U.S. Privacy Legislative and Regulatory Update

Conference Board Counsel of Chief Privacy Officers

ReedSmith

The business of relationships.

October 5 and 6 2010

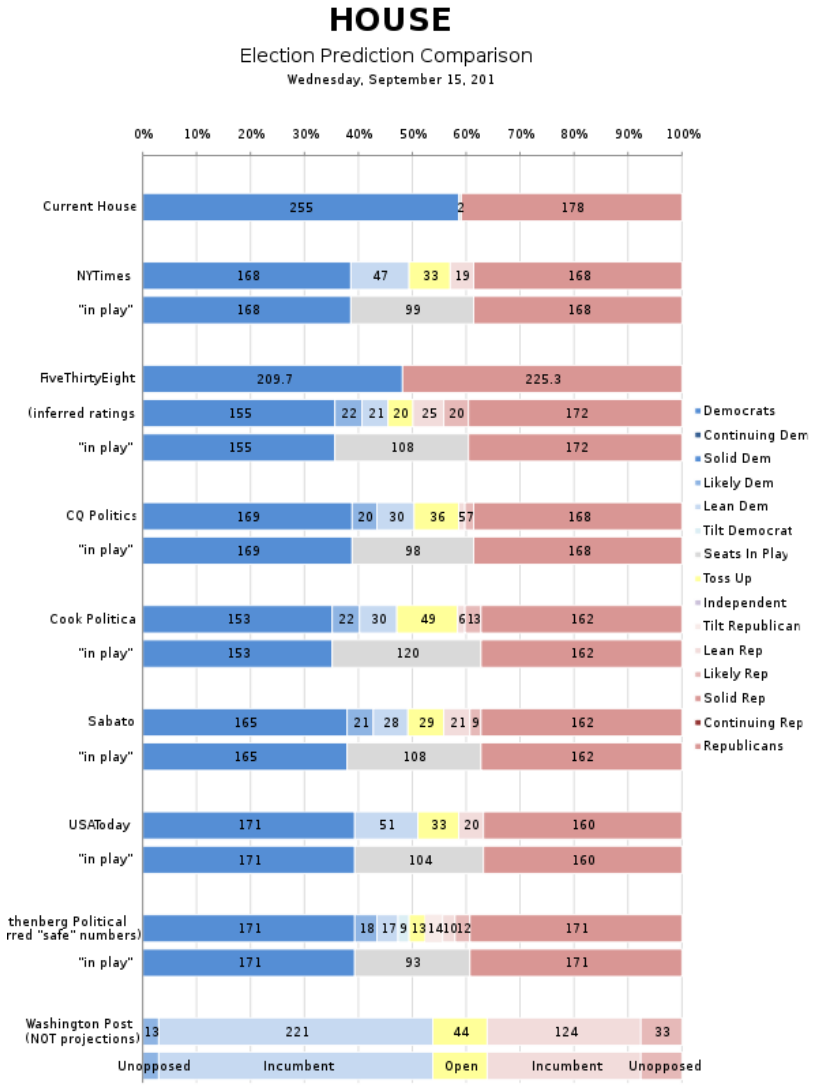
Christopher Cwalina

Counsel, Reed Smith

It’s All About November

Current projections state that the Democrats are likely to hold the Senate and the Republicans have the potential to win the House

The Administration, the regulatory agencies and the Hill are all waiting on releasing privacy initiatives until the outcome of the mid term elections

