

Toronto / Washington DC / Brussels
www.nymity.com



Amy Mushahwar

Associate
Reed Smith
Washington DC

Information Fluidity, Innovation and Trust, Privacy & Security in The Digital Economy: Who's on Point for What in the United States?

Most business executives, legislators, government officials and regulators all agree that information fluidity is critical to innovation and economic growth. The same group would also agree that without trust, commerce on the Internet would come to a standstill. Trust is built through protection, proper management and privacy of information.

Amy Mushahwar has followed the privacy and protection journey on the Hill for many years. She shares her observations of who is on point for what in 2011 in the Administration, Congress and the various agencies. She also provides us with insight into what might be on the privacy, security and information management agendas of those who are in charge.

Amy is a data privacy, security and management attorney at the law offices of Reed Smith and a former data security technical consultant. Amy assists firm clients with crafting public policy advocacy strategies and building enterprise-wide regulatory compliance programs from the ground up.

Nymity: What changes has 2011 brought to Congress and its various committees? What are the issues that are up for discussion and what is the likelihood of legislative action this year?

Mushahwar: The 112th Congress brought many changes to the House due to the shift in party leadership, as Republicans took the majority. As a result, committee leadership also swapped along party lines and new committee chairs are carrying out legislative priorities that may slightly differ from we've seen in the last few Congresses. Despite these changes, privacy and cyber security discussions continue to garner legislative interest as concerns intensify among lawmakers, consumers and stakeholders.

A considerable number of privacy-related legislative proposals have dropped in both chambers. The subject-matter trends that we're seeing are: a national data breach standard, a data privacy legislative framework beyond the sector-specific model that we have in place today, reform for the Electronic Communications Privacy Act (ECPA), greater privacy transparency regarding mobile geolocation and continued work on a cyber security bill for the public and private sectors.

Of course, it is difficult to predict precisely what Congress will do, but as I peer into my crystal ball of potential legislative action, here are my best predictions.

- National Data Breach Bill: Very good prospects for legislative action in both chambers. Bear in mind that Rep. Rush's national data breach bill did pass in the House in the 111th Congress.
- ECPA Reform: Likely, because cloud computing updates are needed.
- Mobile Geolocation Privacy: On June 15th, draft legislation was dropped by the Senate Judiciary Committee's new Privacy Subcommittee (industry is still evaluating its likelihood for passage and whether the bill will be folded into ECPA reform).

- Cyber security: Significant movement of cyber security measures are not likely unless there's resolution of the ongoing turf battle regarding which agency is in charge.
- Privacy (full framework/FIPPs bills, Do Not Track Legislation and Financial Privacy): Not likely unless there is a major government or private incident.

All bets are on a data breach notification bill coming out of Congress this session. We are in the middle of an active breach climate and a perfect storm is brewing for federal action: the number of high-profile data breaches is rising, the rate of privacy breach litigation is increasing, the possibility of regulatory and state legislative actions is great, and the pressure from the international community is intensifying. We are learning that everyone is vulnerable to a breach – from major corporations and banks like Sony and Citi to prominent international entities like the IMF. The calls for a national data breach standard will only get stronger in the coming months as companies clamour for a more streamlined, uniform breach notification process.

Data breach notification bills have momentum in the House with three bills pending (from Reps. Stearns, Bono Mack and Rush). Mary Bono Mack (R-CA), Chair of the Energy and Commerce Committee's, Subcommittee on Commerce, Trade and Consumer Protection, is determined to get data breach notification legislation reported out of her subcommittee. In the Senate, Senators John Kerry (D-MA) and John McCain (R-AZ) are pushing along their commercial privacy bill that would create a notice and choice privacy framework. It has become the bill to watch on the privacy front. We can expect a legislative hearing soon in the Senate Commerce Committee and possible floor action. We also can't count out Chairman Patrick Leahy (D-VT) of the Senate Judiciary Committee and his proposals for ECPA reform and data privacy. If the momentum in both chambers keeps up, we can anticipate some legislative changes this year.

