THE RECORDER
ESSENTIAL CALIFORNIA LEGAL CONTENT

In Practice: The 'California Effect' on Privacy Law

By Paul M. Schwartz

January 2, 2014

Paul Schwartz, Berkeley Law School

California has been a leader in information privacy law for decades. State legislation from the Golden State influences other states, federal lawmakers in Washington, and the world.

A sterling example of the "California Effect" is the state's data breach notification legislation. First passed in Sacramento in 2002, breach notification laws have now been enacted by another 45 states. In the HITECH Act in 2009, federal lawmakers adopted this idea for health care information.

Data breach notification has also gone global. In June 2013, the European Union created a narrow data breach notification obligation for telecommunication companies and Internet service providers. The EU's Proposed Draft Regulation on Data Protection would broadly adopt this California innovation and mandate data breach notification for data processing organizations in its member states.

Today, however, the traditional federal-state privacy model is missing a necessary component due to the likely absence of federal legislative inputs into the process. Traditionally, the California Effect formed only a first stage in a regulatory cycle. After state action, a "flight to Washington" would see federal lawmakers' correcting and improving initial state efforts at regulation. Over time, Washington lawmakers in the privacy realm developed a rich toolkit of lawmaking techniques, including different kinds of preemption and a sharing of federal and state enforcement activities.

The difficulty now is that the federal legislative process for privacy appears broken. It is a victim of the larger dysfunction in the Capitol. The 112th Congress enacted the lowest amount of bills since

comprehensive statistics on federal legislative activity began to be kept in 1947. By this measure, the most recent Congress was, in fact, the least productive one in modern history.

In the face of silence from the nation's Capitol, the state legislatures, in California and elsewhere, should not wait for the federal Godot.

***

We live in a world shaped by technology and fueled by personal information. Personal privacy matters profoundly: Our everyday activities involve the creation and transfer of personal information to an extent previously unknown. Personal information is also the fuel of the modern economy, and the rules for its use profoundly affect key tech companies, many of which are located in California.

Furthermore, the world 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.

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. After an active privacy lawmaking session in the fall of 2013, now is a perfect time to take stock and consider lessons from ongoing experience.

Two examples come immediately to mind. The first is the Song-Beverly Credit Card Act; the second, the Confidentiality of Medical Information Act (CMIA).

The Song-Beverly Act statute, first enacted in 1971 and subsequently amended, represents a broad effort to provide consumer protection in the use of credit cards. The law also provides a private right of action, which has spurred significant litigation about its language. Regarding privacy, the Act prohibits companies that accept credit cards in business from requiring the cardholder to provide "personal identification information."

Beyond this section, the Song-Beverly Act also permits collection of additional information from cardholders under certain conditions because of a retailer's interest in promoting data security and preventing card fraud. For example, it allows the collection of ZIP code information at fuel dispensers in gas stations to block use of stolen credit cards.

This law, now 42 years old, is in need of legislative remodeling for the modern information age. In revisiting it, the state Legislature would be wise to be more explicit about how retailers may use and record personal identification information to prevent fraud and identity theft. As a start, retailers should be allowed to request reasonable, additional information for the prevention of fraud and identity theft, but should be prevented from using this information for unwarranted marketing.

As for a second statute that should be revisited, the CMIA has been termed "California's general health information privacy law." It applies to health care providers, health care service plans, and certain kinds of contractors. It 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.

The CMIA is less than clear, however, as to when use of medical information is not "necessary" for providing patient health care services. There are a variety of uses of information that may not be directly tied 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 rapid state of development since the initial enactment of the CMIA in 1981. A new set of comprehensive federal regulations, issued pursuant to the Health Insurance Portability and Accountability Act (HIPAA), has recently been released. Yet, the CMIA and its required authorization notices exist as a kind of lonely island within the larger HIPAA framework for patient notices. The California Legislature should carefully compare the CMIA's safeguards with those found in federal law. It should streamline the California requirements where they are simply duplicative or where they add an unnecessary overlay of bureaucratic technicalities to federal protections.

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

Recently, 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. We spoke to each other on our cellphones as he took a high-speed train from one EU country to the next. It is time for the California Legislature to join this new communication age and create legislative and legal material, including records of hearings, that will provide vitally important information for privacy lawyers all over the world.

Paul M. Schwartz is the Jefferson E. Peyser Professor of Law at Berkeley Law School and a special advisor to the Privacy and Data Security Practice at Paul Hastings. He can be contacted at paulschwartz@paulhastings.com.

In Practice articles inform readers on developments in substantive law, practice issues or law firm management. Contact Greg Mitchell with submissions or questions at gmitchell@alm.com.

Read more:
http://www.law.com/jsp/ca/PubArticleCA.jsp?id=1202635738034&In_Practice_The_California_Effect_on_Privacy_Law#ixzz2pMcyFT6O