

The Metropolitan Corporate Counsel®

www.metrocorpcounsel.com

Volume 19, No. 9

© 2011 The Metropolitan Corporate Counsel, Inc.

September 2011

Legislative Proposals Compete As Privacy, Data Security, And Breach Notification Continue To Draw The Attention Of Federal Policymakers

Francine E. Friedman,
Jo-Ellyn Sakowitz Klein, James
R. Tucker Jr. and Kristofer A.
Ek Dahl

AKIN GUMP STRAUSS HAUER &
FELD LLP

The Obama administration and Congress view regulations regarding privacy, data security and breach notification as areas where bipartisan agreement may be possible. Well over a dozen bills have been introduced this year alone, and federal agencies ranging from the Federal Trade Commission and the Department of Commerce to the Department of Homeland Security and the Department of Justice have added their input to the debate.

New proposals would change how

Francine E. Friedman is Senior Policy Counsel in Akin Gump's privacy and data protection practice and has a decade of government affairs and lobbying experience. She advises clients on a variety of issues including tax policy involving housing, energy and new markets tax credits; financial services reform; data security; and energy issues. Jo-Ellyn Sakowitz Klein is Senior Counsel and leads the firm's interdisciplinary privacy and data protection initiative. She devotes much of her practice to regulatory, transactional and legislative matters affecting the health industry. She



Francine E.
Friedman



Jo-Ellyn
Sakowitz Klein



James R.
Tucker Jr.



Kristofer A.
Ek Dahl

data is collected, stored and used. They pertain to three areas that often overlap: online and point-of-sale privacy, mobile device and geolocation privacy, and data security and breach notification. The scope of recent proposals is sufficiently broad that a range of industries and sectors would be directly impacted. Retailers, website operators, banks, large employers, data brokers, online marketers, law enforcement, credit reporting agencies, nonprofit organizations and

also advises clients outside the health-care sector that are affected by health-care or privacy law and regulation. James R. Tucker Jr. is a Partner in the firm's data privacy and data protection practice and has 15 years of political and policy experience. He combines this knowledge with a network of government contacts to provide strategic advice to and advocacy on behalf of clients at the federal and state levels. Kristofer A. Ek Dahl is a Senior Public Policy Specialist. All authors are resident in the firm's Washington, DC office.

many other entities need to prepare for the possibility of new regulations.

Array Of Online And Point-Of-Sale Privacy Bills Introduced

Six bills pertain primarily to online and point-of-sale privacy. These bills impose new standards on the collection, use and sharing of consumer information. Key proposals include:

- Rep. Jackie Speier (D-CA): Do Not Track Me Online Act of 2011 (H.R. 654). This bill requires opt-out mechanisms for the collection or use of online and personal data.
- Sens. John Kerry (D-MA) and John McCain (R-AZ): Commercial Privacy Bill of Rights Act of 2011 (S. 799). This bill requires opt-out mechanisms for data sharing, as well as opt-in consent for the collection, storage or sharing of sensitive personal information.
- Rep. Bobby Rush (D-IL): BEST PRACTICES Act (H.R. 611). This bill is similar in structure to the Kerry-McCain proposal. It calls for opt-out mechanisms for data collection and storage, as well as opt-in consent for third-party information sharing.

Please email the authors at ffriedman@akingump.com, jsklein@akingump.com, jtucker@akingump.com and kek Dahl@akingump.com with questions about this article.

AKIN GUMP
STRAUSS HAUER & FELD LLP

- Rep. Cliff Stearns (R-FL): Consumer Privacy Protection Act of 2011 (H.R. 1528). This bill allows consumers to opt out of having their personally identifiable information shared with third parties.

- Sen. John Rockefeller (D-WV): Do-Not-Track Online Act of 2011 (S. 913). As chair of the Commerce Committee, Sen. Rockefeller will play a central role in shaping Senate privacy proposals. His bill gives consumers the ability to opt out of having their online data tracked and stored. His proposal goes one step further than the aforementioned privacy bills by also imposing limits on data collection from mobile devices.

- Reps. Ed Markey (D-MA) and Joe Barton (R-TX): Do-Not-Track-Kids Act (H.R. 1895). Markey and Barton are co-chairs of the congressional Bi-Partisan Privacy Caucus. Their proposal forbids online companies from using personal information for targeted marketing to children, empowers parents to delete their children's digital footprint and requires parental consent for any data tracking online or on mobile devices.

