Senate Judiciary Committee Passes Three Data Security Bills

by Harley Geiger [1]
September 23, 2011

Three bills cleared the Senate Judiciary Committee in a markup [2] session yesterday, bringing federal standards for breach notification and data security one step closer to reality. The three bills, proposed by Chairman Leahy [3] (D-VT), Senator Blumenthal [4] (D-CT), and Senator Feinstein [5] (D-CA), would require businesses to develop data privacy and security plans and set a federal standard for notifying individuals of breaches of sensitive personally identifiable information (SPII). Chairman Leahy's Personal Data Privacy and Security Act of 2011 (S.1151) – presumably the most likely to see action on the Senate floor – also contains amendments to the Computer Fraud and Abuse Act, including welcome language to focus the statute more narrowly on hackers and identity thieves.

All three bills would replace existing state data breach notification laws – currently in effect in nearly all states – with a uniform federal rule requiring most businesses and government agencies to notify individuals of a breach of SPII that is "reasonably believed to have been accessed or acquired." The Leahy and Feinstein bills would relieve businesses and agencies from breach notification if they conduct a risk assessment and conclude there is no significant risk of identity theft, economic loss or physical harm to individuals by the breach; the Blumenthal bill has the same formulation but refers simply to harm generally. Under all three bills, if businesses and agencies conclude there is no significant risk of harm arising from the breach, they must share the results of the risk assessment with the Federal Trade Commission (FTC). As we stated previously [6], CDT believes the "notification as default" or "notify unless there is no harm" contained in these bills is superior to a "notify only if there is harm" model of breach notification. CDT also believes requiring businesses to share risk assessments concluding there is no significant risk of harm with the FTC is a critical safeguard against companies conducting slipshod risk assessments.

Senator Blumenthal's bill, the Personal Data Protection and Breach Accountability Act of 2011, was modified at the markup to include health information in its definition of SPII, using language that resembles California state law [7]. Blumenthal deserves considerable credit for being forward-looking and correcting this gap in consumer privacy protection. Unfortunately, the Leahy and Feinstein bills fail to include health information in the definition of SPII. Last month CDT pointed out [8] that none of the data breach bills included health information held by companies not covered by HIPAA, despite widespread agreement [9] on the sensitivity of identifiable health information. The Blumenthal bill also gives the FTC authority to modify the definition of SPII to keep pace with technology, but the Leahy and Feinstein bills do not (an amendment to the Leahy bill removed this provision during the markup). If the Leahy or Feinstein bills were enacted, then, it would likely take a further act of Congress to bring health information under the law. That means the gap would be difficult to address; after all, the current data breach legislation has been percolating in Congress, in various forms, since 2005.

Three more important points about Senator Leahy's data breach bill. First, an amendment to the bill included a 'data minimization' provision, requiring businesses to establish a plan to minimize the amount of SPII the business retains and to delete SPII that is no longer needed to fulfill a (unspecified) business purpose or legal obligation. Data minimization is a key component of the widely accepted Fair Information Practices. Eliminating unnecessary data, as part of a comprehensive data security plan, lowers the risk of breaches happening in the first place and reduces the severity of breaches when they occur. CDT views the inclusion of data minimization in this and other [10] bills as a positive step forward.

Second, earlier iterations of Leahy's bill included several sections on government access to commercial data, but these have now been stripped out. The deleted provisions would have required the government to audit the information security practices of data brokers prior to entering into

contracts with them, and also to complete privacy impact assessments on government use of commercial information services containing personally identifiable information. Government use of commercial data services is a significant privacy issue and it is unfortunate that Leahy's bill no longer addresses it directly. Senator Blumenthal's bill retains these provisions, however.

Third, Senator Leahy's bill includes amendments to the Computer Fraud and Abuse Act. Some of the amendments increase the penalties for computer crimes. A welcome and important addition during markup, however, was a provision designed to ensure that the CFAA is not used against people who merely violate website terms of service. The provision, offered by Senators Grassley (R-Iowa), Franken (D-MN) and Lee (R-UT) would, as Senator Franken pointed out at the mark up, prevent prosecution as felonies for activities that happen every day, including a father logging onto his son's Facebook account to check up on him, or a 17-year old clicking through a screen requiring him to be 18 years old in order to shop for clothes online. It would also prevent use of the CFAA to prosecute – or hold civilly liable – employees who violate a computer use policy issued by a non-governmental employer. Groups from across the political spectrum welcomed [11] the provision because it would focus the CFAA on the identity thieves and hackers it was designed to target. Going forward, it will have to be reconciled with another provision of the bill that requires the Department of Justice to report to Congress prosecutions that the amendment would outlaw.

Congress has considered data breach legislation several times before [12], so the chances that any of the current bills will be enacted are unclear. Data breach and computer crimes issues could be wrapped into cybersecurity legislation that Senate leadership is prioritizing, but cybersecurity legislation itself faces significant hurdles to enactment. However, the problems of data breach and lax information security are only growing more prevalent, so perhaps this time is different. CDT is glad Congress is focused on these issues, but wants the legislation do be sufficiently protective to represent real progress over current state data breach laws and sufficiently flexible to remain relevant in future years. Notwithstanding any law today's Congress may pass, data security problems are going to stay with us for a long time.

-
- Computer Fraud and Abuse Act

Copyright © 2013 by Center for Democracy & Technology
The content on this website that originates with CDT can be freely copied and used as long as you make no substantive changes and clearly give us credit. Details.
Source URL:
https://cdt.org/blogs/harley-geiger/239senate-judiciary-committee-passes-three-data-security-bills

Links:
[1] https://cdt.org/personnel/harley-geiger
[2] http://judiciary.senate.gov/legislation/BusinessMeetingResults.cfm
[3] http://leahy.senate.gov/press/press_releases/release/?id=4a33543d-7a6d-42d7-ba02-fcd3149c4870
[4] http://blumenthal.senate.gov/newsroom/press/release/blumenthal-statement-on-judiciary-committee-approval-and-passage-of-date-breach-and-security-legislation-
[5] http://feinstein.senate.gov/public/index.cfm/thejudiciarycommittee
[6] http://cdt.org/blogs/cdt/wh-cybersecurity-proposal-good-start-data-breach-notification
[7] http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1798.25-1798.29
[8] http://www.cdt.org/blogs/harley-geiger/148data-breach-bills-exclude-health-information
[9] http://www.markle.org/sites/default/files/7_PrivacyPolicies.final__0.pdf
[10] http://republicans.energycommerce.house.gov/Media/file/Markups/CMT/072011/H2577_RSC_xml.pdf
[11] http://www.cdt.org/files/pdfs/CFAA_signon_ltr_2.pdf
[12]

http://www.pcworld.com/article/181549/senate_panel_approves_databreach_notification_bills.html