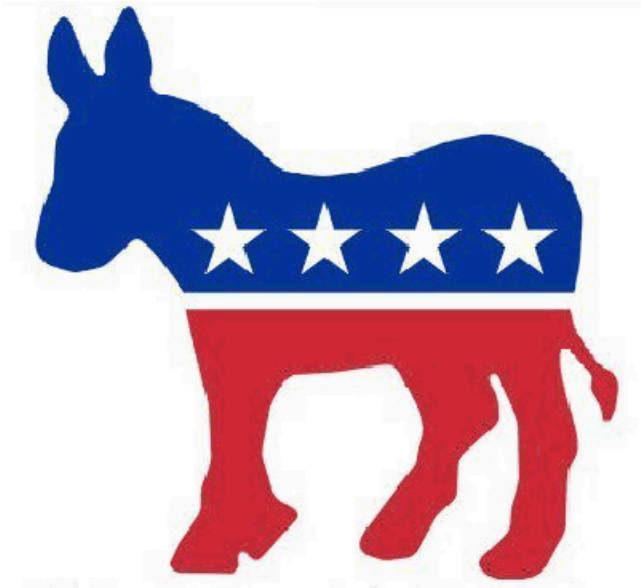


Republican Revolution?

- We are not likely to see a complete landslide / repeat of 1994
- However, if the **House** changes hands we are not likely to see comprehensive Privacy reform out of the House
- As we will discuss, the major pieces of Privacy legislation in the House are being spearheaded by Democrats
- However, if the current projections are wrong and the **Senate** changes hands we are likely to, at least, see government cyber security efforts continue (which will impact those in the audience with a heavy base of government contracts). Private industry data security initiatives will likely slow

Democrats Hold Steady…

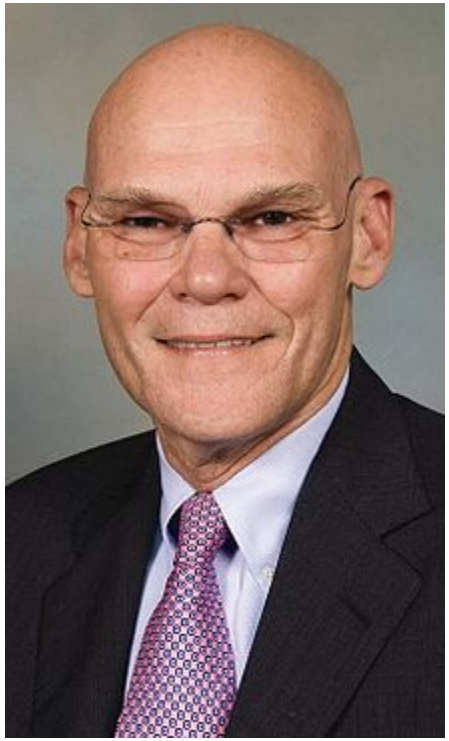
- **Privacy:**
  - Expect continued progress towards an online privacy bill. (Senator Kerry has promised that he would pursue an online privacy bill in the Senate to compliment the efforts of Boucher-Stearns and Rush)
  - ECPA: both the House and Senate Judiciary Committees held hearings last month on how to update ECPA to ensure the government's ability to access stored data 'in the cloud'
- **Data Security**: We are more likely to see private data security reform in addition to government cyber security bills



ReedSmith
The business of relationships.

That Said, Understand the Priorities

- Privacy is a third-tier political issue, far behind the economy, education, immigration, terrorism and healthcare
- Privacy items are not likely to be a major spearheaded initiative (like that of financial regulatory reform, healthcare or the jobs bill)
- Unless privacy items are attached as riders to the jobs bill or appropriation measures we are not likely to see any passed items in the lame duck session
- Instead, major initiatives will be spearheaded through the regulatory agencies



It's the economy, stupid

ReedSmith

The business of relationships.

Status: Federal Regulatory Agencies

FCC

NIST

Consumer Financial Protection Bureau

Elizabeth Warren, Interim CFPB Chief

- A component of the Fed with broad jurisdiction to protect consumers of credit, savings, payment and other consumer financial products and services (and servicers)
- Consolidated authority over for rulemaking, compliance, reporting and enforcement
- Broad rulemaking authority (*i.e.,* FCC-style, not FTC-style)
- Authorized to establish or facilitate registration and licensing regimes
- Broad enforcement powers:
  - Issue subpoenas
  - Civil investigative demands
  - File civil actions in federal district court
  - Issue cease and desist orders
  - Very high penalties (up to $1M/day)
- FTC's primary authority for financial product and services protections will be transferred to the CFPB, but the FTC will retain some measure of enforcement authority that is yet to be determined
- The FTC will remain the lead on data security
- States' authority is not preempted to enact stricter consumer protection laws (*e.g.,* California SB-1). State AGs would also have concurrent authority to enforce laws under the CFPB

FTC Roundtables and Reform, Oh My!

