits it. While the GLB Act grants an exclusive

[8] Rodríguez, *Negotiating Conflict*, supra, at 2124.

enforcement right to the FTC and other federal agencies, it also explicitly provides for non-preemption of state laws that are more protective of privacy. It assigns the FTC authority to decide which states have met this standard. The FTC has issued opinion letters that find state laws in Connecticut, Illinois, North Dakota, and Vermont to provide greater consumer protection than the GLB Act and, therefore, not to be preempted by it. This decision creates a carve-out for enforcement of stricter standards by a handful of state authorities. Outside of these states, financial institutions remain obliged to meet the requirements of the GLB Act and to face FTC enforcement. To this extent, therefore, even the GLB enables joint federal and state enforcement of its provisions through the enforcement by some states of higher standards within their own borders.

HIPPA also grants important authority to federal administrators in deciding the extent to which state law will be part of the landscape of health care privacy. In this area of information privacy law, Congress has not acted as a "primary source of federalism," as Abbe Gluck envisions its role within her paradigm of "National Federalism."[9] In particular, Congress proved unable to enact health care privacy guidelines pursuant to the deadline it originally set itself in HIPAA in 1996. Because Congress did not the date prescribed for enforcement of a health care privacy statute, authority passed to the Department of Health and Human Services (HHS) to create federal privacy law through rulemaking. The resulting HIPAA privacy and security guidelines from the HHS are not the consequence of a congressional strategy for federalism. Rather, the shift in power from Capitol Hill to the HHS and within HHS to the Office of Civil Rights. (OCR) is a consequence of gridlock, pure and simple.

The contours of the administrative role pursuant to HIPAA merit at least brief description. The most important regulation under HIPAA for privacy and preemption purposes is the Privacy Rule, as amended most recently in 2013 by the final omnibus HIPAA Rule. HIPAA's Subtitle F contains a general preemption of any "contrary" provision of state law followed by exemptions for public health and health regulatory reporting. It also permits the granting of exceptions for state laws that are "necessary" for certain enumerated purposes or relate to controlled substances. Finally, it contains a specific exception for state laws that are "more stringent" than the HIPAA standards.[10]

---

[9] Abbe R. Gluck, *Our [National] Federalism*, 123 Yale L.J. 1996, 1997 (2014).

[10] The OCR is the key administrator of this part of HIPAA. A state law is "contrary" to HIPAA if it is "impossible to comply with both the State and federal requirements"; or the state law provision stands as obstacle to the purposes of the federal law. As for the concept of a state law that is "more stringent" than federal law, HIPAA itself does not further define the phrase. 45 C.F.R. § 160.203. To fill this gap, the Privacy Rule, as drafted by the OCR, provides highly detailed specifications. Thus, a state law is more stringent if it prohibits or restricts a use or disclosure that the Privacy Rule would allow. A state law that permits greater individual rights of access or amendment than the Privacy Rule is more stringent. A state law that requires a greater amount of information to be provided to an individual about use of their information or their rights and remedies is more stringent.

II. A Theory of Information Privacy Federalism?

The digital economy is a national one. Indeed, as the European Union is discovering, it is in many regards a global phenomenon, and one for which regulation even at the national level can prove problematic. Is it possible that the patchwork of privacy and security law, federal and state, in the United States offers normative advantages? Is there a positive case for a joint federal-state system of information privacy law? Or are there only lessons to be identified for minimizing the harm from a hodge-podge of second-best solutions? In that case, perhaps the best use of scholarly energy would be to make a case for Congressional action and preemptive federal legislation in an overarching, or "omnibus," statute.

There are now forty-seven data security laws, twenty-nine data disposal laws, and multiple statutes that permit enforcement by both federal agencies and state AG's. Courts play an important role in deciding when and the extent to which existing federal laws apply.[11] In some areas, moreover, only state rules exist, and individual state legislatures continue to enact privacy statutes. In 2014, a relatively quiet year for privacy legislation in California, several notable new laws were enacted or came into effect. These include a "Do Not Track" disclosure requirement for websites; an online "eraser" law for children; and an expansion of state data breach notification law to include a "user name or email address, in combination with a password or security question and answer that would permit access to an online account."

In one view, if there is to be regulation of an area of national economic activity, it should be through national legislation. In this light, consider Chief Justice's Marshall's opinion in *Gibbons v. Ogden* (1824). That case assessed the relative power of a state and Congress to regulate pursuant to the commerce clause. It concerned an important technology of the early 19th Century America, namely, steamboats, and the authority of New York State to grant exclusive rights to operate such vessels in its waters.

