Privacy & Security Law Report™

April 18, 2011

Legislation

Two New Consumer Privacy Protection Bills Seek FTC Self-Regulatory Safe Harbor Plans

by Alexei Alexis and Donald G. Aplin

The face of U.S. consumer privacy law would change dramatically under two highly anticipated bipartisan measures introduced April 12 and April 13 in Congress that each promote business self-regulatory approaches, (S. 799) by Sens. John Kerry (D-Mass.) and John McCain (R-Ariz.) and (H.R. 1528) by Reps. Cliff Stearns (R-Fla.) and Jim Matheson (D-Utah).

The Kerry-McCain "Commercial Privacy Bill of Rights Act" would charge the Federal Trade Commission with promulgating rules governing businesses that collect, use, or share personal data, and follows the Obama administration's call for privacy bill of rights legislation (10 PVLR 441, 3/21/11). S. 799 would require businesses to provide clear disclosures about their data-collection and usage practices and offer an opt-out mechanism.

Under S. 799, the FTC would also be required to set rules establishing "reasonable" data security standards to protect personal information that include data minimization, data integrity, and purpose specification Fair Information Practices principles regarding the collection of user data.

According to an April 12 statement from the Center for Democracy and Technology, S. 799 "is the first comprehensive privacy bill to be introduced in the Senate in over ten years." CDT President Leslie Harris said the bill is a strong first step toward creating "an enduring, flexible privacy framework that protects consumers while encouraging companies to innovate."

The Stearns-Hunt "Consumer Privacy Protection Act" covers some of the same consumer privacy and data security concepts and approaches of the Kerry-McCain bill. H.R. 1528 would require firms to notify consumers before using their personally identifiable information for any purpose unrelated to carrying out a commercial transaction between the firm and a consumer.

Under H.R. 1528, firms must also adopt data security safeguards "designed to prevent the unauthorized disclosure or release of such information."

Both Measures Seek Self-Regulatory Safe Harbor

Both of the new bills would charge the FTC with setting up safe harbor programs for businesses that meet the privacy and data security standards of the respective measures.

S. 799 includes provisions to establish a safe harbor from the proposed law for companies that participate in industry self-regulatory consumer privacy and data security programs. The bill would charge the FTC with approving nongovernmental organizations to oversee these safe harbor programs to exempt firms from the proposed law, under what the bill dubs a "co-regulatory" program.

The bill also would require the Department of Commerce to "develop codes of conduct in support of applications for safe harbor programs."

Commerce appears to be well ahead of that mandate. In December 2010 the department released an online privacy report, calling for a new office within the department to lead the development of self-regulatory privacy "codes of conduct" for U.S. businesses (9 PVLR 1721, 12/20/10).

Under H.R. 1528, the FTC would be required to establish a program to grant a five-year certification to self-regulatory program applicants that demonstrate they provide "substantially equivalent or greater protections" for personally identifiable information than those set out in the bill.

In order to gain FTC approval under the Stearns-Hunt proposal, a self-regulatory program must document that it includes:

- review of a participant's initial privacy policies and subsequent review if any substantive changes are made to the policy;
- at least annual participant self-review and self-certification of its compliance with its privacy policies and practices;
- random compliance testing of participants;
- a consumer complaint and dispute resolution mechanism that offers binding arbitration as one option and is provided at no cost to the consumer;
- notification to consumers of their rights under the program and the use trustmarks or other indications of a firm's participation in the program;
- the opportunity for a participant found not in compliance with the standards of the program to take remedial action prior to any decision to suspend or terminate them from the program.

The FTC would be required to presume that a company in such a self-regulatory program is in compliance with the proposed law and firms could not be assessed civil penalties for violations of the law unless they engaged in willful noncompliance with the program.

H.R. 1528 would require consumers to attempt resolution of their privacy concerns through the self-regulatory dispute process before turning to the FTC to file a complaint.

Kerry Adds Privacy by Design Since Draft Version

The Kerry-McCain bill first surfaced in its March 11 staff working draft form (10 PVLR 442, 3/21/11). In general, the final version of the bill does not differ dramatically from the earlier draft.

The introduced version of the bill does, however, add a new section requiring companies to incorporate privacy by design into their policies and procedures. Privacy by design is aimed at building privacy considerations into the front end of the design and implementation of new information systems and technology.

The addition of the privacy by design provisions, which were not even mentioned in the draft bill, follows the FTC's March 30 proposed administrative consent agreement with Google Inc. over the internet giant's alleged misuse of user data during the launch of its now-abandoned Buzz social network (10 PVLR 511, 4/4/11). In the proposed agreement, the FTC for the first time required the implementation of privacy by design as part of the remedial scheme agreed to by a respondent firm.

S. 799, as introduced, scrapped a provision from the draft bill that would have allowed the FTC to seek civil penalties of up to $2 million against companies for violations of purpose specification, data collection minimization, and transfer of data violations.

The introduced bill also omitted a provision from the draft that would have authorized the FTC to establish a website where consumers could access the opt out functions of any self-regulatory safe harbor programs it approved to exempt companies from the proposed law.

