LexisNexis® Emerging Issues Analysis

Frank Buono, Pamela Strauss, Barbara Block, Melissa Troiano and Marc J. Lederer on

Key Congressional Leaders Introduce Legislation to Protect the Privacy of Consumer Online and Offline Information

2011 Emerging Issues 6016

Click here for more Emerging Issues Analyses related to this Area of Law.

I. OVERVIEW. 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.

---

[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.

Frank Buono, Pamela Strauss, Barbara Block, Melissa Troiano and Marc J. Lederer on

Key Congressional Leaders Introduce Legislation to Protect the Privacy of Consumer Online and Offline Information

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 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]

---

2 A copy of S. 799 as introduced is available, http://thomas.loc.gov/cgi-bin/query/z?c112:S.799:#.

3 For a detailed summary of S. 799 prepared by Willkie Farr & Gallagher LLP, see part II of this commentary.

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.

- **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
- 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]

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;

---

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, http://thomas.loc.gov/cgi-bin/query/z?c109:H.R.1528:#.

8 For a detailed summary of H.R. 1528 prepared by Willkie Farr & Gallagher LLP, see part III of this commentary.

- 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 con-

---

9 A copy of S. 913 as introduced is available, http://thomas.loc.gov/cgi-bin/query/z?c112:S.913:#.

10 For a detailed summary of S. 913 prepared by Willkie Farr & Gallagher LLP, see part IV of this commentary.

sumer 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;

- 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.

II. SUMMARY OF THE COMMERCIAL PRIVACY BILL OF RIGHTS ACT OF 2011 (S. 799).

Sponsors: Sens. Kerry (D-MA), McCain (R-AZ), and Klobuchar (D-MN) (as of June 1, 2011).

Scope: The online and offline collection, use, disclosure, and maintenance of "covered information" by a "covered entity."

Purposes: The Commercial Privacy Bill of Rights Act (the "CPBRA")[11] would establish certain new consumer privacy rights that would be protected through new rulemakings by the Federal Trade Commission ("FTC") addressing the collection and protection of personal information by covered entities. An additional rulemaking would establish a process at the FTC for the recognition and enforcement of "safe harbor" programs. The Department of Commerce ("DOC") would also participate by brokering the development of "codes of conduct" among stakeholders. The CPBRA would establish new penalties for violations. The new rules would be enforced by the FTC and state attorneys general, certain state laws would be preempted, and there would be no private rights of action.

Key Definitions (Sec. 3)

Covered entity—the requirements of the CPBRA would apply to any person/entity that collects, uses, transfers, or stores covered information concerning more than 5,000 individuals during any consecutive 12-month period; and is: (1) a person over which the FTC has authority under Section 5(a)(2) of the FTC Act; (2) a common carrier subject to the Communications Act of 1934; or (3) a nonprofit organization (i.e., an organization that is tax-exempt under the Internal Revenue Code).

Covered information—(1) personally identifiable information ("PII," as defined below); (2) unique identifier information; and (3) any information collected, used, or stored in connection with either of the foregoing that may reasonably be used by the party collecting the information to identify a specific individual. The bill provides four exceptions from this definition for—

11 A copy of S. 799 as introduced is available http://thomas.loc.gov/cgi-bin/query/z?c112:S.799:#.

- PII obtained from public records and not merged with covered information gathered elsewhere;
- PII that is obtained from "a forum" where the individual voluntarily shared the information or authorized it to be shared, and that is both "widely and publicly" available and not restricted with respect to access and viewing;
- PII reported in public media; and
- PII dedicated to contacting an individual at the individual's place of work.

Established Business Relationship—a relationship formed with or without the exchange of consideration, involving the establishment of an account by the person with the covered entity for the receipt of products or services offered by the covered entity.

