KEY CONGRESSIONAL LEADERS INTRODUCE LEGISLATION TO PROTECT THE PRIVACY OF CONSUMER ONLINE AND OFFLINE INFORMATION

Leading congressional proponents of strong privacy protections for consumers' personal information have introduced legislation that advances the debate in Congress regarding whether and how such increased protections should be implemented. While the prospects for new consumer privacy protections are improving because of the apparent bipartisan support for such initiatives, the enactment of legislation is by no means certain at this point because of the differing approaches to the issue taken by the Senate and House sponsors and the congressional committees with jurisdiction over these matters.

This memorandum and the three Willkie summaries linked to it provide both a high-level and a detailed overview of three major privacy bills that have been introduced by leading legislators in the House and Senate, and highlight some of the key issues and differences within and among them. The scope of these bills is quite broad—covering organizations in all industries with respect to their online (and, under some of the bills, their offline) collection, use, and disclosure of personal information—and so businesses should carefully monitor these bills, since, if enacted, they could establish significant new regulatory burdens and costs for a wide range of companies.[1]

On June 1, the House Energy and Commerce Committee announced a plan for review of data security and electronic privacy issues. The first phase will focus on data security and data theft, examining the security of personal information collected and maintained online and the problem of identity theft. Later in the year, the committee will address broader electronic privacy concerns. With the ongoing interest of senior members of the Senate Commerce Committee, as described below, and now the participation of the House committee, the two key congressional committees with jurisdiction over consumer privacy issues are fully engaged in an examination of these issues. The likely result will be a spirited and highly visible debate over consumer privacy issues lasting for at least the rest of this year.

THE KERRY-MCCAIN BILL (S. 799)

On April 12, 2011, Sens. Kerry (D-MA) and McCain (R-AZ) introduced the **Commercial Privacy Bill of Rights Act of 2011** (S. 799) (the "CPBRA").[2] Sen. Kerry chairs the Senate Commerce Committee's Subcommittee on Communications, Technology, and the Internet and

[1] Despite the broad scope of these proposed bills, neither the Kerry-McCain nor the Stearns bill would apply to entities that do not collect, transfer, sell, disclose for consideration, or use personal information of more than 5,000 consumers during any consecutive 12-month period.

[2] A copy of S. 799 as introduced is available here.

Sen. McCain is a former Commerce Committee Chairman. Their bipartisan proposal will likely be the foundation for Commerce Committee efforts to craft a consumer privacy "bill of rights" that could win the support of a majority in the Senate and build momentum for action by the House of Representatives.[3] The committee has already held hearings on an earlier "discussion draft" of their bill, and committee chairman Sen. Rockefeller (D-WV) has made enactment of a privacy bill one of the committee's highest priorities. Thus, the Commerce Committee could proceed relatively quickly to further consideration of the bill but has not as yet announced a specific timetable.[4]

The CPBRA would establish certain new consumer privacy rights that would be protected through several separate and extensive new rulemakings by the Federal Trade Commission ("FTC"), which would be given broad oversight and enforcement authority. Among them are the **consumer's rights to—**

- **Security and accountability**, requiring covered entities to incorporate "privacy by design" into the development of new products and services and to establish procedures for protecting covered information from unauthorized use;

- **Notice**, requiring covered entities to provide individuals with "clear, concise, and timely notice" of their practices for the collection, use, transfer, and storage of covered information, the specific purposes of those practices, and any material change in such practices before the change is implemented, and requiring specific elements for each type of notice;[5]

- **Individual participation**, requiring covered entities to offer individuals clear and conspicuous mechanisms to **opt out** of certain uses of their covered information (and even to **opt *in*** to certain uses or disclosures, such as where sensitive information is at issue), and to provide individuals an opportunity to **access** their personally identifiable information ("PII"), to correct such information to improve its accuracy and, in cases of termination of service or a covered entity's bankruptcy, to have such information rendered not personally identifiable; and

[3] A detailed summary of S. 799 prepared by Willkie Farr & Gallagher LLP may be viewed here.

[4] Note, however, that the Senate Judiciary Committee led by Senator Leahy (D-VT) recently formed a new Subcommittee on Privacy, Technology, and the Law. This subcommittee is chaired by Senator Franken (D-MN) and asserts jurisdiction over major privacy issues, such as online behavioral advertising and social networking. The Senate Commerce Committee leadership disputes the authority of the Franken subcommittee in these areas. Thus, a jurisdictional battle is brewing in the Senate as to which committee will take the lead on privacy legislation, another factor that could slow down and possibly derail passage of a new privacy law.

[5] The bill would authorize the FTC to provide a draft model template for the use by covered entities in designing the required notices.

- Additional rights regarding **data minimization** (*e.g.*, collection of only the data necessary to a specific purpose and retention of data only as long as necessary or reasonable), **constraints on distribution** of personal data to third parties, and **data integrity** (*e.g.*, protecting the accuracy of data critical to a consumer's ability to obtain certain benefits).

