MORRISON | FOERSTER

# Morrison & Foerster Client Alert.

**April 18, 2011**

# Sens. Kerry And McCain Release A "Privacy Bill Of Rights" That Establishes Broad, New Requirements For Businesses Collecting Personal Information

**By D. Reed Freeman, Julie O'Neill, and Kimberly S. Robinson**

On April 12, 2011, after months of negotiations with stakeholders and multiple drafts, Sens. John Kerry (D-Mass.) and John McCain (R-Ariz.) introduced S.799, the "Commercial Privacy Bill of Rights Act of 2011," which would establish, for the first time, a comprehensive framework for the collection, use, storage, and transfer of personally identifiable information ("PII"). The bill's scope is wide. If passed as currently drafted, it would impose generally applicable notice, choice, security, access, and other obligations on companies that collect information, both online and offline, regarding individuals, requiring fundamental changes to how companies do business and interact with their customers. A summary of the 44-page bill is below.

We have noted issues on which we think there is the greatest likelihood of pushback from industry. We expect the legislative process to be somewhat protracted, as other stakeholders, such as privacy advocates, have already complained publicly that the bill should provide greater restrictions on companies' collection, use, and disclosure of data.

## ENFORCEMENT, COVERAGE, AND PREEMPTION

The bill would be enforced by the Federal Trade Commission (FTC) and state Attorneys General. There would be no private right of action. It would apply to non-profits and certain common carriers that are not traditionally subject to FTC jurisdiction. It does not apply to the government.

The bill would preempt **state privacy laws** governing the collection, use, or disclosure of Covered Information, except those relating to health or financial data, fraud, and data breach notification. The scope of this preemption is unclear, but as written, it could apply to state laws regulating Social Security Numbers.

**Beijing**

Paul D. McKenzie 86 10 5909 3366
Jingxiao Fang 86 10 5909 3382

**Brussels**

Karin Retzer 32 2 340 7364
Joanne Lopatowska 32 2 340 7365

**Hong Kong**

Gordon A. Milner 852 2585 0808
Nigel C.H. Stamp 852 2585 0888

**Los Angeles**

Michael C. Cohen (213) 892-5404
David F. McDowell (213) 892-5383
Russell G. Weiss (213) 892-5640

**London**

Ann Bevitt 44 20 7920 4041
Chris Coulter 44 20 7920 4012
Anthony Nagle 44 20 7920 4029

**New York**

John F. Delaney (212) 468-8040
Joan P. Warrington (212) 506-7307
Miriam Wugmeister (212) 506-7213
Sherman W. Kahn (212) 468-8023
Madhavi T. Batliboi (212) 336-5181
Suhna Pierce (212) 336-4150
Marian A. Waldmann (212) 336-4230

**Northern Virginia**

Daniel P. Westman (703) 760-7795
Timothy G. Verrall (703) 760-7306

**Palo Alto**

Christine E. Lyon (650) 813-5770
Bryan Wilson (650) 813-5603

**San Francisco**

Jim McCabe (415) 268-7011
James McGuire (415) 268-7013
William L. Stern (415) 268-7637
Roland E. Brandel (415) 268-7093

**Tokyo**

Daniel P. Levison 81 3 3214 6717
Gabriel E. Meister 81 3 3214 6748
Jay Ponazecki 81 3 3214 6562
Yukihiro Terazawa 81 3 3214 6585
Toshihiro So 81 3 3214 6568

**Washington, D.C.**

Richard Fischer (202) 887-1566
Reed Freeman (202) 887-6948
Andrew M. Smith (202) 887-1558
Julie O'Neill (202) 887-8764
Obrea O. Poindexter (202) 887-8741
Cynthia J. Rich (202) 778-1652
Kimberly Strawbridge Robinson (202) 887-1508
Nathan David Taylor (202) 778-1644

On the Federal side, the bill could reach the activities of many industries already covered by **federal privacy laws**, including financial institutions subject to the Gramm-Leach-Bliley Act.[1] The only preemption of those federal laws is for those *provisions* of the Kerry-McCain bill that conflict with specific *provisions* of federal law under which an entity is regulated. Thus, as written, all non-conflicting provisions of the McCain-Kerry bill could apply to otherwise regulated entities. Where the FTC does not have jurisdiction to enforce under the FTC Act or this bill, such as with banks, enforcement would, presumably, be conducted by the state Attorneys General.

