Testimony

Paul M. Schwartz
Jefferson E. Peyser Professor
Berkeley Law School, University of California, Berkeley

Balancing Privacy and Opportunity in the Internet Age
An Informational Hearing of the Assembly Judiciary Committee, the Assembly Business, Professions & Consumer Protection Committee, and the Assembly Select Committee on Privacy
December 12, 2013
The Louis B. Mayer Theater at Santa Clara University

Thank you, Members of the Assembly, for the honor of speaking with you today about information privacy law. This is a topic about which I have been writing and teaching for over two decades. In Appendix A, I include information about my background in privacy law, including a selected biography.

Today, I wish to talk to you about the "California Effect," the long-standing impact of California legislation in many areas and how legislative dysfunction in Washington, D.C. should encourage us to think differently about it. I will then suggest areas in which the California Legislature should act, albeit with caution and care**.** In my view, there should be a consideration and consolidation of current laws based on lessons learned. I suggest two such statutes in this regard, the Song-Beverly Act and the Confidentiality of Medical Information Act (CMIA). Finally, the entire country and indeed the world are now vitally concerned with California privacy law. Yet, the record of committee hearings and legislative history is far from optimal at present. Legislative action in this area should draw on 21st Century information technology.

I.

There is a rich academic literature concerning the interplay between federal and state government regulation in the United States. This scholarship has documented a "California Effect."[1] This term refers to the significance of legislation in California in different policy areas. Yet, the California Effect is traditionally part of a regulatory cycle in which initial state action is often followed by federal action.

In a classic paper from 1985, Donald Elliot, Bruce Ackerman, and John Millian proposed an evolutionary model of federal and state statutory law.[2] In their paradigm, an important middle period in the regulatory lifecycle involves the flight by regulated entities to Washington, D.C. in search of reform. These entities seek to counter successes at the state level as well as to optimize state laws in different jurisdictions by seeking preemptive lawmaking at the federal level. J.R. DeShazo and Jody Freeman have termed termed this shift to regulation from Washington, D.C.,

[1] Anu Bradford, The Brussels Effect, 107 Northwestern Law Review 1, 5 (2012).
[2] E. Donald Elliott, Bruce Ackerman & John C. Millian, Toward a Theory of Statutory Evolution: The Federalization of Environmental Law, 1 J.L. Econ. & Org. 313 (1985).

"defensive preemption."[3] As DeShazo and Freeman point out, state-level regulations can motivate organizations to demand federal lawmaking. Some of the resulting federal statutes preempt state law, in whole or in part; some also permit enforcement activity to be shared among federal and state regulators.

Information privacy has long benefitted from this kind of federal-state interplay. There has also been a noticeable lack of gridlock at the state sectoral level. If one examines merely the website of the California Office of Information Security and Privacy Protection, one finds a long list of privacy legislation enacted in 2013 and in recent past years.[4] Like environmental law, privacy is a fertile area for politicians, private advocates, and non-governmental organizations to engage in policy entrepreneurship.

The results of this dynamic between federal and state law have been complex. One of the most interesting regulatory models for privacy is the Fair Credit Reporting Act (FCRA), which has contained partial sunsets for certain provisions as well as partial preemption of state law. As amended by FACTA, FCRA now limits the assignment of federal power in certain areas only to behavior mandated by the law, while allowing the states to engage in further regulation regarding a larger subject area.[5] This kind of federal action creates an element of certainty for regulators and regulated entities while also leaving open the possibility for future regulatory innovations by the state.

The difficulty at present, however, is that the federal legislative process appears to be broken. It is a victim of the larger dysfunction in the Capitol about which there is no need to elaborate today. The old question concerned the proper respective roles for federal and state legislatures in collaborative federalism. Today, the California legislature should consider how to act when a federal legislative reaction is unlikely to be forthcoming.

Before answering this new question, I wish to note, as a necessary nuance, that all parts of the federal legal process for privacy do not demonstrate inaction. First, the Federal Trade Commission makes vigorous use of its powers under the Federal Trade Commission Act as well as its authority pursuant to privacy statutes, including the Children's Online Privacy Protection Act, Gramm-Leach-Bliley Act, Telemarketing and Consumer Fraud Protection Act, and Fair Credit Reporting Act.[6] Second, the Department of Commerce's National Telecommunications and Information Administration has begun a promising privacy multi-stake holder process. It seeks to develop legally enforceable codes of conduct that build on the Obama Administration's Consumer Bill of Rights.[7]

---

[3] J.R. DeShazo & Jody Freeman, Timing and Form of Federal Regulation: The Case of Climate Change, 155 U. Pa. L. Rev 1499 (2007).