Personally identifiable information ("PII") means—

> Any of the following with respect to an individual—first name (or initial) and last name; postal address of a physical place of residence; email address; telephone or mobile device number; social security number or other government identification number; credit card account number; unique persistent identifier that alone can be used to identify a specific individual; and biometric data.
>
> Any one of the following if used, transferred, or stored in connection with one or more of the information items listed in the first bullet point above—(1) a birth date; (2) the number of a certificate of birth or adoption; (3) a unique identifier that alone cannot be used to identify a specific individual; (4) precise geographic location, but not including general geographic information derived from an Internet Protocol address; (5) information about an individual's use of voice services; or (6) any other information concerning an individual that "may reasonably be used" to identify that individual.
>
> Sensitive personally identifiable information—a subset of PII, defined as: (1) information which, if lost, compromised, or disclosed without authorization, either alone or with other information, carries a significant risk of economic or physical harm;[12] or (2) information related to a particular medical condition, health record, or religious affiliation of an individual.

---

12 The phrase "significant risk of economic or physical harm" is not defined or explained in the CPBRA.

Third party—a person that, with respect to a covered entity: (1) is not related to a covered entity by common ownership or control; (2) is not a service provider used by a covered entity to receive PII or sensitive PII as part of its services to the covered entity; and (3) does not have an established business relationship with an individual and does not identify itself to the individual at the time the covered information is collected in a clear and conspicuous manner visible to the individual.

Unauthorized use—use of covered information by a covered entity or its service provider for any purpose not authorized by the individual to whom such information relates. There are nine exceptions: (1) to process and enforce a transaction or deliver a service requested by the individual; (2) to operate the covered entity, such as inventory management, financial reporting and accounting, planning, and product or service improvement or forecasting; (3) to prevent or detect fraud or to provide for a physically or virtually secure environment; (4) to investigate a possible crime; (5) as required by law or legal process; (6) to market or advertise from a covered entity within the context of the covered entity's own Internet website, services, or products if the covered information used for such marketing or advertising was collected directly by the covered entity or shared with the covered entity at the affirmative request of the individual, or by an entity with which the individual has an established business relationship; (7) to improve a transaction or service delivery through research, testing, analysis, and development; (8) any use that is necessary for internal operations, such as collecting customer satisfaction surveys to improve customer service information, or collecting information about the visits to an Internet website (e.g., click-through rates) to improve website navigation and performance or to understand and improve the interaction of an individual with the advertising of a covered entity; and (9) any use by a covered entity with which an individual has an established business relationship, so long as such use (i) is one that the individual could reasonably have expected, at the time the relationship was established, is related to a service pursuant to such relationship, and (ii) does not constitute a material change in use or practice from what could have reasonably been expected.

To qualify for any of the nine exceptions from the definition of "unauthorized use," the proposed use of covered information must be "reasonable and consistent with the practices and purposes described in the notice" required by Section 201(a)(1) of the bill (see below).

Unique identifier information—a unique persistent identifier associated with an individual or a networked device, including a customer number held in a cookie, a user ID, a processor serial number, or a device serial number.

Required FTC Rulemakings on Consumer Privacy Rights (Titles I and II)

Implementing the consumer's right to "security and accountability" (Title I)

The FTC would be required to initiate a rulemaking within 180 days of enactment "to require each covered entity to carry out security measures to protect the covered information it collects and maintains." The resulting rule must be consistent with guidance provided by the FTC and recognized industry practices for safety and security that existed on the day before enactment of the bill. The rule would also be required to include at least the following set of requirements for each covered entity that should be applicable in proportion to its size and type and the nature of the covered information it collects—

> Managerial accountability for the adoption of policies and procedures consistent with this legislation;
>
> A process for responding to "non-frivolous inquiries" (undefined) from individuals regarding the collection, use, transfer, or storage of their covered information;
>
> The ability to produce, upon the request of the FTC or a safe harbor program, a description of its means of compliance; and
>
> A comprehensive program for "privacy by design" to assure that the development of new products and services includes consideration of, and addresses, privacy expectations and potential threats to privacy associated with the product or service.