For the *Gibbons* Court, the navigable waters of New York raised legal concerns that went beyond "the internal commerce" of the state. As Marshall wrote for the Court: "[The] deep streams which penetrate our country in every direction, pass

---

[11] HIPPA permits a role for state courts in deciding whether laws that are contrary to HIPAA are also more stringent. For example, a Connecticut court determined in 2006 that a state law that provided a private right of action was preempted by HIPAA, which lacks any such interest. The Connecticut law in question was not one aimed at regulating the privacy of health care information, and hence did not fall under an exception to the HIPAA preemption rule. *Fisher v. Yale Univ.*, No. X10NNHCV044003207S, 2006 WL 1075035 (Conn. Super. Ct., Apr. 3, 2006). In contrast, a court upheld a Louisiana law that limits the ability of the health care provider to release records to anyone other than the patient without the patient's consent. This law allowed grater rights of access or amendment to individual records than HIPAA and, hence, the state law was not preempted. *U.S. ex rel. Stewart v. Louisiana Clinic*, No. 99-1767, 2002 WL 31819130 (E.D. La., Dec. 12, 2002).

through the interior of almost every State in the Union, and furnish the means of exercising this right." By "this right," Marshall meant the interest in operating a vessel in New York, which the state had exclusively granted to Fulton and Livingston, who then offered a license to Ogden.[12] The *Gibbons* Court ruled that the New York law violated the Supremacy Clause and was therefore void. As a consequence of the linkage of the "deep streams," the rivers and other bodies of water of the country, New York's exclusive grant of authority to operate steamboats in its coastal waters impinged upon Congress' statutory licensing of ferries in "coasting trade." In its conclusion, the Court went so far to state: "If Congress has the power to regulate it, that power must be exercised whenever the subject exists . . ."

The deep streams of the 21st Century in the United States are not the Hudson River and the Erie, Oswego, Champlain and Cayuga-Seneca canals. Rather, the Internet and other advanced telecommunication networks provide the essential paths of commerce today. Business enterprises gather and send data due to these new facilities in ways that grow the economy and lead to violations of data privacy and security. One might view information privacy as more than an area in which Congress can regulate, or should regulate, but perhaps in which it *must* regulate.

For a European perspective, Johannes Masing, a member of Germany's Federal Constitutional Court, has helpful views regarding the need for both centralization and subsidiarity in law. Although Masing is a Euro-skeptic regarding privacy law, or data protection law as it is called in the E.U., he accepts the need for some "uniform standards."[13] Writing in the *Neue Juristische Wochenschrift*, a leading German law review, Masing conceded an end to the age in which a single European state would regulate information privacy law for itself. In particular, he observed, "[f]or international Internet Providers, it was not a realistic perspective to be obliged to follow different rules for the same service in each country." At the same time, Masing argued, "A full centralization of data protection would be contra-productive to the development of a differentiated instrument" for discovery and testing of different solutions.[14]

In the United States, companies face different rules for the same services in different states. The Masing question remains unresolved in both EU and U.S. law: to what extent should privacy law be uniform, within national or even surpa-national jurisdictions, and to what extent should it remain decentralized? Even if there is to be some decentralization, moreover, a necessary goal might be improvements in the systematic process for consolidation of results from different regulatory experiments in the states as "laboratories." In his famous dissent in *New State Ice*, Brandeis praised "the value of the process of trial and error." In privacy and security law in the U.S., there is ample evidence of both experiments and error. There is less proof of consolidation of

---

[12] A New York court had enjoined Gibbons from operating steamboats in the state.
[13] Johannes Masing, *Herausforderungen des Datenschutzes*, 32 Neu Juristische Wochenschrift 2305, 2310 (2012).
[14] Id. at 2311.

lessons learned, whether by the states amending their laws around new models, or through federal legislation that builds on the best state examples.

One possible prism for viewing these issues is through the literature regarding collective action. My colleague Robert Cooter and Neil Siegel argue that as a larger number of states are obliged to work together to solve a problem, the larger the costs of cooperation become, and the greater the chances of failure.[15] Such pathology would favor national solutions for information privacy. To be sure, states sometimes fail to cooperate on information privacy, as demonstrated by the failure to adopt uniform legislation for data breach notification or uniform state versions of health privacy legislation. At the same time, state attorney generals have a strong record of collaboration on enforcement actions pursuant to their authority under a number of federal laws and through state mini-FTC Acts. Sometimes state cooperation can be the norm.