- ***NOTE:*** We expect that this provision will be subject to additional negotiation, as those entities that are already subject to significant federal regulatory regimes are unlikely to want to take on new, additional regulatory burdens. We also expect advocates to push back on the scope of state preemption.

The bill would also apply to non-profit organizations and common carriers that are subject to the Communications Act of 1934 – entities over which the FTC has generally not had enforcement authority.

- ***NOTE:*** This expansion of FTC jurisdiction is significant and something the FTC has been seeking for years. The long-term risk is that an expansion of jurisdiction here opens the door to expansion of the Commission's jurisdiction elsewhere, or even generally, in an amendment to the FTC Act.

It is also important to note that while the bill appears to have been drafted to address consumer data, it is not limited to consumer data. On its face, the bill could regulate data about individuals, whether they are customers or employees.

## GENERAL SUBSTANTIVE PROVISIONS

As outlined in greater detail below, the bill would:

- Impose federally required notice requirements;
- Require an opt-out choice for most "unauthorized uses" of personally identifiable information;
- Require businesses to provide a robust opt-out mechanism for online behavioral advertising (but not for first-party marketing);
- Require an opt-in choice for the collection, use, or disclosure of sensitive personal information;
- Require an opt-in choice for a new material use or disclosure of previously collected information, where the use creates a risk of economic or physical harm;
- Restrict the transfer of covered information to third parties;
- Codify the requirement that businesses maintain reasonable security for personal information;
- Impose accountability, access and correction, anonymization, data minimization, and data integrity standards, which are drawn from the Fair Information Practice Principles stressed in the Green Paper released last year by the Department of Commerce; and
- Give the FTC wide latitude in promulgating rules to implement its requirements.

[1] Current Federal privacy laws include the Fair Credit Reporting Act, the Fair Debt Collection Practices Act, the Children's Privacy Protection Act, Title V of the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act, and others.

## WHO AND WHAT WOULD THE BILL COVER?

The bill would generally regulate **"Covered Entities**,**"** defined as those that collect, use, transfer, or store the "Covered Information" of more than 5,000 individuals during any consecutive 12-month period.

**"Covered Information"** is defined broadly and obscures the traditional distinction between PII and non-PII. It includes PII,[2] unique identifier information[3] ("UII"), and any information collected, used, or stored in connection with PII or UII that may be used to identify an individual.

"**Sensitive PII"** means information related to a medical condition, health record, or religious affiliation, as well as PII which, if lost, compromised, or disclosed without authorization, carries a significant risk of economic or physical harm. Neither "significant risk" nor "harm" are defined, leaving open the possibility of a broad reading.

## WHAT WOULD THE BILL REQUIRE?

**1. The bill would impose a notice and choice regime.**

The bill directs the FTC to promulgate rules to require a Covered Entity to provide **clear, concise, timely notice** of its Covered Information collection, use, transfer, and storage practices. A Covered Entity would have to maintain the notice in a readily accessible format. In addition, it would be required to provide clear, concise, and timely notice to individuals before changing its practices in a material way. It would not, however, be required to obtain affected individuals' opt-in consent to any such change, as the FTC currently requires. Rather, the bill would require opt-in consent only where the change creates a risk of economic or physical harm to the individual.

While the bill does not differentiate between information collected online and offline, the FTC could (and likely would) impose different requirements for different media. The bill permits the FTC to allow a Covered Entity that is unable to provide the notice at the time the information is collected to comply by providing a way for the individual to promptly obtain the notice. Additionally, in promulgating rules, the FTC may draft guidance on the design and construction of the notice (including a draft model template).