Implementing the consumer's right to "notice and individual participation"—two separate rulemakings (Title II)

The FTC would be required to initiate a rulemaking within 60 days of enactment to require each covered entity to provide individuals with "clear, concise, and timely notice" (1) of the covered entity's practices for the collection, use, transfer, and storage of covered information, and the specific purposes of those practices; and (2) of any material change in such practices before the change is implemented. The FTC would have discretionary authority to allow a covered entity an alternative time and means for providing the required notice if the entity is unable to to provide such notice when information is collected.[13]

Under Title II, the FTC would be required to initiate a second rulemaking, within 180 days after enactment, to require each covered entity to (1) offer individuals a "clear and conspicuous" opt-out mechanism for any unauthorized uses (as defined above) of their covered information; (2) offer individuals a "robust, clear, and conspicuous" opt-out mechanism for the third-party use of their covered information for behavioral advertising or marketing; (3) offer a clear and conspicuous opt-in mechanism for the collection, use, or transfer of sensitive PII;[14] and (4) offer a clear and conspicuous opt-in mechanism for the use of previously collected covered information by the covered entity and for the transfer of previously collected covered information to a third party for unauthorized use if there is a material change in the covered entity's stated practices that requires notice under the CPBRA and such use or transfer creates a risk of economic or physical harm to an individual.

This rulemaking must also require a covered entity to provide individuals with the opportunity for "appropriate and reasonable" access to their PII held by the entity and mechanisms to correct or improve the accuracy of such information. The resulting rule must also permit individuals, when a covered entity enters bankruptcy or the individual seeks termination of service by the entity, "to easily request" that: (1) certain PII be rendered not personally identifiable"; or (2) the covered entity cease its unauthorized use or transfer to a third party for an unauthorized use of such information, or cease use of such information for marketing, unless such unauthorized use or transfer is otherwise required by law.

---

13 This alternative time provision may be addressing offline companies' concerns over their ability to provide privacy notices at the point of sale.

14 Opt-in consent would not be required for the collection, use, or transfer of PII to process a transaction or service requested by the individual or for fraud detection and prevention or to provide for "a secure physical or virtual environment."

This rulemaking must further provide that when an individual has given opt-in consent for the transfer of covered information to a third party for unauthorized use, the third party may not use the information for any purpose other than that stated in the required privacy notice under Section 201 (a) and consented to by the individual.

The CPBRA generally provides that a service provider's use of covered information obtained from a covered entity to perform services or functions for and under the instructions of the covered entity would not be construed as an unauthorized use, so long as the covered entity enters into a contract that restricts the service provider's uses of such information, consistent with the CPBRA and the covered entity's policies and practices regarding such information. A covered entity remains liable for the protection of covered information that has been transferred to a service provider for processing, notwithstanding any agreement to the contrary between a covered entity and the service provider.

Consumer Rights Relating to Data Minimization, Constraints on Distribution, and Data Integrity (Title III)

Data minimization—covered entities would be required to collect only as much covered information as is reasonably necessary to: (1) effect a transaction requested or consented to by the consumer; (2) prevent or detect fraud; (3) provide for a secure environment; (4) investigate a possible crime; (5) comply with law; (6) conduct any research and development to carry out a transaction or to deliver a service; (7) conduct certain specified internal operational or compliance functions; or (8) market or advertise to individuals whose information the entity had directly collected. In addition, covered entities would be required to retain the information for only as long as necessary to provide the transaction/service or for "a reasonable period of time" if service is ongoing.

Constraints on distribution—covered entities would be required to limit third parties by contract as to the distribution and use of covered information and to take "appropriate action" in the case of a material violation of the contract by such third parties. Specifically, third parties must be contractually: (1) required to use the information only for purposes that are specified in the contract and consistent with the purposes of the CPBRA; and (2) prohibited from combining non-PII received from a covered entity with other information that would allow the third party to identify individuals, unless opt-in consent is obtained from the affected individuals to permit such combination and identification.

A covered entity would be prohibited from transferring covered information to an "unreliable third party." Before contracting with a third party, covered entities would be re-

quired to undertake due diligence to "assure" that the third party is "a legitimate organization." Once a contract is in force, a covered entity would be required to notify the FTC of a material violation of the contract by the third party.