- Undertaking a comprehensive review of all privacy regs and industry information sharing practices
- Hosted three day-long roundtables discussing the privacy challenges posed by 21st century technology and business practices that collect and use consumer data
  - **First Roundtable (Dec. 7, 2009):** Examined risks/benefits of information-sharing practices, consumer expectations regarding such practices, behavioral advertising, information brokers, and the adequacy of existing legal and self-regulatory frameworks
  - **Second Roundtable (Jan. 28, 2010):** Examined how technology affects consumer privacy, including its potential to weaken and/or strengthen privacy protections
  - **Third Roundtable (Mar. 17, 2010):** Examined health data and other sensitive consumer information, and identity management and accountability approaches to privacy

David Vladeck
Consumer Protection Bureau Head

His theme throughout these roundtables was identifying the evolution of privacy as an individual right.

FTC Report (Fall/Winter)

- Report will address broad, privacy framework topics. An initial report is likely to be released with a comment period before recommendations are finalized
- Derived from the Privacy Roundtables:
  - **Deficiencies Recognized:** in the Notice and Choice model (*e.g.,* privacy policies) and harm-based approaches to privacy (e.g., protections against financial harm (identity theft), physical harm (stalking) and intrusions (spam and malware), gaps exist given the rapid growth of technology, computing power and new business models that rely on the collection and use of data
  - **Privacy / Prosperity & Funding of Free Content:** In the marketing context, balancing is needed to weigh consumer protections against the invisible collection and sharing of data without harming the many benefits coming from the free flow of data (and the fact that data on the web is, for the most part, funded by advertising
  - **PII:** The line separating data that is personally identifiable and that which is non- personally identifiable is very blurry
  - **Sensitive Information**: As recognized in the behavioral advertising guidelines, are there certain classes of data that should not be collected at all?
- Broad concepts to be addressed in the FTC Staff Report:
  - **Privacy by Design**: Business must build privacy protections in product/service development process. Responsible companies need to make privacy a priority; *e.g.,* designation of CPO, training employees, appropriately securing data, having responsible data retention practices
  - **Simplifications Needed:** To the notice and choice mechanisms. Think clarity and standardization, as was done with GLBA
  - **Access/Correction:** Providing consumers with a right to access held data (and potentially correct it, if it is in error)

FCC – Broadband Plan and Cybersecurity Roadmap

- Previously, the FCC issued a Public Notice associated with the Broadband Plan requesting comments on privacy issues raised by CDT. This included meeting consumer expectations on privacy, building privacy into the design of new products and services, the creation and use of transactional data, and concerns about applications' use of data.
- Generally, the FCC is not likely to take the lead on privacy issues – however, it will address privacy matters to the extent that they touch and concern traditional areas of FCC regulation (*i.e.*, common carriers, cable carriers, telemarketing) but the FCC is trying to take the lead on cybersecurity
- This summer, the FCC requested comments on the 'roadmap' for who should regulate Cybersecurity, many major telecom, cable, energy and public policy players commented

Chairman Genachowski

Commerce Department

Secretary Locke

- Privacy NOI issued as part of DoC's Internet Task Force comprehensive review of the nexus between privacy policy, copyright, global free flow of information, cybersecurity, and innovation in the Internet economy. Internet Task Force Report is expected by year end
- Notice requested comment on the US Privacy framework going forward: state, federal and international privacy laws and regulations; new privacy enhancing technologies; and the role of government, particularly the Commerce Department
- The Commerce Department with its National Telecommunications and Information Administration is expected to heavily coordinate with the FCC and FTC

Department of Energy

- Requested comments on consumer privacy within the smart grid system. *See* Implementing the National Broadband Plan by Empowering Consumers and the Smart Grid: Data Access, Third Party Use, and Privacy (75 Fed. Reg. 26203)(May 11, 2010), including the following items:
  - Whether smart grid technologies require specific privacy rules.
  - What safeguards need to be in place to prevent security breaches and reliability deficiencies?
  - What information may be released to third parties by the utility or those that provide services for or market on behalf of the utility?