[4] State of California Department of Justice, Office of the Attorney General, 2013 Privacy Legislation Enacted, http://oag.ca.gov/privacy/privacy-legislation/leg2013.

[5] For a discussion, see Paul M. Schwartz, Preemption and Privacy, 118 Yale L.J. 902, 943-44 (2009).

[6] The FTC's role in developing a new kind of "common law" of privacy is analyzed by Daniel Solove and Woodrow Hartzog, The FTC and the New Common Law of Privacy, 114 Columbia Law Review -- (forthcoming 2014).

[7] See NTIA, Privacy Multistakeholder Process: Mobile Application Transparency, at http://www.ntia.doc.gov/other-publication/2013/privacy-multistakeholder-process-mobile-application-transparency

Nonetheless, the traditional federal-state privacy model is missing a necessary component due to the likely absence of federal *legislative* inputs into the process. This raises the issue of a proper response from state legislatures in the face of Congressional inaction.

One is reminded of the immortal dialogue at the end of WAITING FOR GODOT:

VLADIMIR:
Well? Shall we go?

ESTRAGON:
Yes, let's go.
They do not move.

To act or not to act? To legislate or not?

II.

My recommendation to the California Assembly would be against waiting for Godot. It should take action, but be carefully in how it acts. This extra care is needed due to the absence of the kinds of negotiations, corrections, and further developments that follow from federal involvement in the privacy area.

The California Assembly should remain engaged in this area. We live in a world shaped by technology and fueled by personal information. Information privacy matters profoundly: our everyday activities involve the creation and transfer of personal information to an extent previously unknown. This information is also the fuel of the modern economy, and the rules for its use profoundly affect key tech companies, many of whom are located in our state.

The world also now looks to California privacy law. Our state is the world's ninth largest economy. In the global digital economy, commercial transactions with California residents are a "must" for companies located throughout the United States and across the globe. Moreover, European regulators are concerned about the vigor of privacy safeguards in the United States. Efficient and effective privacy law in California has the potential to make a significant contribution to the international dialogue. Indeed, California's data breach law, enacted in 2002, has proved a model not only for other states, but for the world. As just one example of this influence, Articles 31 and 32 of the European Union's Proposed Draft Regulation on Data Protection adopts this California innovation and mandates data breach notification within European Member States.[8]

If the California Legislature is to act, there are two ideal areas for activity. First, it should adopt a program of consolidation and amendment of existing privacy statutes. Now is a perfect time for stock-taking and consideration of lessons from ongoing experience. Second, and in light of

[8] Proposal for a Regulation of the European Parliament and of the Council – on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (Proposed Data Protection Regulation), (Jan. 25, 2012). The EU has also adopted data breach notification requirements through its Commission Regulation (EU) No 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications.

California's national and international role in privacy law, it is time to evaluate how it records and documents its legislative process. California law is just that important and the costs of these documentary improvements, due to digital technology, should be modest.

A.

Regarding the consolidation, I would like to point to two areas of legislation that might be revisited: (1) the Song-Beverly Credit Card Act; and (2) the Confidentiality of Medical Information Act. To be sure, amendment might be useful in other areas as well. I am confident, moreover, that involvement of stakeholders by the Legislature will permit identification of such other areas-- and ones of possible broad agreement.

1. The Song-Beverly Credit Card Act. Regarding the Song-Beverly Act, this statute, first enacted in 1971, represents a broad effort to provide consumer protection in the use of credit cards. The law provides a private right of action, which has caused significant litigation about its language. Of particular centrality for privacy is its Section 1747.08, which prohibits companies that accept credit cards in business from requiring the cardholder to provide "personal identification information." The Act defines personal identification information as "information concerning the cardholder … including, but not limited to, the cardholder's address and telephone number."[9]

Beyond the language in Section 1747.08, however, the Song-Beverly Act also acknowledges a retailer's interest in promoting data security and preventing card fraud. The statute does permit collection of additional information from cardholders under certain conditions. For example, it allows the collection of ZIP code information at fuel dispensers in gas station to block a specific way that stolen credit cards can be used.[10]

The problem is that the law, now forty-two years old, is in need of legislative remodeling for the modern information age. The California Supreme Court has helped in this regard, but at high cost to litigants and through a judicial process that necessarily only decides the specific question before the state's high court. Allow me briefly to discuss two examples of recent judicial decisions about this statute.