In general, a third party receiving covered information from a covered entity would be subject to the CPBRA's provisions as if the third party were a covered entity, unless the third party is in a class exempted by the FTC.

Data integrity—covered entities would generally be required "to attempt" to implement reasonable procedures to ensure that the PII it maintains is accurate if the information could be used "to deny consumers benefits or cause significant harm." This provision does not apply to covered information provided to the covered entity directly by the individual to which such information relates, or by another entity at such individual's request.

Enforcement, Penalties, Preemption (Title IV)

A "knowing or repetitive" violation of the CPBRA or its implementing regulations would be treated as an "unfair or deceptive act or practice" within the meaning of the FTC Act and FTC regulations.

The FTC would have the same enforcement powers with respect to violations of the CPBRA that it currently has under the FTC Act and is also expressly authorized to undertake enforcement against common carriers and nonprofit organizations.

A state attorney general would be authorized to bring a civil enforcement action in federal court if there is reason to believe that a state resident has suffered economic or physical harm because of a covered entity's violation. A previously launched FTC action would preempt such state actions, and the FTC can intervene in any state action. Successful actions by state attorneys general could result in an injunction or civil fines against the violator or an order to compel compliance. The CPBRA would impose additional penalties for violations established through a state attorney general's action under this provision and would cap such additional penalties at a maximum of $3,000,000 for violations under Title I (data security) and $3,000,000 for violations under Title II (notice and consent).

The CPBRA expressly precludes a private right of action.

The CPBRA would not expand or limit the duty or authority of a covered entity or third party to disclose PII to a government entity.

The CPBRA would preempt any state law related to the collection, use, or disclosure by a covered entity of covered information as defined by the CPBRA or PII as addressed by state law. However, it would not preempt state laws that address (1) the collection, use, or disclosure of health or financial information, (2) data breach notification, or (3) acts of fraud.

Required FTC Rulemaking on Safe Harbor Programs (Title V)

Within 365 days of enactment, the FTC would be required to initiate a rulemaking regarding requirements for the establishment and administration of safe harbor programs that would be administered by a "non-governmental organization" ("NGO"). Each such program would be required to include a mechanism for participants to carry out the CPBRA's requirements with regard to: (1) the unauthorized use of covered information; and (2) furnishing consumers with a "clear, conspicuous, persistent, and effective means" for opting out of the transfer of covered information by a covered entity that participates in the program to a third party for purposes of behavioral or location-based advertising or any other unauthorized use.

The FTC would be authorized to select an NGO to administer a safe harbor program through the application procedures set forth in the CPBRA. The FTC would have authority to approve, oversee, and supervise safe harbor programs through ongoing oversight of each administering NGO. However, the legislation does not describe the specific duties of an NGO selected to administer a safe harbor program.

The FTC would have authority to exempt a safe harbor program participant from the provisions of Titles II or III of the CPBRA if the safe harbor program includes requirements that are substantially the same as or more protective of individual privacy than the pertinent provisions of the CPBRA.

Application with Other Federal Laws (Title VI)

Any person subject to the CPBRA that is also subject to a provision of one of the 14 federal privacy laws listed in Title VI of the CPBRA (which include, among others, the Fair Credit Reporting Act ("FCRA"), the Children's Online Privacy Protection Act of 1998 ("COPPA"), Title V of the Gramm-Leach-Bliley Act of 1999 ("GLBA"), the Right to Finan-

cial Privacy Act of 1978 ("RFPA"), and the Health Insurance Portability and Accountability Act of 1996 ("HIPAA")) shall not be subject to the provision of the CPBRA to the extent that such provision of federal privacy law applies to such person. None of the CPBRA's provisions should be construed to "modify, limit or supersede" the operation of these 14 federal privacy laws.

Any person subject to the CPNI privacy provisions (under section 222) or the cable privacy provisions (under section 631) of the Communications Act shall no longer be subject to those provisions to the extent it is subject to a provision of the CPBRA. (Note that this provision could have a fairly dramatic impact on cable operators and telecommunications carriers in that (contrary to how all other companies subject to existing privacy regulations are handled by the bill) the CPBRA appears to contemplate replacing the current privacy regimes that apply to cable and telecommunications companies with the regulations promulgated under the CPBRA.)