Kerry Bill Lacks Do-Not-Track Mandate

Consumer Watchdog, the Center for Digital Democracy, Consumer Action, Privacy Rights Clearinghouse, and Privacy Times sent a joint letter to Kerry and McCain April 12, saying that they cannot support the measure because it does not go far enough, particularly in failing to include a provision directing the FTC to mandate and enforce a "do-not-track" mechanism for online consumers.

CDT Consumer Privacy Project Director Justin Brookman emphasized that the proliferation of online user tracking technologies demanded attention but that the bill provided "a solid foundation" for discussions on the issue of no-track.

Kerry, who chairs the Senate Commerce Subcommittee on Communications, Technology and the Internet, said such a provision did not seem to fit with the goal of developing a bill that balances consumer and industry concerns. However, he said it could potentially be considered as an amendment in a committee markup or on the floor.

Mike Zaneis, senior vice president for public policy and general counsel for the Interactive Advertising Bureau, a trade group that represents leading online marketing firms, told BNA

April 12 that the bill "provides the FTC with far too much discretion in drafting implementing rules."

Lisa Sotto, a partner at Hunton & Williams LLP, in New York City, told BNA that "There is heavy reliance in [S. 799] on FTC rulemakings. This will give the FTC significant power to shape the privacy landscape in this country." Sotto said that several provisions in the bill are reminiscent of European concepts, such as providing consumers with the ability to access or correct their data.

"There are some consumer advocacy groups who still don't support this bill, and there are some in industry that still don't support this bill, but at least we have some of the major players [backing] this legislation," McCain said at a press conference announcing the bill. He said it is supported by Microsoft Corp., eBay, and Intel.

Senate Bill Coverage, Enforcement Details

The legislation would apply to any entity that collects, uses, transfers, or stores covered information involving more than 5,000 individuals during any consecutive 12-month period and is subject to Section 5 of the FTC Act, which prohibits unfair and deceptive trade practices, or is a common carrier subject to the Communications Act.

The bill would preempt state laws that cover the same ground but specifically says it would not preempt state laws protecting health information, requiring data breach notification, or that are designed to combat fraud.

The measure would give the FTC primary enforcement power. In addition to the FTC, state attorneys general would be authorized to enforce the proposed law and seek civil penalties of $16,500 per day for each specific data security and consent and notice rules violation and up to $3 million for multiple violations arising from the same event.

Consumers would not have a private right of action under S. 799, which Amy Mushahwar, an attorney at Reed Smith LLP, in Washington, said it was good news for businesses.

"This bill does not make the same mistake that was made in the telemarketing context nearly twenty years ago," she said in an e-mailed statement. "The aftermath of the Telephone Consumer Protection Act clearly shows that consumer class actions rarely benefit anyone."

Stearns Bill Coverage, User Control of Data

Stearns first discussed the contours of his bill March 4 (10 PVLR 359, 3/7/11). He said then that the measure is based on a bill that he introduced in 2005 (H.R. 1263) and also builds on legislative work that he did in the 111th Congress with then Rep. Rick Boucher (D-Va.) (9 PVLR 657, 5/10/10).

Both Stearns and Hunt serve on the House Commerce Subcommittee on Commerce, Manufacturing and Trade, which has jurisdiction over privacy issues.

In an April 13 statement, Stearns said he looked forward to working with Subcommittee Chair Mary Bono Mack (R-Calif.) to get privacy legislation enacted.

In March, Bono Mack said the subcommittee will examine online privacy issues in upcoming hearings this spring focusing on what effect current privacy laws are having on the U.S. technology sector (10 PVLR 441, 3/21/11).

The Stearns bill would apply to businesses and non-profit organizations that collect, use, sell, or disclose "personally identifiable information of more than 5,000 consumers during any consecutive 12-month period."

Covered entities would be required to adopt privacy policies that included the requirement that they give notice to consumers in advance of collecting and using their personal data.

Businesses would also be required to give consumers the opportunity to preclude the sale or disclosure of their information to any organization that is not an "information-sharing affiliate," which is defined as "any affiliate that is under common control with a covered entity, or is contractually obligated to comply" with the privacy and data security policies and practices of the covered entity.

H.R. 1528 would authorize the FTC to enforce the proposed law under the unfair and deceptive practice provisions of Section 5 of the FTC Act, "except that the amount of any civil penalty under such Act shall be doubled for a violation of this Act, but may not exceed $500,000 for all related violations by a single violator."

Under the legislation, consumers would not be entitled to file lawsuits to enforce the proposed law.

If enacted, the Stearns legislation would preempt state laws on data collection, use, and disclosure.

Privacy, Ad Groups Unhappy With House Bill

"This bill does nothing meaningful for privacy, but is a step backwards as far as protecting consumers' rights because of the preemption of state law," John Simpson, consumer advocate for the advocacy group Consumer Watchdog, said in an April 13 statement.

The Direct Marketing Association issued a statement saying that the measure is "overly prescriptive" and delegates too much additional authority to the FTC, particularly in the area of self-regulation.

"It is not necessary or appropriate to give the FTC authority to regulate self-regulatory programs or to review corporate privacy policies," the association said. "This type of government oversight would reduce the effectiveness of existing self-regulatory efforts and discourage future efforts by industry."