The bill also directs the FTC to promulgate rules to require a Covered Entity to:

- Offer **a clear and conspicuous opt-out mechanism** for any **Unauthorized Use** of Covered Information (except for any use requiring opt-in consent).
- **"Unauthorized Use"** means use for any purpose "not authorized by the individual." Unauthorized Use does not include certain commonly accepted uses by a Covered Entity or its service provider, including first-party marketing (*i.e.*, marketing or advertising in the context of the Covered Entity's own website, services, or products) or analytics, as long as the Covered Information used was either collected directly by the Covered Entity or its Service Provider,

[2] **PII** includes first name (or initial) and last name; residential address; telephone or mobile number (excluding a work number); SSN or other government-issued ID number; credit card account number; unique identifier information that alone can be used to identify a specific individual; and biometric data (including fingerprints and retina scans). It also includes the following, if used, transferred, or stored in connection with any PII: birth date; birth or adoption certificate number; place of birth; unique identifier information that alone cannot be used to identify a specific person; precise geographic location (not including general geographic information derived from an IP address); information about an individual's quantity, technical configuration, type, destination, location, and amount of use of voice services; and any other information concerning an individual that may reasonably be used to identify him/her.

[3] **UII** means 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.

shared with the Covered Entity at the request of the individual, or shared with the Covered Entity by an entity with which the individual has an Established Business Relationship.[4]

  - **No Unauthorized Use for Working With Service Providers**: A service provider may receive Covered Information in performing services or functions on behalf of the Covered Entity if the contract between the Covered Entity and the service provider requires the service provider to collect, use, and store the information in a manner consistent with the Act and the Covered Entity's policies and practices related to such information. Moreover, a service provider may disclose the Covered Information to another service provider in order to perform the same service or function. The Covered Entity, however, remains liable for the protection of the Covered Information, even if the contract between the Covered Entity and service provider provides otherwise.

  - ***NOTE:*** This framework is likely to be subject to negotiation now, as it would be difficult for service providers – vendors that typically work for many customers – to agree by contract to comply with the policies and practices for each one of their clients.

- **Offer a robust, clear, and conspicuous opt-out mechanism** for the use by Third Parties[5] of Covered Information for behavioral advertising or marketing.[6]

- **Offer a clear and conspicuous mechanism for opt-in consent** for:

  - The collection, use, or transfer of **Sensitive PII**, except in limited circumstances;[7] and

  - **The use of previously collected Covered Information or the transfer to a Third Party for an Unauthorized Use of previously collected Covered Information if there is a material change in the Covered Entity's stated practices and the use or transfer creates a risk of economic or physical harm to an individual.**[8]

  - ***NOTE:*** This standard is far less stringent than that currently espoused by the FTC, which requires notice and opt-in consent to any material, retroactively-applied change to a privacy policy – regardless of whether the change presents the risk of harm.

[4] **"Established Business Relationship"** means a relationship (formed with or without consideration) involving the establishment of an account with the Covered Entity for products or services offered by it. The following uses are the other exceptions to the definition of "Unauthorized Use": to process a transaction or deliver a service requested by the individual; to operate the Covered Entity, such as inventory management, financial reporting and accounting, planning, and product or service improvement or forecasting; to prevent or detect fraud or provide security; to investigate a possible crime; that is required by law or legal process; that is necessary for the improvement of the transaction or service through research, testing, analysis, and development; that is necessary for internal operations, including collecting customer satisfaction surveys or conducting consumer research to improve customer service information, and website collection of information about visits and click-through rates to improve site navigation or to understand and improve the individual's interaction with advertising; or by a Covered Entity with which the individual has an Established Business Relationship, which the individual could reasonably have expected at the time of the establishment of the relationship, and which is not a material change from what reasonably could have been expected.

[5] "**Third Party**" is defined as a person that is not related to the Covered Entity by common ownership or control; is not the Covered Entity's service provider; does not have an Established Business Relationship with the individual and does not identify itself to the individual at the time of information collection.

[6] The FTC Staff's December 2010 preliminary privacy report supported a Do Not Track mechanism for online behavioral advertising. Although not specified in the bill, such a mechanism may meet its requirements. *See* http://www.mofo.com/files/Uploads/Images/101203-Do-not-track-list.pdf.

[7] Opt-in consent is not required to process a transaction or service requested by the individual, for fraud prevention and detection, or to provide for a secure environment.

[8] Where Covered Information is transferred to a Third Party, the Third Party may use the Covered Information only for the purposes stated in the notice provided to the individual by the Covered Entity and authorized by the individual when the individual gave consent to transfer the information.