Role of the Department of Commerce (Title VII)

The DOC would be required to "contribute to the development of commercial data privacy policy" by:

> Convening private sector stakeholders to develop "codes of conduct in support of applications for safe harbor programs under Title V";
> Expanding interoperability between the U.S. "commercial date privacy framework" and the frameworks of other countries and regions; and
> Conducting research related to improving privacy protection and data sharing practices, including the use of unauthorized data and "growing the information economy."

Other Provisions (Sec. 402)

The FTC would be prohibited from issuing regulations that require the deployment or use of any specific products or technologies, including any specific software or hardware.

III. SUMMARY OF THE CONSUMER PRIVACY PROTECTION ACT (H.R. 1528)

Sponsors: Reps. Stearns (R-FL), Matheson (D-UT), Manzullo (R-IL), Bilbray (R-CA), and Duncan (R-TN) (as of June 1, 2011).

Scope: The Consumer Privacy Protection Act (the "CPPA")[15] would apply to the personally identifiable information ("PII") of consumers that is collected online *or* offline by a covered entity.

Purposes: The CPPA would require covered entities to: (1) have a privacy policy with respect to the collection, sale, disclosure for consideration, and certain other uses of a consumer's PII; (2) make the policy easily available to consumers and notify them of any material change to the policy; (3) notify consumers before their PII could be used for any purpose other than for a transaction requested by the consumer; and (4) allow consumers to preclude the sale or disclosure of their information to any other entity that is not an "information sharing affiliate." The CPPA would encourage covered entities to participate in self-regulatory programs approved by the Federal Trade Commission (the "FTC") by regarding participating entities as 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 preempt state laws regarding matters addressed by the CPPA and would exclude private rights of action with respect to alleged violations.

Key Definitions (Sec. 3)

- **Consumer**—an individual acting in the individual's personal, family, or household capacity.
- **Covered entity**—an entity, an agent, or an affiliate of the entity that collects through any medium, sells, discloses for consideration, or uses PII of more than 5,000 consumers during any consecutive 12-month period. The definition includes nonprofit organizations, but excludes: (1) governmental agencies; (2) providers of professional services (and their affiliates) that are bound by law or rules of professional ethics not to voluntarily disclose confidential client information without the client's consent; and (3) data processing outsourcing entities.
- **Data processing outsourcing entity**—with respect to a covered entity, is a nonaffiliated entity that: (1) provides information technology processing, Web hosting, or telecommunications services to the covered entity; (2) is contractually obligated to comply with security con-

---

15 A copy of H.R. 1528 as introduced is available, http://thomas.loc.gov/cgi-bin/query/z?c109:H.R.1528:#.

trols specified by the covered entity; and (3) has no right to use the covered entity's PII other than for performing the data processing outsourcing services for the covered entity as required by contract or law.

- Information-sharing affiliate—an affiliate under common control with a covered entity, or one that is contractually obligated to comply with the covered entity's privacy policy.
- Personally identifiable information—individually identifiable information relating to a living individual who can be identified from that information, and includes with respect to the individual: (1) the combination of a first name (or initial) and last name; (2) postal address of the individual's physical place of residence; (3) email address; (4) telephone or mobile device number dedicated to contacting such individual at any place other than the individual's place of work; (5) social security number or other government-issued identification; or (6) the complete account number of a credit or debit card issued to the individual. When combined with any of the preceding, PII would also include (i) the individual's date or place of birth; (ii) birth or adoption certificate number; or (iii) electronic address, including an IP address. However, PII would not include: (a) anonymous or aggregate data; (b) any other information that does not identify a unique living individual; (c) information "inferred" about a consumer from data already maintained about the consumer; or (d) information about a consumer that is lawfully publicly available or obtained from a public record.
- **Process**—any value-added activity performed on PII by automated means.
- **Transaction**—an interaction between a consumer and a covered entity resulting in—