Secretary Chu

DHHS - HITECH Regulatory Update

"Our goal is for all Americans to live healthier, more prosperous, and more productive lives."

– Secretary Sebelius

- The HITECH Regulations addressing changes to the Privacy, Security, and Enforcement Rules was published on July 14, 2010
- Comments are in, and a final rule could come out at any time (though we should keep in mind that the federal government is not usually all that speedy)
- Per the proposed rule, the finalized provisions in the Rule will likely be enforced by HHS approximately eight months after publication of the final rule
- Additionally, business associate agreements that are in place prior to publication of the final rule will be "grandfathered" for approximately 18 months from publication of the final rule

ReedSmith

The business of relationships.

Status: Pending Legislation

Privacy: Use of PII Legal Framework

- **House**
  - There are two bills on this topic: one was introduced by Rick Boucher (D-VA) and another by Bobby Rush (D-IL)
  - **Boucher-Stearns**
    - Untitled, Discussion Draft and Executive Summary released May 4, 2010
    - Confidential comments filed June 4, 2010
    - Rumors are that another iteration of the bill will come in 2011
  - **Rush**
    - Rush introduced Best Practices Act of 2010 (H.R. 5777) on July 19, 2009, referred to his Committee and hearing held over the summer
- **Senate Support of House Privacy Initiatives is Likely if D's Remain Control:** On July 27, 2010 John Kerry (D-MA) announced he would pursue an online privacy bill in the Senate, pledging to go beyond targeted advertising to also include new, baseline standards for privacy protection

Boucher - Stearns

- "Online advertising supports much of the commercial content, applications and services that are available on the Internet today without charge, and this legislation will not disrupt this well established and successful business model"
- **Disclosure of privacy practices:** Any company that collects PII about individuals must conspicuously display a clearly-written, understandable privacy policy
- **Collection and use of information:** Generally, opt-out (applies when a website relies upon services delivered by another party to effectuate a first party transaction, such as the serving of ads on that website)
- No consent is required to collect and use operational or transactional data—the routine web logs or session cookies that are necessary for the functioning of the website—or to use aggregate data or data that has been rendered anonymous
- Opt-in consent required for collection of sensitive information about an individual (medical records, financial accounts, SSN, sexual orientation, government-issued identifiers and precise geographic location information)

Boucher-Stearns (continued)

- **Disclosure of information to unaffiliated parties:**
  - Opt-in consent: if a company wants to share an individual's personally-identifiable information with unaffiliated third parties other than for an operational or transactional purpose
  - Opt-in exception: opt-out consent for sharing an individual's information with a third-party ad network if there is a clear, easy-to-find link to a webpage for the ad network that allows a person to edit their profile, and to opt out of having a profile, provided that the ad network does not share the individual's information with anyone else
- **Implementation and enforcement:**
  - The Federal Trade Commission would adopt rules to implement and enforce the measure. States may also enforce the FTC's rules through State attorneys general or State consumer protection agencies

Rush – Best Practices Act of 2010

Congressman Rush

- This bill would:
  - require companies to notify individuals of the type of information they are collecting and why, or face sanctions by the FTC
  - require companies to provide individuals with an ‘opt-out’ option and obtain consent before collecting, using or disclosing sensitive information
  - exclude companies participating in an FTC-approved Safe Harbor Self-Regulatory Choice Program from the requirements.

ReedSmith

The business of relationships.

