

# Privacy Updates in the 111<sup>th</sup> Congress and How Your Business May be Affected

By: Danielle M. Benoit



Danielle practices primarily in the area of Communications Law with a focus on Data Privacy and Security. Based in the firm's Washington, D.C. office, she is well-positioned to closely monitor regulatory issues across industry. She concentrates her practice on international data protection matters and advises clients on new media privacy issues, including Web site management, behavioral advertising, Customer Proprietary Network Information (CPNI), and online safety for minors. Danielle is experienced in drafting privacy policies and conducting client audits to help protect their various stakeholders' personally identifiable information. She can be reached at (202) 857-4537 or DBenoit@wcsr.com.

Although health care and economic recovery seemingly dominated the Congressional schedule this year, legislators in both the House and Senate have been busy on the privacy front as well. Congressional leadership recognizes that comprehensive privacy legislation is long overdue as several attempts to pass broad privacy reform have failed in recent years.

Nearly twenty bills have been introduced in the 111<sup>th</sup> Congress, covering breach notification, cybersecurity, health privacy, identity theft, and data transfers, among others.

To date, three comprehensive bills have been voted out of their respective Committees and are ready for a full consideration. Whether these bills strike the right balance to improve data security to better protect Americans' privacy and personal information while promoting commerce remains to be seen as votes will likely come by early next year.

Senate Bill 1490, the Personal Data Privacy and Security Act, a bipartisan effort introduced by Sen. Patrick Leahy (D-VT) and cosponsored by Sen. Orrin Hatch (R-Utah), is sweeping legislation creating a national standard for data protection, tighter criminal penalties for identity theft and willful concealment of a breach, and requires businesses to implement preventative security standards to guard against internal and external threats. Under the federal breach notification standard, which would preempt the laws of 46 states, companies would be required to notify affected individuals, and under certain circumstances,

credit reporting agencies and the United States Secret Service, if their customers' personal data is compromised. Companies and data brokers will also be required to implement security risk assessments, testing, data access controls and mechanisms to detect unauthorized access at the storage point or when data is in transit. Some exemptions will be given to those companies who use encryption or other advanced measures to protect sensitive data. Senators Leahy and Hatch have twice introduced this bill, beginning in 2005, and it was favorably reported out of the Senate Judiciary Committee only to die at full Senate vote. The bill was again voted out of the Judiciary Committee on November 5, 2009.

Senate Bill 139, the Data Breach Notification Act, introduced by Sen. Diane Feinstein (D-CA), authorizes Federal and State Attorneys General to bring civil actions against entities that fail to notify individuals whose personal information has been compromised in a breach and would extend notification requirements to government agencies. Any federal agency or business that collects sensitive personal information and discovers a breach of that information must notify the affected individual without unreasonable delay, and in some cases relevant media outlets and appropriate government agencies. Under the bill, the notification must also include a specific description of the categories of information at risk and contact information where consumers may learn more about the breach. The bill also defines penalties up to \$1 million per violation and there are exemptions for law enforcement or national security purposes. Sen. Feinstein introduced a similar bill in 2007, which failed to pass the Senate. This version was voted out of the Senate Judiciary Committee on November 5, 2009.

Finally, House Bill 2221, the Data Accountability and Trust Act, introduced by Rep. Bobby Rush (D-IL), creates strict requirements regarding the collection, retention, and accuracy of personal information and sets forth data breach notification requirements. The bill authorizes the Federal Trade Commission to promulgate regulations requiring entities to implement security policies and procedures to safeguard sensitive personal data and create standards for data destruction. The bill also imposes additional requirements

on data brokers by requiring them to submit a copy of their security policy to the FTC along with a breach notification and implement audit procedures to authenticate consumer information. The House passed the bill on December 8, 2009 and it has moved to the Senate for consideration.

In addition to the sweeping reform efforts, Rep. Rick Boucher (D-VA), chairman of the House Subcommittee on Communications, Technology and the Internet (House Energy and Commerce Committee) has placed privacy initiatives at the top of his legislative agenda. Boucher continues to draft his highly anticipated behavioral advertising legislation that will set guidelines for Internet users and companies as they engage in commerce over the web. Boucher is working to balance consumer privacy against the economic benefits that targeted advertising brings to consumers. Boucher approves of the industry self-regulation principles and does not wish to disrupt the ad-based model or create a flat ban on targeted ads. Boucher has repeatedly stated that the legislation should not

prescribe specific practices. Rather, legislation should establish solid consumer protection principles and will likely focus on how companies are collecting and using consumer behavior. Boucher hopes to circulate the bill to lawmakers next month. Boucher's Senate counterparts are not on an accelerated timeline to introduce legislation covering behavioral advertising as their efforts remain focused on cybersecurity and comprehensive privacy reform.

While the exact timeframe for action is uncertain, votes are likely to come these bills in 2010 as lawmakers recognize that privacy is a high priority for their constituents. Likewise, these bills should be a priority for affected companies whose stakeholder and business behaviors will be impacted. Companies should remain in close contact with knowledgeable legal counsel to stay informed about pending changes in federal laws and regulations.



[www.wcsr.com](http://www.wcsr.com)

WOMBLE CARLYLE SANDRIDGE & RICE, PLLC 1209\_5708

WOMBLE  
CARLYLE  
INNOVATORS AT LAW®

GA | SC | NC | VA | DC | MD | DE | ©2009