    - Any use of information that is necessary to complete the interaction or provide a good or service requested by the consumer, including use—

        - To approve, guarantee, process, administer, complete, enforce, provide, or market a product, service, account, benefit, transaction, or payment method that is requested or approved by the consumer;
        - To deliver goods, services, funds, or other consideration to, or on behalf of, the consumer;

- To protect the health and safety of the consumer; and
- Related to website analytics methods or measurements for improving or enhancing products or services;
- Disclosure of information that is necessary for the consumer to enforce the consumer's rights;
- Disclosure of information required by law or by a court order;
- Use of information: (1) to verify the consumer's PII; (2) to evaluate, detect, or reduce the risk of fraud or other criminal activity; or (3) for other risk management activities; and
- Collection or use of PII for marketing or advertising a covered entity's products or services to its own customers or potential customers.

Privacy Notices to Consumers (Sec. 4)

- A covered entity would be required to provide a consumer with a privacy notice before using any PII collected from the consumer for a purpose unrelated to a transaction. Notice would also be required for a "material change" to the privacy policy and "to the extent practicable" would have to be given to a consumer whose PII had been collected no later than the first time after such change that the covered entity seeks to sell, disclose for consideration, or use the consumer's PII.
- The required notice would have to be provided in a clear and conspicuous manner, be prominently displayed or explicitly stated to the consumer, and contain the following information: (1) a statement that the PII collected by the covered entity may be used or disclosed for purposes or transactions unrelated to that for which it was collected, as described in the existing privacy policy statement; (2) information regarding how the consumer can obtain the privacy policy statement of the covered entity that is required by Section 5 (including a website or toll-free telephone number); and (3) if applicable, a statement that there has been a material change in the covered entity's privacy policy.

Privacy Policy Statements (Sec. 5)

- A covered entity would be required to have a privacy policy statement regarding its collection, sale, disclosure for consideration, dissemination, use, and security of PII. The statement would have to meet the following

requirements: (1) be "brief, concise, clear, conspicuous, and written in plain language"; and (2) be available to all of the entity's consumers, regardless of how transactions are conducted between the covered entity and the consumer, and at no charge, at the time the entity first collects the consumer's PII that may be used for a purpose unrelated to a transaction with the consumer and subsequently.

In addition, the statement would be required to disclose *only* the following:

- The identity of each covered entity, or a description of each class or type of covered entity, that may collect or use the information;
- The types of information that may be collected or used;
- How the information may be used;
- Whether the consumer is required to provide the information in order to do business with the covered entity;
- The extent to which the information may be sold or disclosed for consideration to a covered entity that is not an information-sharing affiliate of the covered entity, including—
    - A clear and prominent statement that the information is subject to sale or disclosure for consideration;
    - A description of each class or type of covered entity to which the information may be sold or disclosed for consideration;
    - To the extent practicable, the purpose for which the information may be used; and
    - The types of information that may be sold or disclosed for consideration; and
    - Whether the covered entity's information security practices meet the security requirements set forth in Section 8 of the CPPA, in order to prevent unauthorized disclosure or release of PII.

The FTC would be authorized to take actions to facilitate industry-wide use of consistent wording or graphics to convey the required privacy policy statements.

Consumer Opportunity to Limit Sale or Disclosure of PII (Sec. 6)

- A covered entity would be required to provide consumers, without charge, the opportunity to "preclude" the sale or disclosure for consid-

eration of the consumer's PII in a particular data collection to any covered entity that is not an information-sharing affiliate of the covered entity for a purpose other than a transaction with the consumer.

- Such a "preclusion" exercised by a consumer would remain in effect for five years or until lifted by the consumer, whichever occurs sooner. However, a covered entity may request the consumer's reconsideration after one year.
- A covered entity may give a consumer the opportunity to permit the sale or disclosure of the consumer's PII in exchange for a benefit to the consumer.
- The opportunity to preclude (or, if offered, to permit) the sale or disclosure for consideration of PII would have to be easy to access and use and be effected through a clear and conspicuous notice.