In *Pineda v. Williams-Sonoma Stores, Inc.* (2011), the California Supreme Court found that a ZIP Code constituted "personal identification information" within the meaning of the statute.[11] The *Pineda* Court held that the Song-Beverly Act prohibited a retailer from requesting or recording this information. In *Apple Inc. v. Superior Court* (2013), the California Supreme Court then decided that the Act did not prohibit an online retailer from requesting or requiring personal identification information from a customer as a condition to accepting a credit card payment for an electronically downloadable product.[12] After a careful reading of the legislative language, Justice Goodwin Liu concluded for the California High Court that the applicable section did not govern these type of transactions.[13] In his opinion, Justice Liu further observed that the Song-Beverly Act intended to balance privacy protection with the need to safeguard against fraud and identity theft.[14]

---

[9] California Civil Code, 1747.08(b).
[10] Id. at 1747.08(c)(B).
[11] Pineda v. Williams-Sonoma Stores, Inc., 246 P.3d 162 (Cal. 2011).
[12] Apple Inc. v. Superior Court, 292 P.3d 883 (Cal. 2013).
[13] Id. at 885.
[14] Id. at 889.

The Legislature would be wise to revisit this law to be more explicit about how it permits retailers to use and record personal identification information to prevent fraud and identity theft. These goals, as Justice Liu notes, serve the interests not only of retailers but of consumers.[15]

2. The Confidentiality of Medical Information Act (CMIA). The CMIA has been termed "California's general health information privacy law."[16] It applies to health care providers, health care service plans, and certain contractors. This law prohibits the use or disclosure of health information "for any purpose not necessary to provision of health care services to the patient" unless the individual authorizes it or the statute otherwise permits it.[17]

The CMIA is quite specific about the form of its required notice for a valid authorization. It is less clear as to its broad prohibition on the use of "medical information for any purpose not necessary to provide health care services to the patient."[18] There are a variety of uses of information that may not be directly related to the provision of health care services to a patient, but that fall within normal operations of a modern health care entity, including its risk management operations.

Moreover, federal health care privacy law has been in a state of development, and one that the CMIA does not reflect. The HITECH Act of 2009 has been followed by the issuance of the final omnibus HIPAA Regulations in 2013.[19] Currently, however, the CMIA and its required authorization notices exist as a kind of lonely island within the larger HIPAA framework for notices. This isolation has the potential to lead to enforcement actions for companies centered on technical issues not directly related to harms that flow from privacy violations. The Legislature would be well advised to compare CMIA's safeguards with those found in HIPAA. It may be possible to streamline the California requirements where they are simply duplicative or add an unnecessary overlay of bureaucratic technicalities to federal protections.

B.

My final point relates to California's important role in information privacy law. Attorneys and policy-makers from all over the world are vitally concerned with California legal developments. Yet, legislative material from our state is not available to the same extent and in the same form as federal legislative material. Just last week, a leading global privacy lawyer, based in Washington, D.C., but speaking with me during a business trip in Europe, bemoaned the lack of legislative material regarding key issues about the California data breach notification statute of 2002. We spoke to each other on our cellphones as he took a high speed train from one EU country to the next.

The Legislature should join this new communications age. To be sure, one can divine some aspects of the path of California legislation by comparing different versions of bills. Yet, digital technology and transcription technology now make it possible to publish legislative history and

---

[15] Id.
[16] Paul T. Smith, Health Information Privacy, Business Law: Privacy and Compliance Litigation in California § 7.4 (2013).
[17] Civil Code § 56.10(a).
[18] Id.
[19] Department of Health and Human Services, Final Omnibus HIPAA Rule, 78 Federal Registrar 5566 (Jan. 25, 2013).

committee hearings at a low cost. Legislative hearings should also be designed to collect the kinds of evidence that the Legislature needs to make its decisions. As a single example, in revisiting the Song-Beverly Act, it might collect data on the antifraud function served by collection of personal identification information.[20]

***** *****

Thank you again for the chance to participate in today's hearing. It has been an honor for me to speak with you.

[20] See Apple Inc. v. Superior Court, 292 P.3d 883, 905 (Cal. 2013)(Baxter, J., dissenting).

Appendix A

Biographical Information

Paul Schwartz is a leading international expert on information privacy law. He is the Jefferson E. Peyser Professor at UC Berkeley School of Law and a Director of the Berkeley Center for Law and Technology. Schwartz is also a Senior Advisor at Paul Hastings, where he works in the Privacy and Data Security Practice.

