

Inching toward consensus: A roundup of U.S. privacy legislation

08.29.2011



By Jay Cline, CIPP

The prospects for major new privacy regulation emerging from the U.S. Congress during the remainder of the current session continue to be elusive. In spite of privacy's status as the rare bipartisan issue, its span across multiple committee jurisdictions and agencies; lack of any national emergency, and absence of a concerted interest group pose significant obstacles to any broad-based privacy bill. As a result, the most likely developments in the coming year will be a national standard for data breach notification, rulemaking by federal agencies and narrowly targeted bills or amendments at the federal and state levels.

The U.S. Congress can be a legislative graveyard where the vast majority of bills die for lack of broad and deep support. The privacy docket of the 112th Congress—saddled with multiple wars, economic uncertainty and an impending election season—will fight an uphill battle to become an exception to this rule.

The most likely breakthrough continues to appear to be a common national standard for data breach notification. Such a standard, in principle, has long garnered industry support as a way to reduce legal and operational fees. Companies operating across the 50 states seek one definition of what constitutes a data breach; what level of data protection qualifies as a safe harbor to exempt the need to notify affected individuals; one approach toward notifying state attorneys general, and one approach toward remedying affected individuals.

"Data security breach legislation is most likely to be enacted this Congress of all of the bills," Stu Ingis, Washington, DC-based partner at [Venable LLP](#), tells *The Privacy Advisor*.

"The issue and the bills have matured to the point where a law is feasible and consensus is emerging among regulators and the impacted businesses," he adds.

Toward that end, on June 7, Senator Patrick Leahy (D-VT) reintroduced for the fourth time the Personal Data Privacy and Security Act ([S. 1151](#)), which would supersede or "preempt" state data breach notification laws. Federal preemption of state laws has often been cited by observers as necessary for achieving one national standard for data breach notification. The Senate Judiciary Committee is the next stop for this bill. A week later, Sens. Jay Rockefeller (D-WV) and Mark Pryor (D-AR) reintroduced the Data Security and Breach Notification Act of 2011 ([S. 1207](#)), which has been referred to the Senate Commerce Committee. In addition to establishing data breach notification standards, it requires covered entities to establish information security policies; appoint security

officers; conduct risk assessments, and remediate vulnerabilities, in language that harkens to the Gramm-Leach-Bliley Security Rule.

On July 19, Rep. Mary Bono Mack (R-CA) introduced the Secure and Fortify Electronic (SAFE) Data Act ([H.R. 2577](#)) in the U.S. House of Representatives, where it has moved on to the full Energy and Commerce Committee. Like its Senate counterparts, the bill includes federal preemption of state laws. It also establishes minimum data security and data minimization requirements. The act's requirement to notify affected individuals "not later than 48 hours after" determining who those individuals are has encountered universal industry opposition, however, and promises a future path of continued changes.

Mobile device privacy and the protection of location-based and online data is the next-most-likely area to see a break in the logjam. Companion bills on this topic have been introduced in both houses, and the work of a new Senate subcommittee has given heightened visibility and legislative momentum to the bills.

On June 14 and 15, respectively, Reps. Jason Chaffetz (R-UT) and Bob Goodlatte (R-VA) introduced H.R. 2168, while Sen. Ron Wyden (D-OR) introduced S. 1212. The bills require mobile device service providers to gain consumer consent before sharing their geo-location data with third parties. The companion bills also mandate that law enforcement obtain a warrant before accessing geo-location data.

The next day, on June 16, Sens. Al Franken (D-MN) and Richard Blumenthal (D-CT) introduced S. 1223, the Location Privacy Protection Act of 2011. Like the aforementioned bills, the act would amend the Electronic Communications Privacy Act (ECPA) by requiring mobile service providers to obtain express consent before collection or sharing geo-location data collected from consumers.

In May, Sen. Rockefeller introduced the Do-Not-Track Online Act of 2011 ([S. 913](#)), which directs the Federal Trade Commission to, within a year of passage, establish rules that would enable consumers to "simply and easily indicate whether the individual prefers to have personal information collected by providers of online services, including by providers of mobile applications and services." The act—which has generated considerable industry discussion about its technical feasibility—has been referred to the Senate Commerce Committee.

One scenario that appears more likely than any is that the U.S. Congress will not anytime soon consider omnibus privacy legislation similar to Canada's PIPEDA or Europe's directive on personal data protection.

"There is little consensus on either the need for broader privacy legislation or what it would encompass," Ingis explains.

"Such consensus may be difficult to reach given the current partisan posture in Washington and the fact that elections are approaching," he adds.

Even if the aforementioned bills pass, their impact on U.S.-based businesses may pale in comparison to final rulemaking expected from the U.S. Department of Health and Human Services.

In May 2011, HHS released the next in a series of rules called for by the HITECH Act of 2008. Public comments on the draft rules—which address accounting of disclosures of protected health information—were due on August 1. In the [draft](#), covered entities such as hospitals and insurers must log when and to what extent their employees, contractors and service providers access a medical record. The new rules effectively provide patients with a new right to an "access report," which was

not included in HIPAA or HITECH. In this access report, patients would be provided the names of the employees—and employees of all contractors and service providers—who have accessed their medical records, even where that access was entirely legal and appropriate.

“This new ‘access report’ represents a collision between the supposed privacy interests of patients and employees’ privacy rights, including their right to do their jobs without fear of harassment,” Ann Waldo, partner at Washington, DC-based Wittie, Letsche & Waldo, LLP tells *The Privacy Advisor*.

The industry reaction to this draft—as evidenced in the public comments submitted and industry conferences and webinars held in the aftermath—has been widely negative. Few healthcare organizations currently log accesses and disclosures to the level of detail apparently needed to comply with the rule. Retrofitting and integrating applications to meet this standard could rival efforts taken in the late 1990s to prepare for the Y2K date changeover.

“The rules as written would pose an enormous burden on healthcare institutions,” Waldo added. “That burden is not justified by any meaningful gains in patient privacy.”

HHS has indicated that it is targeting year-end 2011 for publication of the final rule, but it would not be surprising if HHS took additional time to consider requested changes.

For its part, the U.S. Department of Education has also voiced its intention to issue by the end of 2011 final, revised [rules](#) implementing the Family Educational Rights and Privacy (FERPA) of 1974. FERPA is perhaps the least enforced federal privacy law in the United States, so a new approach in this area could have a dramatic effect on the large American educational sector.

The wildcard for 2011 and beyond are U.S. state legislatures. Many companies are still implementing policies and procedures to comply with State of Massachusetts 201 CMR 17, which established a de facto national standard on information security for companies doing business in all 50 states. The Massachusetts legislature and others before it have shown a propensity to address the data privacy concerns of their citizens that are being unanswered by Washington, DC. What the consumer privacy concerns of 2012 will be depend at least in part on new technology innovations that have yet to be unveiled.

Jay Cline, CIPP, is president of [Minnesota Privacy Consultants](#), the winner of the 2010 Privacy Innovation Award for Small Organizations.