In addition to the existence of coordination problems, Cooter and Siegel worry about a race to the bottom as interstate externalities and national markets contribute to collection action pathologies. Here the Cooter-Siegel brand of federalism suggests a pattern that does not exist in information privacy law. In their interpretation of the internal logic of federalism, Cooter and Siegel are worried about a state shifting the costs of their action on their neighbor. Their paradigmatic act is one not taken: the decision not to place a tax or other cost on industry for some beneficial purpose. This inaction becomes particularly tempting if the costs of inaction, such as in certain kinds of pollution, are shared at least in part by neighboring states.

Yet, some states have acted and imposed higher information privacy standards than other states. States have chosen to, as Cooter and Siegel put it, "disadvantage their industries by imposing higher . . . standards."[16] Moreover, only some privacy and security laws are capable of leading to net savings to residents. For example, data breach notification laws and data security laws might work to reduce the overall cost of identity theft. There is no proof, however, that these states craft these statutes with an eye to providing an efficient amount of security. Indeed, in many instances, these statutes lead to an over-notification of security incidents. Other privacy laws are even more difficult to justify in terms of cost savings to state residents as they arguably prevent efficiencies in market differentiation or segmentation.

At a minimum, information privacy law scholars must confront the rich landscape of federalism that exists in this area. As Aziz Huq proposes as a general requirement, the need is "for more retail analysis of specific institutional parameters and

---

[15] Robert D. Cooter & Neil S. Siegel, *Collective Action Federalism*, 63 Stan. L. Rev. 115, 140 (2010). As they state, "the holdout problem makes the probability of cooperation fall with the number of actors who must cooperate."

[16] Id. at 168.

dynamics within the institutional forms of federalism."[17] Huq proposes that collective action is "an unruly and diverse collection of dynamics."[18] The goal of any work concerning information privacy federalism must be, as Huq argues, to analyze this policy area with attention to "the incentives, investments and strategic options of each state participant within whatever logic of collective action is at work." The difficulty in information privacy law is that there are so many different kinds of state participation that any scholarship will end by being less a taxonomy than a laundry list.

III. Comparative Law

As my chapter, *The Value of Information Privacy Federalism* indicates, jurisdictions outside the United States are wrestling with the same kinds of regulatory choices for personal data use. In the E.U., the Draft Data Protection Regulation shows a strong move to centralization of the law.[19] This controversial development shows the E.U. moving in the opposite direction from the US, where decentralization remains the modus operandi.

The E.U. developments also demonstrate possible advantages of the US approach. To point to just one, the Draft Regulation handles some of the thorniest issues in information privacy law at a high level of generality and abstraction. An example would be rules for when data processing is permissible. At least until the Commission offers further specifications in its "delegated" and "implementing" acts as well as through its use of the "consistency mechanism," Member States will interpret these provisions in light of their existing national data protection rules.[20] The result will not lead to greater uniformity of regulation throughout the E.U., but will only heighten regulatory uncertainty.

As a final observation, and one that turns to a different jurisdiction, Canada has a well-developed system of privacy federalism. Its Personal Information Protection and Electronic Documents Act (PIPEDA), enacted in 2000, is a European-style "omnibus" privacy law that regulates the private and public sector alike. Canada also permits PIPEDA to be displaced by provincial laws that are "substantially similar" to it. The law assigns authority to make this finding to the Governor in Council, legal adjunct to the federal cabinet, with recommendations from the Ministry of Industry and the Privacy Commissioner of Canada. The three provinces with omnibus privacy laws for the private sector have all received exemptions. This federal process has also found that

---

[17] Aziz Huq, *Does the Logic of Collective Action Explain Federalism Doctrine?* 66 Stanford L. Rev. 217, 258 (2013).

[18] Id. at 242 (emphasis removed). Indeed, on first review at least, the kinds of interactions present in the creation and administration of information privacy law appear sufficiently diverse to fit into any single of Huq's five-part (partial) taxonomy of collective action in federalism.

[19] See Paul M. Schwartz, The US-E.U. Privacy Collision, 126 Harv. L. Rev. 1966 (2013). For further criticism of it on these grounds, see Alexander Rossnagel, *War wird aus der Datenschutzgrundverordnung?*, Zeitschrift für Datenschutz 545 (2014).

[20] Schwartz, US-E.U. Privacy Collision, at 1998.

a sectoral privacy law in Ontario from 2004, the Personal Health Information Protection Act, met PIPEDA's standards.

At a minimum, there are lessons to be learned from Canada regarding consolidation of experiments under a federal system. PIPEDA provides an incentive for the provinces to enact omnibus and sectoral laws that follow it, but also allows innovation by permitting "substantially similar" statutes to displace it. Moreover, the Canadian path for privacy innovation is no one-way street. Through a five-year review process embedded in PIPEDA, the Parliament permits itself an opportunity to draw lessons from the second-generation privacy laws of the provinces in considering new legislative amendments.