Despite this ambitious agenda, we need keep in mind that there are only about 6-9 months for legislative action before Washington gears up for the 2012 election. However, it looks like all issues are in play for some legislative changes. We provide a chart below of the pending legislation, as there are many more pending legislative proposals than what we've discussed above. The chart is organized by chamber and subject matter.

PENDING DATA PRIVACY, SECURITY & MANAGEMENT BILLS IN THE 112th CONGRESS

BILL NO.	AUTHOR	TITLE	BILL TOPIC
Senate Bills			
S. 1011	Sen. Patrick Leahy (D-VT)	ECPA Amendments Act of 2011	Geolocation / ECPA
S. 1212/H.R. 2168	Sen. Ron Wyden (D-OR)/Rep. Jason Chaffetz (R-UT)	Geolocational Surveillance and Privacy (GPS) Act	Geolocation / ECPA
S.1223	Sens. Al Franken (D-MN) and Richard Blumenthal (D-CT)	Location Privacy Protection Act of 2011	Geolocation / ECPA
S. 913	Sen. Jay Rockefeller (D-WV)	Do-Not-Track Online Act of 2011	Privacy – Do Not Track
S. 799	Sens. John Kerry (D-MA) and John McCain (R-AZ)	Commercial Privacy Bill of Rights Act of 2011	Privacy—Framework Bill
S. 1029	Sens. Mark Udall (D-CO) and Scott Brown (R-MA)	Electric Consumer Right to Know Act	Smart Grid
S. 1151	Sen. Patrick Leahy (D-VT)	Personal Data Privacy and Security Act of 2011	Data Breach Notification
S. 1207	Sens. Mark Pryor (D-AR) and Jay Rockefeller (D-WV)	Data Security and Breach Notification Act	Data Breach Notification
S. 413	Sen. Joe Lieberman (I-CT)	Cybersecurity and Internet Freedom Act	Cyber Security
S. 21	Sen. Harry Reid (D-NV)	Cyber Security and American Cyber Competitiveness Act of 2011	Cyber Security –Marker

BILL NO.	AUTHOR	TITLE	BILL TOPIC
House Bills			
H.R. 1528	Reps. Cliff Stearns (R-FL) and Jim Matheson (D-UT)	Consumer Privacy Act of 2011	Privacy—Framework Bill
H.R. 611	Rep. Bobby Rush (D-IL)	BEST PRACTICES Act	Privacy—Framework Bill
H.R. 1895	Rep. Ed Markey (D-MA)	Do Not Track Kids Act of 2011	Privacy – COPPA Amendment Contemplating Children, Teens and Do Not Track
H.R. 654	Rep. Jackie Speier (D-CA)	Do Not Track Me Online Act	Privacy – Do Not Track Specific
H.R. 653	Rep. Jackie Speier (D-CA)	Financial Information and Privacy Act	Privacy – Financial Privacy
H.R. 1707	Rep. Bobby Rush (D-IL)	Data Accountability and Trust Act	Data Breach Notification
H.R. 1841	Reps. Cliff Stearns (R-FL) and Jim Matheson (D-UT)	Data Accountability and Trust Act (DATA) of 2011	Data Breach Notification
H.R. ____	Rep. Mary Bono Mack (R-CA)	Secure and Fortify Electronic Data Act	Data Breach Notification
H.R. 2096	Reps. Mike McCaul (R-TX) and Dan Lipinski (D-IL)	Cybersecurity Enhancement Act of 2011	Cyber Security

Nymity: The FTC and the Department of Commerce both released papers on privacy in the last year. Comments have been received. What are their key points and what regulatory activities have we seen or can we expect in the coming year from these agencies? How would specific industries be affected and what actions can they take to ensure compliance?

Mushahwar: Regulatory activities we have seen on privacy and cybersecurity can potentially impact nearly all industries.