The new regulations would be enforced by the FTC and subject to the penalties applicable to Section 5 of the FTC Act. State attorneys general could bring enforcement actions in federal court. CPBRA violations established through a state attorney general's action could result in additional civil penalties of up to $3,000,000.

The bill would also mandate an additional rulemaking to establish a process for the FTC's recognition, oversight, and enforcement of "safe harbor" programs that would be administered by a nongovernmental organization selected by the FTC. Under such programs, participating covered entities would be required to meet minimum privacy protection requirements in exchange for an exemption from provisions of the CPBRA that are addressed by the safe harbor programs. The Department of Commerce ("DOC") would participate by brokering the development of "codes of conduct" among stakeholders that would be the basis for the safe harbor programs.

Overlapping state laws would be preempted—except for laws relating to data breach notification, fraud, or the collection, use, or disclosure of health or financial information—and there would be no private rights of action.

The bill provides that if a covered entity is subject to the CPBRA and any one of the federal privacy statutes enumerated in the bill, such as the Gramm-Leach Bliley Act (the "GLBA") or the Fair Credit Reporting Act (the "FCRA"), then such other federal statute would prevail.[6] However, in a provision the effect of which is not entirely clear, but which could be significant, the bill would appear to replace the existing customer privacy rules that currently apply to cable operators and telecommunications carriers with the bill's new requirements.

THE STEARNS BILL (H.R. 1528)

On April 13, 2011, Rep. Stearns (R-FL) introduced the **Consumer Privacy Protection Act** (H.R. 1528) (the "CPPA").[7] The Stearns bill, which also has bipartisan support, differs from the Kerry-McCain proposal in several material respects, and its prospects are less certain.[8]

---

[6] It is unclear how broadly such deemed compliance would apply in practice. For example, since both the GLBA and the CPBRA have sections that address when consumer consent is required, it is possible that a covered entity subject to both laws would have to comply only with the GLBA's consent provisions, despite the fact that the two consent sections do not completely overlap.

[7] A copy of H.R. 1528 as introduced is available here.

[8] A detailed summary of H.R. 1528 prepared by Willkie Farr & Gallagher LLP may be viewed here.

Although Rep. Stearns is a senior member of the House Energy and Commerce Committee, to which his bill was referred, the lead role on privacy issues in that committee has been assigned to Rep. Bono Mack (R-CA), who chairs the Subcommittee on Commerce, Manufacturing, and Trade. Bono Mack has publicly acknowledged the critical importance of protecting individual privacy, but has indicated that this is a difficult area in which to legislate and that the effect of privacy laws on the U.S. technology sector and that sector's ability to compete internationally is very important as well. Bono Mack has announced her intention to examine both concerns. Her subcommittee is a key player in the Energy and Commerce Committee's plan to review data security and electronic privacy as announced on June 1.

The CPPA would require covered entities to—

- Implement a privacy policy with respect to the collection, sale, disclosure for consideration, and certain other uses of a consumer's PII;

- Make the policy easily available to consumers at the time their PII is first collected, if the PII may be used for a purpose unrelated to a transaction with a consumer;

- Provide a privacy notice to consumers before any PII is used by the covered entity for a purpose unrelated to a transaction with the consumer and upon any material change in the privacy policy;

- Allow consumers to "preclude" the sale or disclosure of their information, for a purpose unrelated to a transaction with the consumer, to certain entities not affiliated with a covered entity; and

- Implement an information security policy that is designed to prevent the unauthorized disclosure or release of a consumer's PII.

These requirements would be enforced by the FTC, which would be authorized to issue implementing regulations and guidance regarding compliance. A violation of the provisions established by the CPPA would be considered a violation of Section 5 of the FTC Act and would be subject to civil penalties of double the amount provided by the FTC Act, up to a maximum of $500,000 for all related violations by a single violator.

The CPPA would encourage covered entities to participate in self-regulatory programs approved by the FTC by deeming participating entities compliant with the requirements established by the CPPA. It would also prescribe the terms of a dispute resolution process for entities in a self-regulatory program. The measure would fully preempt state laws regarding matters addressed by the CPPA and would exclude private rights of action with respect to alleged violations. Existing federal privacy laws, such as the GLBA and FCRA, would not be preempted by the CPPA.

THE ROCKEFELLER BILL (S. 913)

On May 9, 2011, Chairman Rockefeller introduced the **Do-Not-Track Online Act of 2011** (S. 913) (the "DNTOA").[9] The DNTOA is not a comprehensive consumer privacy bill but requires only the implementation of a "Do-Not-Track" ("DNT") mechanism to allow individuals the option of directing that their online activities not be tracked. It would apply to providers of online services that are already subject to the FTC Act, and to nonprofit organizations.[10]

The DNTOA would direct the FTC to issue regulations that: (1) establish standards for DNT mechanisms by which an individual could state a preference as to the collection of information about the individual by providers of online services, including providers of mobile applications and services; and (2) require online companies to accommodate a consumer's DNT preference unless (i) the collection and use of information are necessary to provide a service requested by the consumer and the information is either anonymized or deleted after the service is delivered, or (ii) notice was provided and consumer consent was obtained. The regulations would be enforced by the FTC, but could also be enforced through civil actions brought by state attorneys general or other state officials.