**2. The bill would restrict the transfer of Covered Information to Third Parties.**
A Covered Entity that transfers Covered Information to a Third Party would be bound by certain obligations. Specifically, it would have to:

- Assure through due diligence that the Third Party is legitimate before executing a contract with the Third Party. Curiously, for such a broad term, the word "legitimate" is not defined in the bill. Nor does the FTC have rulemaking authority to define it. Accordingly, this term is likely to be defined through enforcement action;
- Contractually require that the Third Party use the information only for purposes that are consistent with the Act and specified in the contract;
- Contractually prohibit the Third Party from combining information that the Covered Entity has transferred to it and that relates to an individual but is not personally identifiable with other information in order to identify the individual, unless the Covered Entity has obtained the individual's opt-in consent for such combination and identification; and
- Notify the FTC of a material violation of the contract.
    - ***NOTE:*** This last provision is also likely to be the subject of significant negotiation, as requiring reporting to the FTC is a novel provision under U.S. law.

A Covered Entity may not transfer Covered Information to a Third Party that it knows has intentionally or willfully violated a contract required by the Act and is likely to violate the contract.

Notably, the bill provides that a Third Party that receives Covered Information from a Covered Entity is subject to the Act as if it were a Covered Entity; however, it permits the FTC to exempt classes of Third Parties from liability in connection with its notice and choice provisions if the FTC finds that: (1) such class of Third Parties cannot reasonably comply with those provisions; or (2) compliance by such class would not sufficiently benefit individuals.

**3. The bill would make "privacy by design" a legal requirement.**
The bill would require Covered Entities to implement **a comprehensive information privacy program**. Specifically, they would have to incorporate, throughout the product life cycle, development processes and practices designed to safeguard PII in a manner consistent with individuals' reasonable expectations and to address relevant threats. Again, the term "reasonable expectations" is not defined in the bill, and the FTC does not have rulemaking authority under the bill to define it. Any clarity on this concept will likely come from enforcement actions.

Additionally, Covered Entities would be required to maintain management processes and practices designed to ensure that information systems comply with the law, the Covered Entity's privacy policies, and the individual's privacy preferences.

**4. The bill would codify the requirement that businesses maintain reasonable security for personal information.**
The bill directs the FTC to promulgate rules to require reasonable security for Covered Information that is proportional to the size, type, and nature of the Covered Information. These rules must be consistent with current FTC guidance and industry practices. The bill prohibits the FTC from mandating the use of any specific technology.

**5. The bill would impose other requirements grounded in Fair Information Practice Principles.**
***Accountability:*** Proportional to the size, type, and nature of the Covered Information it collects, a Covered Entity would be required to: (1) have managerial accountability, proportional to its size and structure, for the adoption and implementation of policies consistent with the law; (2) have a process to respond to non-frivolous complaints from

individuals; and (3) upon request from the FTC or a safe harbor program (described below), explain how it complies with the law.

***Access and Correction:*** The bill directs the FTC to promulgate rules to require a Covered Entity to provide any individual whose PII it maintains appropriate and reasonable access to, and mechanisms to correct, the information.

***Right to Request Anonymization:*** The bill directs the FTC to promulgate rules to permit an individual to easily request that all of his/her PII be rendered not personally identifiable if the Covered Entity enters bankruptcy or the individual requests the termination of his/her relationship with the Covered Entity. (There is an exception for information that the individual authorized the sharing of or which he/she shared with the Covered Entity in a forum that is widely and publicly available.) Where it is not possible to anonymize the PII, the individual may request that the Covered Entity cease using the PII for marketing or for an unauthorized use (including transfer to a Third Party for an unauthorized use).

- ***NOTE:*** We expect further negotiation to restrict the anonymization provision to protect the billing, collections, and related activities of commercial entities.