Consumer Opportunity to Limit Other Information Practices (Sec. 7)

- A covered entity may provide consumers the opportunity to limit other practices of the covered entity with respect to a particular collection or use of PII other than as required by Section 6. If such an opportunity is available, the covered entity would be required to: (1) provide a notice and description of such opportunity in its privacy statement; (2) make it easy to access and use; and (3) maintain any limitation exercised by the consumer unless the consumer withdraws the limitation, or the covered entity provides at least 30 days notice to the consumer before materially changing the limitation or ceasing to comply with it.

Information Security Obligations (Sec. 8)

- A covered entity would be required to implement an information security policy approved by the entity's senior management and designed to prevent the unauthorized disclosure or release of the PII it maintains. The policy would have to include: (1) a process for taking corrective action to prevent or mitigate unauthorized disclosure of information; and (2) the designation of an officer of the entity to be responsible for information security.

Self-Regulatory Programs (Sec. 9)

- The CPPA would give the FTC authority to review and approve applications to establish self-regulatory programs meeting certain requirements and to revoke its approval of programs that fail to meet such requirements. In general, programs would be approved for a period of five years.
- A participant in an approved self-regulatory program would presumptively be in compliance with the requirements of Sections 4 through 8 of the CPPA and immune to certain civil penalties as long as it is subject to enforcement under the program's procedures and requirements and does not willfully violate the terms of the program. However, the presumption of compliance could be overcome by clear and convincing evidence of noncompliance.
- Approved self-regulatory programs would be required to include each of the following elements—

    - The requirement that a program participant provide protections for consumers and their PII that is substantially equal to or greater than that provided in Sections 4 through 8 of the CPPA;
    - Procedures for initial review of a participant's privacy policy and subsequent reviews whenever such statement is "substantively changed";
    - Procedures for a participant's periodic self-review and self-certification of compliance with the program and submission of its self-review to "any administrator" of the program;
    - Random compliance testing of each participant at intervals of not less than every three years and full compliance testing of participants for which compliance issues have been identified or against which there is "a high number" of complaints;
    - A process for notice to the FTC and public notice of a participant's suspension or termination from the program, and the opportunity for remediation prior to suspension or termination of a participant;
    - Requirements and restrictions to assure independence—with respect to program eligibility, compliance, and dispute resolution mechanisms—from improper interference by the participant's management or ownership; and
    - A dispute resolution process that would be available without charge to the consumer, inform the consumer of the proce-

dures, be concluded generally within 60 days, and that could offer binding arbitration among other choices.

- The FTC would have authority to resolve consumer disputes with program participants that could not be resolved through the self-regulatory program's procedures.
- The FTC would have authority to investigate compliance by a participant in a self-regulatory program on its own initiative or on the basis of a complaint from other than a consumer.
- However, before an investigation is instituted, the covered entity would be allowed a reasonable opportunity to invoke its own remedial procedures and assure compliance.
- The FTC would be prohibited from compelling a program participant or administrator to disclose proprietary information or PII unless the FTC provides assurances that such information would not be disclosed.
- A covered entity would be prohibited from misrepresenting that it is a participant in a self-regulatory program.
- Entities that are not covered entities within the meaning of the CPPA would be permitted to participate voluntarily in a self-regulatory program and obtain the rights and benefits of covered entity participants.

Enforcement (Sec. 10)

- 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 FTC would be authorized to issue regulations and interpretive rules to assist compliance with the CPPA's provisions.

No Private Right of Action (Sec. 11)

- The CPPA would expressly preclude private rights of action.

Effect on Other Laws / Preemption (Sec. 12)

- To the extent that PII that would be protected under the CPPA is also protected under one of the 18 federal privacy statutes enumerated in

the CPPA (which include, among others, the Fair Credit Reporting Act ("FCRA"), the Children's Online Privacy Protection Act of 1998 ("COPPA"), Title V of the Gramm-Leach-Bliley Act of 1999 ("GLBA"), the Right to Financial Privacy Act of 1978 ("RFPA"), the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the Cable Communications Policy Act of 1984, the Video Privacy Act of 1988, and the CAN-SPAM Act of 2003), a covered entity complying with the relevant provisions of such other privacy statute would be deemed to have complied with the corresponding provision of the CPPA. The CPPA provides that none of its provisions should be construed to "modify, limit, supersede, or interfere with" the operation of these 18 federal laws.