Mobile Privacy And Geolocation Bills Becoming More Common

While the Rockefeller and Barton-Markey proposals touch on many aspects of consumer privacy, including mobile privacy, a second group of bills focuses solely on mobile devices. These bills restrict the collection and sharing of geolocation data. Key proposals include:

- Sen. Ron Wyden (D-OR) and Rep. Jason Chaffetz (R-UT): Geolocation and Privacy Surveillance (GPS) Act (S. 1212, H.R. 2168). Released as companion bills in the Senate and House, these bills prohibit companies from collecting or sharing geolocation information without the user's express consent.

- Sens. Al Franken (D-MN) and Richard Blumenthal (D-CT): Location Privacy Protection Act of 2011 (S. 1223). This bill requires any covered entity to offer up-front notice and receive informed consent from users to track their geolocation information.

- Sen. Patrick Leahy (D-VT): Electronic Communications Privacy Act Amendments Act of 2011 (S. 1011). Sen.

Leahy chairs the Judiciary Committee and has been active in privacy debates. Enacted in 1986, the ECPA restricts third-party access to private electronic communications, such as online activity and e-mails. Because the ECPA does not cover GPS-based information, Leahy's proposal adds geolocation information as a new class of private communications subject to the protections of the ECPA.

Data Security And Breach Notification Bills Gaining Traction

Seven bills have been introduced that primarily focus on data security and breach notification. These bills require entities that collect or store data to implement safeguards to protect data and create a standard for notifying government agencies and consumers if an organization's files are breached. Key proposals include:

- Rep. Mary Bono Mack (R-FL): SAFE Data Act (H.R. 2577). As chair of the Commerce, Manufacturing, and Trade Subcommittee, Bono Mack is one of the key leaders in the House. Her proposal requires businesses to notify consumers and the FTC after a breach is contained and assessed. It also calls for data minimization and stronger security, and it would entitle affected individuals to free credit monitoring services for two years.

- Sens. Rockefeller and Mark Pryor (D-AR): Data Security and Breach Notification Act of 2011 (S. 1207). This bill requires businesses and nonprofit organizations that store personal information to implement reasonable security measures and alert consumers when their data has been compromised. In the event of a breach, affected individuals would be entitled to free credit monitoring services for two years.

- Sen. Leahy: Personal Data Privacy and Security Act (S. 1151). This bill is similar to bills he has introduced in previous Congresses. His proposal calls for businesses to enact security procedures to protect sensitive data, and it creates a federal standard for notifying appropriate parties in the event of a breach.

- Sens. Tom Carper (D-DE) and Roy Blunt (R-MO): Data Security Act of 2011 (S. 1434). This bill requires entities that possess sensitive information to

build safeguards, as well as to enact policies for investigating security breaches and notifying consumers when a substantial risk of identity theft or account fraud exists.

- Sen. Dianne Feinstein (D-CA): Data Breach Notification Act of 2011 (S. 1408). Unlike some other proposals in this category, this bill only applies to breach notification standards. This is the fifth consecutive session of Congress in which Sen. Feinstein has introduced a breach notification bill.

- Rep. Rush: Data Accountability and Trust Act (H.R. 1707). This bill mandates stricter data security policies and creates a national standard for breach notification.

- Rep. Stearns: DATA Act of 2011 (H.R. 1841). Stearns' security and breach notification bill is similar to Rush's in its call for tighter protections of data storage and a standard for notifying affected individuals and government authorities in the event of a breach.

Despite Obstacles, New Regulations May Still Be Implemented

A highly partisan atmosphere certainly clouds the prospects for congressional approval of new data security and privacy regulations. Moreover, the sheer number of bills complicates attempts to build a coalition behind a single proposal, and congressional committees continue to jockey for their claim to jurisdiction over these issues. Yet, given the loud drumbeat from privacy advocates and the seemingly incessant revelations of high-profile breaches, policymakers will continue to push forward in the areas of privacy, data security and breach notification regulations. Even in the absence of meaningful congressional action, the Obama administration may opt to enact its own changes based on its existing regulatory authority. The realm of consumer privacy and data security in the digital era is fast-evolving, and as federal policymakers try to keep pace, much is at stake for everyone involved.

Portions of this article originally appeared in BNA Daily Report for Executives, 139 DER B-1, 7/20/11, copyright 2011, and are reproduced with permission of The Bureau of National Affairs, Inc. (800-372-1033), <http://www.bna.com>.