As for privacy, the FTC and Department of Commerce issued papers that propose privacy baselines, and they plan to release final reports sometime this summer or fall after reviewing comments from industry and stakeholder groups. The FTC paper proposes a privacy baseline that includes the following components: privacy by design, consumer notice, choice, data access, data minimization and a self-regulatory safe harbor. The FTC staff also expressed support for a Do Not Track mechanism that would allow consumers to choose whether to allow the collection and use of data gleaned from their online searching and browsing activities.

In comparison to the FTC paper, Commerce's Green Paper provides more flexibility to private companies by promoting industry self-regulation and supporting the idea that voluntary industry codes of conduct would be better suited to help companies adapt to the pace of innovation. Its data privacy road map includes: keeping the U.S. sector-specific framework while filling in any identifiable gaps, using Fair Information Practice Principles (FIPPs) to establish a basis for greater interoperability between the US and international commercial privacy frameworks, creating a Privacy Policy Office (PPO) within Commerce, and considering a national standard for security breach notifications. In addition, the Administration is urging Congress to adopt a privacy baseline consisting of FIPPs.

Cybersecurity is another area that is getting attention from the Administration as well as federal agencies. The White House introduced a Cybersecurity legislative proposal that is a follow-up from the President's Cyberspace Policy Review. Shortly thereafter, Commerce released a second request for comments on a set of voluntary codes of conduct that would help companies strengthen their individual cybersecurity. Although considerable Administration and Agency discussions have occurred as of late, we don't see a resolution of this issue if the players can't even resolve their own turf war regarding which of them will be primarily responsible for developing cybersecurity standards and policing security conduct. At the moment, the Commerce proposal designates itself as the voluntary code developer and the FTC as the 'enforcer' of such codes, to the extent that a company's cybersecurity representations could result in a Section 5 action.

Regulatory actions must be tracked carefully because some of these proposals can be implemented without an act of Congress. And should Congress fail to pass legislation in the time frame it has left before the elections, the FTC and Commerce may take administrative action to fill any perceived public policy gaps.

Nymity: Are any states are getting ahead of the federal government on privacy?

Mushahwar: In addition to federal activity, privacy regulation on the state level should also be monitored closely. States like California are trying to pass Do Not Track legislation. As we have seen in the data breach notification context, state bills can be a vehicle to spur action on the national level given the geographic fluidity of web sites.

Nymity: Besides regulatory enforcement, litigation is another area of concern for our readers. Can you describe the current litigation landscape?

Mushahwar: There has been an explosion in breach and privacy-related litigation. You are well aware of the breach litigation regarding Sony and others (which is proving to be very costly). Industry estimates that the Sony and Epsilon breaches will each cost approximately \$2-3 billion. Plus, Sony is facing class action lawsuits, Hill inquiries and a potential FTC investigation. But there is also privacy practices litigation that is now emerging (absent any breach). Some examples include suits involving online tracking, flash cookies, history snuffing and call center/text messaging compliance.

In terms of privacy-related litigation, many credible companies are only a complaint away from a class action headache. Companies using flash cookies or “Local Shared Objects” to track computers of their web visitors are vulnerable to litigation. These actions are costly even if they are dismissed in the early stages. Litigants are also trending towards filing suits under statutes that provide for fixed damages (and thus avoiding an Article III harm analysis), such as the Driver’s License Protection Act, ECPA/SCA, the Computer Fraud and Abuse Act and the Telephone Consumer Protection Act.

Companies should keep in mind that they can mitigate these risks by proactively developing privacy, and security and data management policies. Thinking ahead on information retention guidelines, storage of data, and privacy policies could prevent court or agency enforcement actions.

Nymity: In closing, what is the bottom line that our readers can take away?

Mushahwar: Privacy, data security and cybersecurity are hot button issues that are gaining traction. We are seeing activity in all three areas by way of federal and state legislation, proposed regulatory action, and litigation. The bottom line is that the regulatory and legislative action proposed create a large impetus to get self regulation right (and to consider if further programs are advisable beyond the existing program for online behavioral advertising).

Congress has a short time to act, but given the current political climate, it looks like the right pieces are coming together for some legislative action. However, it is important to keep in mind that there are agency actors that may step into the fray without an act of Congress.