SIMILARITIES AND DIFFERENCES AMONG THE BILLS

The Rockefeller bill has just one purpose—to implement a DNT mechanism. The Kerry-McCain and Stearns bills are more comprehensive privacy proposals and are similar to each other in some respects. Such similarities suggest that elements common to both bills could garner enough support in Congress to become the basis for legislation that may eventually be enacted. Based on the current versions of each bill, such common elements thus far include—

- Subjecting both *online* and *offline* collection and use of consumers' PII to new privacy rules;

- Requirements that "covered entities" that collect, use, or disclose PII: (1) furnish clear and conspicuous notice to consumers of the entities' data collection, use, and disclosure practices; (2) explain the purposes for which the information is collected, used, and disclosed; (3) provide notice of material changes to the terms of the initial privacy notice; (4) afford consumers the opportunity to oppose the sharing of their PII with third parties for marketing and other purposes outside of listed exceptions; and (5) undertake measures to protect the security of consumer PII, including when sharing the data with a third party;

[9] A copy of S. 913 as introduced is available here.

[10] A detailed summary of S. 913 prepared by Willkie Farr & Gallagher LLP may be viewed here.

- Broad preemption of overlapping state laws (although CPBRA contains significant carve-outs for state laws that address: (1) the collection, use, or disclosure of health or financial information, (2) data breach notification, or (3) acts of fraud);

- Giving effect to existing federal privacy laws, such as the GLBA, the FCRA, the Right to Financial Privacy Act (the "RFPA"), and the Health Insurance Portability and Accountability Act ("HIPAA"), so that covered entities would not be subject to multiple and perhaps conflicting privacy requirements (although cable and telecommunications companies are treated differently by the two bills, with CPBRA appearing to replace the existing privacy regulations currently applicable to these companies with the regulations promulgated under CPBRA);

- Preclusion of private rights of action;

- Additional penalties for certain violations; and

- Establishment of voluntary self-regulatory or "safe harbor" programs under which participating entities would comply with at least a minimum set of privacy protection standards in exchange for immunity from FTC enforcement actions and relief from requirements for compliance with certain provisions of law.

However, although both the Kerry-McCain and the Stearns bills incorporate certain similar basic principles, they differ considerably in how such principles would be implemented and enforced. At a high level, the Kerry-McCain bill is more sweeping and prescriptive than the Stearns bill in that it covers more areas, contains more detailed baseline requirements of what is acceptable and expected behavior by companies, and would invest the FTC with new rulemaking and other powers to accomplish its broader objectives. By contrast, the Stearns bill focuses primarily on required disclosures through privacy policies and industry self-regulatory programs approved by the FTC. Notably, for example, the Stearns bill ***does not*** include the following elements of the Kerry-McCain bill—

- Establish a privacy "bill of rights" or endow the FTC with new rulemaking authority with respect to such rights;

- Formalize and mandate "privacy by design" as a new integral component of a company's development of its products and services;

- Specify a list of authorized uses for an individual's PII;

- Require opt-*in* consent for certain uses or disclosures of certain PII;

- Require that covered entities engage in specific due diligence before selecting service providers and impose data use restrictions on them;

- Afford individuals the right to access and correct their PII maintained by covered entities;

- Mandate supervision of safe harbor programs by any specific entity or type of entity;
- Permit enforcement by state attorneys general; or
- Provide a role for the DOC or any other governmental entity in brokering the provisions of a safe harbor program.

These key differences between the bills will no doubt lead to vigorous debate and will make it more difficult to achieve compromise privacy legislation in this Congress.

* * * * * * * * * * * * * * *

If you have any questions regarding this Memorandum, please contact Frank Buono (202-303-1104, fbuono@willkie.com), Pamela Strauss (202-303-1154, pstrauss@willkie.com), Barbara Block (202-303-1178, bblock@willkie.com), Melissa Troiano (202-303-1183, mtroiano@willkie.com), Marc J. Lederer (212-728-8624, mlederer@willkie.com), or the Willkie attorney with whom you regularly work.

Willkie Farr & Gallagher LLP is headquartered at 787 Seventh Avenue, New York, NY 10019-6099 and has an office located at 1875 K Street, NW, Washington, DC 20006-1238. Our New York telephone number is (212) 728-8000 and our facsimile number is (212) 728-8111. Our Washington, DC telephone number is (202) 303-1000 and our facsimile number is (202) 303-2000. Our website is located at www.willkie.com.

June 9, 2011