***Data Minimization:*** The bill would require a Covered Entity to collect only as much Covered Information as is reasonably necessary:

- To process or enforce a transaction or deliver service requested by the individual;
- To provide a transaction or deliver a service requested by the individual, such as inventory management, financial reporting and accounting, planning, product or service improvement or forecasting, and customer support and service;
- To prevent or detect fraud or provide security;
- To investigate a possible crime;
- To comply with a law;
- For the Covered Entity to market or advertise to the individual (if the Covered Information used for such marketing or advertising was collected directly by the Covered Entity);
- For research and development conducted to improve the transaction or service; or
- For internal operations, including: (a) collecting customer satisfaction surveys and conducting customer research to improve customer service, and (b) collecting from a website information about visits and click-through rates to improve site navigation and performance and the customer's experience.
- ***NOTE:*** We expect further negotiations on this requirement, as businesses often find new uses of previously collected data. Where such uses are not material, we expect that businesses will want to preserve the right to use data in those ways.

The Covered Entity would also be permitted to retain Covered Information only as long as necessary to provide the transaction or service (or for a reasonable period of time if the service is ongoing), to conduct research and development, or to comply with the law. While the FTC has been suggesting that this is a Section 5 requirement for some time, this data retention provision would be a new statutory obligation in the United States, and may require organizations to make significant changes to their existing retention practices.

***Data Integrity:*** Where Covered Information could be used to deny consumers benefits or cause significant harm, a Covered Entity would be required to "attempt to" establish and maintain reasonable procedures to ensure that PII is accurate. This requirement would not apply to Covered Information provided directly to the Covered Entity by the individual or by another entity at the request of the individual.

## HOW WOULD THE BILL BE ENFORCED?

There is **no private right of action** in the bill. Rather, the bill's provisions would be enforced by the FTC and state Attorneys General.

A "knowing or repetitive" violation of a provision of the bill – or of a rule promulgated pursuant to it – would be treated by the FTC as an unfair or deceptive act or practice in violation of an FTC rule – which, in addition to injunctive relief, would subject the offender to civil penalties of up to $16,000 per violation.

State Attorneys General would be authorized to enjoin further violations, compel compliance, or obtain civil penalties. The bill specifies the available civil penalties, which would be capped at $3 million:

- For knowing or repeat violations of Title I (security, accountability, privacy by design), a Covered Entity would be liable for a civil penalty equal to the amount calculated by multiplying the number of days of noncompliance by an amount not to exceed $16,500; and
- For knowing or repeat violations of Title II (notice, choice, access, anonymization), a Covered Entity would be liable for a civil penalty equal to the amount calculated by multiplying the greater of the number of days of noncompliance or the number of individuals for whom it failed to obtain required consent by an amount not to exceed $16,500.

## WOULD THERE BE ANY SAFE HARBORS FROM LIABILITY?

The bill directs the FTC to issue rules to establish safe harbor programs to be administered by a non-governmental organization. The programs would establish mechanisms for participants to implement the law's requirements with regard to (1) online behavioral advertising, (2) location-based advertising, and (3) other Unauthorized Uses. The programs would offer consumers a clear, conspicuous, persistent, and effective means of opting out of the transfer of Covered Information by a Covered Entity participating in the safe harbor program to a Third Party for: (1) online behavioral advertising purposes, (2) location-based advertising purposes, (3) other specific types of Unauthorized Use, or (4) any Unauthorized Use.

Participating and compliant Covered Entities would be exempt only from the provisions of Title II (notice, choice, access, and anonymization) and Title III (data minimization, constraints on distribution, and data integrity).

**About Morrison & Foerster:**

We are Morrison & Foerster—a global firm of exceptional credentials in many areas. Our clients include some of the largest financial institutions, investment banks, Fortune 100, technology and life science companies. We've been included on *The American Lawyer*'s A-List for seven straight years, and *Fortune* named us one of the "100 Best Companies to Work For." Our lawyers are committed to achieving innovative and business-minded results for our clients, while preserving the differences that make us stronger. This is MoFo. Visit us at www.mofo.com.

Morrison & Foerster has a world-class privacy and data security practice that is cross-disciplinary and spans our global offices. With more than 60 lawyers actively counseling, litigating, and representing clients before regulators around the world on privacy and security of information issues, we have been recognized by *Chambers* and *Legal 500* as having one of the best domestic and global practices in this area.

For more information about our people and services and the resources we offer such as our free online Privacy Library, please visit: http://www.mofo.com/privacy--data-security-services/.

*Because of the generality of this update, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations.*