



## DMA Analysis of Boucher-Stearns Privacy Discussion Draft

May 5, 2010

On May 4, 2010, Rep. Rick Boucher (D-VA), Chairman of the House Energy and Commerce Committee's Subcommittee on Communications, Technology, and the Internet, and Subcommittee Ranking Member Cliff Stearns (R-FL) released a Discussion Draft bill on consumer privacy ("bill"). The bill has the stated purpose of requiring "notice to and consent of an individual prior to the collection and disclosure of certain personal information relating to that individual."<sup>1</sup> The bill would broadly restrict the collection and transfer of consumer data online as well as offline, and would establish notice and opt-out consent requirements for first party data collection and use (including transfers among affiliates), with some exceptions, a practice that is not required or generally practiced today. The bill would also effectively require opt-in consent for the transfer of personal data to third parties except in limited circumstances. If enacted, this bill would have major implications for many longstanding and important business practices. Both Reps. Boucher and Stearns have indicated a willingness to work with industry and have requested comments on the bill. They stated that the comments will be taken into consideration before the bill is formally introduced. A brief summary of the bill follows below.

### **Section 3. Notice and Consent Requirements for the Collection, Use, and Disclosure of Covered Information**

The bill would impose notice and consent requirements on "covered entities" collecting "covered information." The term "covered entity" is used throughout the bill and is defined very broadly as "a person engaged in interstate commerce that collects data containing covered information," but does not include a government agency or anyone that collects covered information from fewer than 5,000 individuals in a year and does not collect sensitive information. Sec. 2(4).

The term "covered information" refers to identifiable individuals and identifiable computers, and equates less-sensitive identifiers such as names with traditionally more sensitive identifiers such as Social Security numbers and credit card numbers. More specifically, the term refers to any of the following: (1) *any unique persistent identifier*, such as a customer number, unique pseudonym or user alias, IP address, or other unique identifier *where the identifier is used to collect, store, or identify information about a specific individual* or a computer, device, or software application owned or used by a particular user or that is otherwise associated with a particular user; (2) a *preference profile*; (3) a first name or initial and last name; (4) a postal address; (5) a phone or fax number; (6) an email address; (7) unique biometric data, including a fingerprint or retina scan; (8) a Social Security number, tax identification number, passport number, driver's license number, or any other government-issued number; (9) a financial account number, or credit or debit card number, and any required security code, access code, or password that is necessary to permit access to an individual's financial account; (10) *any other information* collected, stored, used, or disclosed in connection with any covered information described above. Sec. 2(5) (emphasis added).

The bill would require that a covered entity shall not collect, use, or disclose covered information *from or about an individual for any purpose* without prior notice to and consent of the individual. Sec. 3(a)(1).

---

<sup>1</sup> Bill p.1.

## ***Prescribed Notice***

The bill would require that, if a covered entity collects covered information online, the notice must be both (1) posted clearly and conspicuously on the website through which information is collected and (2) accessible through a direct link from the entity's home page. Sec. 3(a)(2)(A). For offline collection of information, the privacy notice must be made available *in writing and prior* to any information collection, subject to the exceptions for "transactional" and "operational" purposes described below. This offline notice requirement would have broad implications for offline collection and use of data.

The bill prescribes the content of the notice that individuals must receive prior to the collection of their information when such collection takes place online or offline, and would require the notice to include specific information such as a hyperlink to the Federal Trade Commission's ("FTC") online consumer complaint form or a toll-free phone number to the FTC's Consumer Response Center.<sup>2</sup>

## ***Opt-Out Consent***

To obtain consent for information collection and use, (1) a covered entity must provide a "clear statement" to the individual containing the information required for a privacy notice and inform the individual of the right to decline consent, and (2) the individual must either affirmatively consent *or not decline* consent when the statement is presented. Sec. 3(a)(3). This is a requirement beyond current practices, particularly in the offline environment where first parties do not have to provide notice and choice with respect to their own collection and use of customer information. Affiliates of covered entities are treated as a part of the "first party" company and it appears the bill does not impose independent consent requirements for transfers among affiliates. Transfers to affiliates would be subject to the opt-out consent requirements described above. The bill would require a different consent standard for data transfers to third parties. A first party would be required to obtain the express affirmative consent of an individual to whom the covered information relates before transferring data to third parties.