Schwartz has testified before Congress and served as an advisor to the Commission of the European Union and other international organizations. He assists numerous corporations and international organizations with regulatory, policy, and governance issues relating to information privacy. He is a frequent speaker at technology conferences and corporate events in the United States and abroad.

Schwartz is the author of many books, including the leading casebook, Information Privacy Law, and the distilled guide, Privacy Law Fundamentals, each with Daniel Solove. Information Privacy Law, now in its fourth edition, is used in courses at more than twenty law schools. Schwartz's over fifty articles have appeared in journals such as the Harvard Law Review, Yale Law Journal, Stanford Law Review, and Chicago Law Review. Fluent in German, he contributes to German legal reviews. Schwartz publishes on a wide array of topics including data analytics, telecommunications surveillance, data security breaches, health care privacy, privacy governance, data mining, financial privacy, European data privacy law, and comparative privacy law.

Schwartz is co-reporter of the American Law Institute's Restatement of Privacy Law Principles. He is a past recipient of the Berlin Prize Fellowship at the American Academy in Berlin and a Research Fellowship at the German Marshall Fund in Brussels. Schwartz is also a recipient of grants from the Alexander von Humboldt Foundation, Fulbright Foundation, the German Academic Exchange, and the Harry Frank Guggenheim Foundation. He is a member of the organizing committee of the Privacy Law Salon and of the American Law Institute.

Schwartz belongs to the Editorial Boards of International Data Privacy Law, the International Journal of Law and Information Technology, and the Zeitschrift für Datenschutz (Data Protection Journal). He is a graduate of Yale Law School, where he served as a senior editor of the Yale Law Journal, and Brown University.

Selected Recent Publications

Books

PRIVACY LAW FUNDAMENTALS
(IAPP 2013) with Daniel Solove

A distilled guide, Privacy Law Fundamentals provides the essential elements of privacy law at your fingertips. It includes: an introductory chapter summarizing key new developments, analysis of

leading cases, numerous charts and tables, summaries of key state privacy laws, an overview of FTC enforcement actions, and answers to frequently asked privacy questions.

INFORMATION PRIVACY LAW
(Aspen Publishers, 4th ed. 2011) with Daniel Solove

This book surveys the field of information privacy law, with excerpts from the leading cases and scholarship. It covers privacy issues involving the media, health and genetic privacy, law enforcement, freedom of association, anonymity, identification, computers, records, cyberspace, home, school, workplace, and international privacy.

Articles, Essays & Chapters

Reconciling Personal Information in the U.S. and EU,
102 California Law Review — (forthcoming 2014) with Daniel Solove

The EU-US Privacy Collision: A Turn to Institutions and Procedures,
126 Harvard Law Review 1966 (2013)

Information Privacy in the Cloud,
161 University of Pennsylvania Law Review 1623 (2013)

EU Privacy and the Cloud: Consent and Jurisdiction Under the Proposed Regulation, 12 PVLR 718 (Apr. 28, 2013)

Systematic Government Access to Private-Sector Data in Germany,
2 International Data Privacy Law 289 (2012)

The PII Problem: Privacy and a New Concept of Personally Identifiable Information, 86 N.Y.U. Law Review 1814 (2011) with Daniel Solove

Regulating Governmental Data Mining in the United States and Germany: Constitutional Courts, the State, and New Technology, 53 William & Mary Law Review 351 (2011)

Shorter works

Blog, What Is Personally Identifiable Information (PII)? Finding Common Ground in the EU and US, Concurring Opinions (June 26, 2013) with Daniel Solove

Reforming the concept of personally identified information: U.S. privacy law and PII 2.0 (with Daniel Solove), in Neue Regulierungsschub im Datenschutzrecht? 55 (Rolf H. Weber & Florent Thouvenin, eds.), Schulthess Verlag (Switzerland)(2012).

Op ed, Privacy Firsts at Berkeley Law, San Francisco Chronicle (Feb. 25, 2012)

Blog, PII 2.0, Technology | Policy | Academics (Jan. 16, 2012) with Daniel Solove

Blog, Google Ngram and Information Privacy, Google Policy by the Numbers (Jan. 9, 2012) with Daniel Solove

PII 2.0: Privacy and a New Approach to Personal Information, Privacy and Security Law Report, 11 PVLR 142 (January 23, 2012) with Daniel Solove

For more publications of mine, see http://paulschwartz.net/?page_id=12