National Retail Federation®
The Voice of Retail Worldwide

Policy Council
Issue Summary

Consumer Privacy and Online Marketing

February 2012

THE ISSUE:
Questions concerning the privacy of data periodically arise as technology evolves. From time to time these discussions reach Congress, in less than clear fashion. Concepts such as data breach, privacy and identity theft can become hopelessly intertwined. These debates are often driven by fear of new technology or couched as protections for children. Indeed, the Federal Trade Commission (FTC) held a comment period for proposed amendments to the Children's Online Privacy Protection Act (COPPA) and will likely release a final rule later this year. The Obama Administration has also sent proposed cyber security legislation to lawmakers on Capitol Hill, which includes a data breach provision. Current cyber security legislative drafts in the Senate and House do not include data breach, but instead focus on critical infrastructure; however several Senators are interested in offering amendments regarding data breach provisions. Senator Reid has indicated that the Senate will consider comprehensive cyber legislation during the work period in early March. Given the interrelatedness of these issues on the Hill, this means that unrelated "privacy" legislation that could adversely affect retailers' ability to market could be encompassed within a final cyber security bill.

BACKGROUND:
Driven in part by conceptual confusion, Congress has shown a renewed interest in data security and privacy, and several key lawmakers have introduced legislation and held hearings on these issues in the 112th Congress. Most of the activity is taking place in the Senate. At this time, three data security bills have been reported out of the Senate Judiciary Committee. The Chairman of the House Energy and Commerce Committee has indicated that data security legislation will not be considered by the full committee until a consensus can be reached among Republicans and industry. The Senate Commerce Committee continues to work on their data security bill, potentially as an amendment to the larger cyber security package.

During the first half of last year, the White House released the President's Cyber Security Legislative Proposal. The proposal, which would preempt state laws (with one exception in regards to consumer breach notice), broadly defines sensitive personally identifiable information, gives the FTC broad ("APA") rulemaking and enforcement authority, and requires consumer notice in almost all instances of a breach as well as providing notice to the media and law enforcement.

In September 2011, the Senate Judiciary Committee reported out the following three data security and breach notification bills, which have been placed on the Senate calendar:

- S. 1151, the "Personal Data Privacy and Security Act of 2011" (re-introduced by Sen. Pat Leahy (D-VT) in June 2011. This bill attempts to prevent and mitigate identify theft, to provide notice of security breaches, and enhance criminal penalties for improper use of sensitive personal

information. Sen. Leahy's bill is also being considered as language for a possible data breach amendment to the cyber security package.

- S. 1408, the "Data Breach Notification Act" (introduced by Sen. Dianne Feinstein (D-CA) in July 2011. This narrower in scope than the other data breach bills, and is most similar to existing state legislation. However, the bill expands the definition of sensitive personally identifiable information and lowers the trigger for customer notification with extensive civil penalty provisions.
- S. 1535, the "Personal Data Protection and Breach Accountability Act of 2011" (introduced by Sen. Richard Blumenthal (D-CT) in September 2011). This bill attempts to prevent and mitigate identity theft with criminal and civil penalties against the breached companies; requires credit monitoring services for customers receiving breach notice, and grants the FTC APA rulemaking authority to amend key definitions.

Elsewhere, the Senate Commerce Committee also took up the data security issue but appears to have reached an impasse in attempting to craft a bipartisan agreement in regards to the Pryor (D-AR)/Rockefeller (D-WV) data security bill. This bill imposes steep obligations on a breached entity, including broad notification requirements and a provision requiring companies to offer free credit monitoring services for potential breaches to consumers. It is possible that the Pryor/Rockefeller draft substitute from late last year will be considered as an amendment to the cyber security legislation.

On July 28, 2011, Senator Thomas Carper (D-DE) and Senator Roy Blunt (R-MO) introduced S. 1434, the "Data Security Act of 2011," which was referred to the Senate Committee on Banking, Housing and Urban Affairs. This bill is modeled after the data security and breach response regime established under the Gramm-Leach-Bliley Act. No hearings or markups have been scheduled.

Meanwhile, in the House, Rep. Mary Bono Mack (R-CA), Chairwoman of the House Energy and Commerce Subcommittee on Commerce, Manufacturing, and Trade held a series of hearings exploring privacy and data security issues, while also working on her SAFE Data Act, H.R. 2577. The Commerce, Manufacturing and Trade subcommittee reported the bill out on July 22, 2011, despite facing significant opposition by industry. Energy and Commerce Chairman Fred Upton (R-MI) has indicated he will not hold a full committee mark up until Republicans and industry can reach agreement on the bill. Rep. Bono Mack is reportedly working on a new draft.

Beyond data breach, Senator Jay Rockefeller , Chairman of the Senate Commerce, Science and Transportation Committee, introduced S. 913, the "Do-Not-Track Online Act of 2011." This bill gives the FTC APA rulemaking authority to create and oversee a Do-Not-Track program, similar to the National Do-Not-Call list. Rep. Edward Markey (D-MA) introduced a narrower but politically more pointed H.R. 1895, "Do Not Track Kids Act of 2011." H.R. 1895 amends COPPA to extend the provisions relating to the collection, use and disclosure of children's personal information.

Finally, Senator John Kerry (D-MA), Chairman of the Communications, Technology and Internet Subcommittee, and Senator John McCain (R-AZ) introduced S. 799, the "Commercial Privacy Bill of Rights Act of 2011." Rep. Cliff Stearns (R-FL), Chairman of the House Energy and Commerce Committee's Oversight and Investigations Subcommittee, and Rep. Jim Matheson (D-UT) introduced H.R. 1528, the "Consumer Privacy Protection Act of 2011." Neither bill has been reported out of committee at this time.

IMPACT ON RETAILING:
NRF remains engaged in this issue to protect retailers' relationships with their customers and promote growth and innovation in the retail industry. Online merchants have been specifically targeted by some of the proposals but, onerous as they are, the spill-over to brick and mortar merchants would be even worse. NRF would support a uniform, national standard for data breach notification, if it closely comported to the most typical of the existing state laws and it contained strong preemptive language to avoid businesses having to comply with 46 state data breach laws. The definition of personal information should be limited to information that if connected and hacked creates a real risk of economic harm to the customer. NRF opposes granting the FTC APA rulemaking authority to unilaterally expand the definition of personal information or responsibilities of companies after a breach.

Notice to consumers after a breach should be subject to a full investigation determining exactly what information was breached and which customers were affected. Including a hair trigger for breached companies to notify all potentially affected customers improperly diverts resources from helping those actually harmed and investing in security improvements. Civil penalties against hacked companies should reflect the pervasive nature of hacking on all industries and extreme penalties, such as mandatory provision of credit monitoring services for all customers, should not be imposed on companies when there is no perceivable benefit or retributive effect. Overly broad privacy legislation and regulation pose significant threats to successful e-commerce and have potentially negative impact on retailers.

NRF ACTION:
NRF has met repeatedly with congressional offices and committees most interested in the privacy agenda as well as the Federal Trade Commission. We are also filing comments with agencies providing the retail perspective and balance to the privacy horror scenarios pushed by other groups. Our efforts have begun to pay off. Congress is taking a much more deliberate view of this subject than appeared likely at the beginning of last year, however as the Senate begins to consider data breach as part of cyber security legislation, retailers' value to the economy and jobs remains an important message in the context of the potential burdensome regulations being discussed.