If an individual later declines consent after an initial collection of information, the covered entity must stop collecting information and must not use any information that was collected earlier. Sec. 3(a)(3)(A). However, the bill does not appear to require that the individual be presented with repeated opportunities to decline consent.

The bill would permit covered entities to give individuals the option of declining consent for the collection and use of some covered information while granting consent for other information. However, it appears that the individual still must be given the opportunity to decline consent for the collection and use of all covered information, in the form of an all-or-nothing choice. Sec. 3(a)(3)(B).

## ***Express Consent Required for Disclosure of Covered Information to Unaffiliated Parties***

Notwithstanding the opt-out requirement set forth above, section (3)(b) of the bill would require a "covered entity" to obtain the *express affirmative consent* of an individual before selling, sharing, or

---

<sup>2</sup> Sec. 3(a)(2)(B). In addition to including a hyperlink or listing of the FTC's online consumer complaint form, the bill would require online privacy notices to include the following information: (1) the covered entity's identity; (2) a description of the collected covered information; (3) how the covered entity collects the information; (4) specific purposes for which the covered entity collects or uses such information; (5) how the covered entity stores the information; (6) how the covered entity may merge, link, or combine the information with other information about the person obtained from unaffiliated parties; (7) how long the covered entity retains the information in identifiable form; (8) after the retention period ends, how the covered entity disposes of or renders anonymous the information; (9) when the information may be disclosed and the categories of unaffiliated parties who may receive the information for those purposes; (10) the choice and means the covered entity provides individuals to limit or prohibit the collection and disclosure of their information; (11) how individuals may access the collected information; (12) how an individual can contact a covered entity with questions or complaints regarding handling of the information; (13) how covered entities notify individuals of material changes to the covered entities' privacy notices; and (14) the effective date of the policy. Sec. 3(a)(2)(B).

otherwise disclosing “covered information” to an “unaffiliated party.”<sup>3</sup> This requirement would be a departure from current industry practice and standards, which do not require first parties to obtain affirmative consent for all transfers to third parties for marketing purposes. In addition, the bill would require a covered entity that has acquired express affirmative consent from an individual to provide a means, without charge, to withdraw consent at any time. Sec. 3(b)(2).

The bill, however, contains a limited service provider exception. Under this provision, a covered entity would not be required to obtain express affirmative consent to disclose covered information to a service provider for the purpose of executing a “first party transaction” if: (1) the covered entity has obtained consent (*i.e.*, opt-out consent) for the collection of covered information, and (2) the service provider agrees to use such covered information solely for the purpose of providing an agreed-upon service to the covered entity and not to disclose the covered information to any other person. A “first party transaction” refers to “an interaction between an entity that collects covered information when an individual visits that entity’s website or place of business and the individual from whom covered information is collected.” Sec. 2(6).

### ***Material Changes to Privacy Practices***

The bill would require a covered entity to obtain express affirmative consent *before* making a “material change” in privacy practices that govern information previously collected from an individual or disclosing covered information for a purpose that was not previously disclosed and which the individual “acting reasonably under the circumstances would not expect” based on the prior privacy notice. Sec. 3(a)(4). The term “material change” is not defined. Current best practices and certain legal requirements require companies to set forth the methods by which they will notify consumers about changes in their privacy policies, and then determine what types of notice and/or choices are appropriate under the circumstances.

### ***Exemptions from Notice and Consent Requirements***

As described in more detail below, the bill would provide limited exemptions from the general notice and opt-out consent requirements for certain first party collection and use of information, but these exemptions would not extend to the collection of data for marketing, advertising, or sales purposes, or any use of or disclosure of covered information to an unaffiliated party for such purposes.

Specifically, the bill provides exemptions from the notice requirements for:

- Covered information that is collected offline *and*
- Is collected for a “transactional purpose” or an “operational purpose”; *or*
- Consists solely of a name, address, telephone/fax number, and/or email address and is part of a “first party transaction.”<sup>4</sup>

In addition to providing for these exemptions from the *notice* requirements for certain offline collections, the bill would also exempt certain actions from the *consent* requirements. Specifically, the bill would not require consent for the collection, use, or disclosure of covered information for: (1) a “transactional purpose,” which means a “purpose necessary for effecting, administering, or enforcing a transaction between a covered entity and an individual,” or (2) an “operational purpose,” not including marketing, advertising or selling. Sec. 3(a)(5). This exemption from the consent requirement does not appear to be limited to the offline context.