- The CPPA would preempt "any statutory law, common law, rule, or regulation" of a state, or a political subdivision thereof, to the extent that such law, rule, or regulation relates to or affects the collection, use, sale, disclosure, retention, or dissemination of PII "in commerce."
- State and local authorities would be prohibited from taking any action to enforce the CPPA.

Effective Date (Sec. 13)

- The CPPA would apply to PII collected beginning one year after the date of enactment.

IV. SUMMARY OF THE DO-NOT-TRACK ONLINE ACT OF 2011 (S. 913)

Sponsor: Sen. Rockefeller (D-WV).

Scope: The Do-Not-Track Online Act (the "DNTOA") would apply to any entities already subject to the Federal Trade Commission ("FTC") Act, as well as nonprofit organizations.[16]

Purposes: The DNTOA would establish a framework for a "do-not-track" ("DNT") legal obligation by directing 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 in-

16 A copy of the Rockefeller bill is available, http://thomas.loc.gov/cgi-bin/query/z?c112:S.913:.

formation 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.

Regulations Relating to "Do-Not-Track Mechanisms" (Sec. 2)

- The legislation would require the FTC to promulgate regulations within one year of the date of enactment that would establish standards for the implementation of a DNT mechanism by which individuals could "simply and easily" indicate whether they prefer the collection of personal information about them by providers of online services, including providers of mobile applications and services.[17]
- The FTC would be required to issue rules that would generally prohibit providers from collecting personal information on individuals who, by using a DNT mechanism that meets FTC standards, have indicated a preference not to have such information collected.
- The DNTOA would allow an exception from the DNT rules for the collection and use of information on individuals who have utilized the DNT mechanism to the extent that: (1) the collection of such information is necessary to provide a service requested by the individual and the information is anonymized or deleted as soon as the service is provided; or (2) the individual is given clear notice of the collection and use of such information and affirmatively consents (*i.e.,* opts in) to it.
- The DNTOA would require the FTC to take the following factors into account as it develops the required standards and rules for a DNT mechanism:

    - The appropriate scope of the standards and rules;
    - The technical feasibility and cost of implementation and compliance;
    - Existing mechanisms that are targeted at achieving comparable goals;
    - How DNT mechanisms should be publicized and offered to individuals;

---

17 The bill defines neither "personal information" nor "providers of online services."

- Whether and how information can be collected and used on an anonymous basis so that the information cannot be reasonably linked to or identified with a person or device (both on its own and in combination with other information) and would not qualify as personal information; and
- The standards under which personal information may be collected and used to provide the content or service requested by an individual who has otherwise elected the DNT option.

Enforcement (Sec. 3)

- A violation of the rule prohibiting the collection of personal information from individuals who have expressed a preference against it would be treated as an unfair and deceptive act or practice in violation of Section 18 of the FTC Act.
- State attorneys general and other state officials would be authorized to enforce the DNTOA through civil actions brought in federal court and to seek civil penalties of up to $16,000 per day for noncompliance, up to a maximum total liability of $15,000,000. If the FTC brings an action, this would preclude a state from bringing an action against any defendant named in the FTC's action.

Biennial Review

- The FTC would be required to review implementation and effectiveness of the DNTOA every two years.

Effective Date

- The bill would take effect on the date of its enactment. The implementing regulations would have to be issued no later than one year after that date.

Click here for more Emerging Issues Analyses related to this Area of Law.

About the Authors. 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), **Me-**

Frank Buono, Pamela Strauss, Barbara Block, Melissa Troiano and Marc J. Lederer on

Key Congressional Leaders Introduce Legislation to Protect the Privacy of Consumer Online and Offline Information

lissa Troiano (202-303-1183, mtroiano@willkie.com), or **Marc J. Lederer** (212-728-8624, mlederer@willkie.com).

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.