House Outlook

- Overall, both bills appear to work alongside advertisers in supporting the industry's current self-regulatory practices, although Rush's bill gives the FTC a much stronger hand in regulatory enforcement
- Both measures have predictably come under fire from all sides, with privacy advocacy groups criticizing the definition of sensitive information as too narrow and calling for stronger measures, and industry groups arguing the bills would stifle innovation and add extra costs and burdens for companies
- All three congressmen (Boucher, Stearns and Rush) have pledged to work together, but politics will certainly come into play as Boucher faces a tough reelection campaign and a turf battle emerges between the two subcommittees and their respective chairmen
- Rush has taken the lead in advancing his bill, holding a hearing in July on the measure. Nonetheless, neither bill appears to have the momentum to step ahead of other legislation this session, meaning the issue will be pushed to the next Congress

Senate Outlook

- Sen. Kerry has yet to introduce legislation, signaling much of the legislative legwork on the issue will fall to the next Congress
- Despite the slower start, look for Senate action to be much more sweeping than the House, with top Democrats on the Senate Commerce Committee, including Chairman Jay Rockefeller (D-W.Va.), already calling for broad new rules and a series of tough hearings on every aspect of the issue throughout 2010
- Left unknown at both ends of the Capitol is what would happen should the midterm elections produce a Republican majority
- On the Senate side, a GOP win would shake up the leadership of the Commerce Committee that has pledged to enact stringent rules, while a Speaker Boehner in the House could mean Cliff Stearns appointed as chairman of the House Energy and Commerce Committee

Data Breach

- For data breach matters, the Rush Bill (H.R. 2221) was already passed out of the House. And, there are a number of pending bills in the Senate (*i.e.,* S. 1490, S. 139, S. 3742, S. 3579)
- Mark Pryor (D-Ark.) and Jay Rockefeller's (D-W.Va.) S. 3742, Data Security and Breach Notification Act of 2010 has emerged as the lead bill
  - This bill is a piece of companion legislation to Rush's H.R. 2221
  - Referred to Senate Commerce, Science and Transportation Committee on August 5, 2010
  - Hearing held September 22, 2010. Senate Commerce Subcommittee on Consumer Protection, Product Safety and Insurance
  - The Federal Trade Commission submitted testimony saying that it "strongly supports" the Data Security and Breach Notification Act of 2010 (S 3742), which would require entities with sensitive consumer information to develop a comprehensive data compliance protection plan and adhere to strict breach reporting requirements
  - Imposes new requirements on information brokers giving consumers the right to access and correct the information that is collected about them
  - Preemption:
    - Creates a national standard for PII and breach notification
    - However, permits state AG enforcement of the national standard

ReedSmith
The business of relationships.

Cybersecurity, S. 3480

- There are a number of pending cybersecurity bills, as identified in our matrix
- Presently, the Lieberman bill, S. 3480 has been identified as the 'comprehensive bill,' but there are rumors that another draft compromise bill could be in the works
- The present lead bill would create an Office of Cyber Policy in the White House that would lead all federal efforts and devise a national cyberstrategy
- In turn, DHS would have a National Center for Cyber security and Communications that would create and enforce cyber security policies throughout the government **and the private sector**
- The comprehensive bill remains on hold because Majority Leader Reid has yet to settle the long-standing dispute over which federal agency should have authority over private sector cybersecurity (Commerce, the FCC, DHS and the FTC are all clamoring for this role)

ReedSmith

The business of relationships.

Subject Matter Specific Bills

- Driver's License Information Privacy, S. 1261
- Health IT Privacy, S. 179, S. 444, H.R. 1031 and H.R. 2630
- Identity Theft Reporting, H.R. 123 and S. 3579
- P2P Sharing (at the intersection of privacy/piracy), H.R. 1319
- SSN Privacy, S. 141, H.R. 122 and H.R. 220
- Wireless Privacy, H.R. 428
- Trans-boarder Transfers of Data, H.R. 427
- Online Shopping, S. 3386 and H.R. 5707
- Youth Safety, H.R. 1076

ReedSmith

The business of relationships.

Questions?

- Please contact Christopher Cwalina
- ccwalina@reedsmith.com