---

<sup>3</sup> Sec. 3(b)(1). An “unaffiliated party” is defined to mean “any entity that is not related by common ownership or affiliated with a covered entity.” Sec. 2(13).

<sup>4</sup> Sec. 3(a)(5). A “first party transaction” refers to “an interaction between an entity that collects covered information when an individual visits that entity’s website or place of business and the individual from whom covered information is collected.” Sec. 2(6).

An “operational purpose” is defined to mean a purpose “reasonably necessary” for the operation of the covered entity, and the bill provides various illustrations of activities that would be deemed to be operational, such as order fulfillment, analyzing data related to the product or service, and fraud detection.<sup>5</sup> For such operational purposes as well as for transactional purposes, notice would generally be required if information is collected online but not if collected offline, and consent would not be required for either offline or online collection, use or disclosure.

However, notably, the term “operational purpose” specifically excludes “the use of covered information for marketing, advertising, or sales purposes, or any use of or disclosure of covered information to an unaffiliated party for such purposes.” Sec. 2(7)(B). Thus, the “operational purpose” exemptions from the notice and opt-out consent requirements would not apply to the collection, use or disclosure of covered information for marketing, advertising, or selling purposes. Sec. 3(a)(5)(A). Because many covered entities collect covered information precisely for marketing purposes or share such information with unaffiliated parties for marketing purposes, many entities would not be in a position to use this exemption. Indeed, disclosures to unaffiliated parties for marketing as well as other purposes would be subject to the express affirmative consent requirement described above.

### ***Express Consent for Collection or Disclosure of Sensitive Information***

The bill would impose limitations on the collection or disclosure of “sensitive information.” In particular, before a covered entity would be permitted to *collect or disclose* sensitive information from or about an individual for any purpose, pursuant to Section 3(c), a “covered entity” would be required to provide a privacy notice (as provided in Section 3(a)(2)) *and* obtain the prior express affirmative consent of the individual. The definition of “sensitive information” tracks in many respects that which is used in the European Union. More specifically, “sensitive information” would be defined as “any information that is associated with covered information of an individual and relates to that individual’s: (A) medical records, including medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; (B) race or ethnicity; (C) religious beliefs; (D) sexual orientation; (E) financial records and other financial information associated with a financial account, including balances and other financial information; or (F) precise geolocation information.” Sec. 2(10).

### ***Express Consent for Collection or Disclosure of All or Substantially All of an Individual’s Online Activity***

The bill would require entities that collect or disclose covered information about all or substantially all of individual’s online activity, including across websites, for any purpose, to provide a privacy notice and obtain the express affirmative consent of the individual to whom the information relates prior to collecting or disclosing such covered information. Sec. 3(d)

---

<sup>5</sup> Sec. 2(7)(A). The activities that the bill lists as being operational are (emphasis supplied):

- “(i) providing, operating, or improving a product or service used, requested, or authorized by an individual;
- (ii) detecting, preventing, or acting against actual or reasonably suspected *threats to the covered entity’s product or service*, including security attacks, unauthorized transactions, and *fraud*;
- (iii) *analyzing data related to use of the product or service for purposes of optimizing or improving the covered entity’s products, services, or operations*;
- (iv) carrying out an employment relationship with an individual;
- (v) disclosing covered information based on a good faith belief that such disclosure is necessary to comply with a Federal, State, or local law, rule, or other applicable legal requirement, including disclosures pursuant to a court order, subpoena, summons, or other properly executed compulsory process; and
- (vi) disclosing covered information to a parent company of, controlled subsidiary of, or affiliate of the covered entity, or other covered entity under common control with the covered entity where the parent, subsidiary, affiliate, or other covered entity operates under a common or substantially similar set of internal policies and procedures as the covered entity, and the policies and procedures include adherence to the covered entity’s privacy policies as set forth in its privacy notice.” Sec. 2(7)(A).

### ***Exception for Individual Managed Preference Profiles***

The bill's only exception to the requirement that an entity that shares information with unaffiliated parties obtain prior express affirmative consent is found in Section 3(e). This exception contains requirements that are far more stringent than industry standards for choice and transparency. Specifically, the bill would permit a covered entity to disclose covered information to unaffiliated third parties without prior express affirmative consent if all of the following four requirements are met:

- (1) *Opt out*: the covered entity provides individuals with the ability to opt-out of collection, use, and disclosure of covered information through a readily accessible opt-out mechanism (e.g., Internet mechanism, a toll-free number, or letter to address provided by the covered entity) and the opt-out choice is preserved and protected from incidental or accidental deletion;
- (2) *Data purging*: the covered entity deletes or renders anonymous any covered information not later than 18 months after the date the covered information is first collected;
- (3) *Access to profiles*: the covered entity places a symbol or seal in a prominent location on its website and on or near any advertisement delivered by the covered entity based the preference profile of an individual and the symbol or seal enables an individual to link to additional information that
  - (A) describes the practices used by the covered entity or by an advertisement network in which the covered entity participates to create a preference profile and that led to the delivery of the advertisement using an individual's preference profile, including the information, categories of information, or list of preferences associated with the individual that may have led to the delivery of the advertisement to that individual; and
  - (B) allows individuals to review and modify, or completely opt out of having, a preference profile created and maintained by a covered entity or by an advertisement network in which the entity participates; and
- (4) *Opt in for redisclosures*: an advertisement network to which the covered entity discloses covered information does not disclose the information to any other entity without the express affirmative consent of the individual to whom the covered information relates.

The term "render anonymous" means to remove or obscure covered information such that the remaining information provides "no reasonable basis" to identify either the specific individual to whom the information relates or a computer or device owned or used by a particular user.

### **Section 4. Accuracy and Security**

The bill would impose obligations on companies to establish reasonable procedures to ensure the accuracy of covered information. Sec. 4(a). Covered entities that collect covered information about an individual for any purpose would be required to establish, implement and maintain administrative, technical, and physical safeguards that the FTC determines are necessary, and the bill sets out factors that the FTC must consider in developing such standards. Sec. 4(b). The bill would require the FTC to educate the public about their opt-out and opt-in rights. Sec. 4(c).

### **Section 5. Anonymous Information**

The bill would not prevent businesses from collecting or disclosing aggregated information or information that has been rendered anonymous within the definition of the bill.

### **Section 6. Location-Based Information**

In general, the bill would require product or service providers that use location-based information not to disclose such information without the express opt-in consent of the user. The bill would also establish that location-based information is “call location information” that falls within the Communications Act’s prohibition on disclosure of such information without a customer’s express prior authorization.

### **Section 7. Report to Congress from FCC**

The bill would require the Federal Communications Commission (“FCC”) to report to Congress within one year after the bill’s enactment and describe communication laws on subscriber privacy and how those laws may be harmonized with this bill.

### **Section 8. Enforcement**

The bill would give the FTC authority to enforce the bill; a violation would constitute an unfair or deceptive act or practice in violation of the FTC Act. The bill would also provide the FTC with rulemaking authority to issue regulations to implement the bill under the procedures prescribed in the Administrative Procedure Act, but states that the FTC may not require the deployment or use of any specific products or technologies. Sec. 8(a). Additionally, the bill would provide the State attorneys general or state consumer protection agencies the authority to bring civil suits. The FTC would have the right to intervene in such an action. Sec. 8(b).

### **Section 9. No Private Right of Action**

The bill would not give individuals a private right of action.

### **Section 10. Preemption**

The bill would supersede any state regulation on collecting, using, or disclosing covered information.

### **Section 11. Effect on Other Laws**

Subject to its provisions, the bill would not affect other federal privacy laws.<sup>6</sup>

### **Section 12. Effective Date**

The bill would take effect one year after the bill's enactment.

---

<sup>6</sup> Specifically, the bill would have “no effect” on the activities covered by the following laws: (1) Title V of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.); (2) The Fair Credit Reporting Act (15 U.S.C. 1681 et seq.); (3) The Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191); (4) Part C of title XI of the Social Security Act (42 U.S.C. 1320d et seq.); (5) The Communications Act of 1934 (47 U.S.C. 151 et seq.); (6) The Children's Online Privacy Act of 1998 (15 U.S.C. 6501 et seq.); and (7) The CAN-SPAM Act of 2003 (15 U.S.C. 7701 et seq.).