
**ATTORNEY-CLIENT COMMUNICATION
PRIVILEGED & CONFIDENTIAL**

TO Interactive Advertising Bureau FROM Venable LLP RE Summary of Rep. Rush's H.R. 5777, the BEST PRACTICES Act	DATE July 26, 2010 EMAIL singis@venable.com PHONE 202-344-4613
---	---

On July 19, 2010, Rep. Bobby Rush (D-IL), Chairman of the House Energy and Commerce Committee's Subcommittee on Commerce, Trade, and Consumer Protection introduced H.R. 5777, the "Building Effective Strategies To Promote Responsibility Accountability Choice Transparency Innovation Consumer Expectations and Safeguards Act" ("BEST PRACTICES Act"). This bill builds on the discussion draft released by Rep. Rick Boucher (D-VA) in May 2010, but includes several significant differences.

Like Rep. Boucher's bill, the BEST PRACTICES Act 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. The bill would also effectively require opt-in consent for the transfer of personal data to third parties except in limited circumstances.

However, Rep. Rush's bill takes a different approach in providing a safe harbor under which entities that comply with approved self-regulatory programs are not subject to certain requirements. In particular, participating companies would be permitted to transfer data to third parties subject to an opt-out. Our summary focuses on this new development in the first section below. Another significant aspect of this bill that is different from Rep. Boucher's draft is the inclusion of accuracy, access, and dispute resolution provisions. A brief summary of the bill follows.

Title IV. Safe Harbor and Self-Regulatory Choice Program

A significant difference between Rep. Rush's bill and the discussion draft circulated by Rep. Boucher is the addition of a safe harbor for "covered entities"¹ that comply with a self-regulatory program. Sec. 401.

¹ A "covered entity" is defined in the legislation as "a person engaged in interstate commerce that collects or stores information containing covered information or sensitive information." Excluded from this definition are government entities and any person that can demonstrate that it meets all of the following criteria: stores covered information from or about fewer than 15,000 individuals, collects covered information from or about fewer than 10,000 individuals in any 12-month period, does not collect or store "sensitive information," and does not use covered information to study, monitor, or analyze the behavior of individuals as the person's primary business. Sec. 2(3).

Rep. Rush's legislation would provide that a covered entity that participates in and is compliant with a Commission-approved self-regulatory "Choice Program" is exempt from the following significant aspects of the bill: (1) obtaining consumers' affirmative express consent for information uses that are covered by the self-regulatory program; (2) providing consumers with access to information as Title II of the bill would otherwise require; and (3) liability in private lawsuits. Sec. 401. This title has the effect of giving an entity the option of providing a high level of transparency to consumers coupled with an opt-out mechanism, as an alternative to providing notice coupled with affirmative express consent, for third-party information disclosures. However, the legislation's opt-out consent requirements for first-party data collection and use would still apply. *See* Sec. 401.

The legislation would task the Commission with reviewing and deciding on applications to administer self-regulatory Choice Programs. Sec. 402. Decisions on initial applications would be made within 270 days, using a notice and comment procedure. Sec. 402(a). The Commission would be granted with authority to approve any material changes to a program. Applications for a material change to a program would be decided within 120 days. Sec. 402(b).

In order to be approved by the Commission, among other requirements, a Choice Program must:

- Provide individuals a clear and conspicuous **opt-out** mechanism that, when selected by the individual, prohibits all covered entities participating in the Choice Program from disclosing covered information to a "third party"² for specified uses, which could take the form of a preference management tool that permits more detailed choices;
- Provide individuals a clear and conspicuous mechanism for setting preferences that will apply to all covered entities in the Choice Program regarding communication, online behavioral advertising, and other issues;
- Establish guidelines and procedures requiring a covered entity to provide protections at least equivalent to those the legislation would provide in the areas of transparency, notice, and individual choice (Title I) and accuracy, access, and dispute resolution (Title II);

The Commission would be authorized to promulgate regulations that set forth criteria for opt-out mechanisms and communication and online behavioral advertising preferences that meet the law's requirements. Sec. 404.

² The term "third party" refers to persons that are not related by common ownership or corporate control to a covered entity. Sec. 2(10)(A)(i). Notably, "third party" is also defined to include business units or entities that hold themselves out to be a separate entity "such that an individual acting reasonably under the circumstances would not expect it to be related to the covered entity or to have access to covered information the individual provides to that covered entity." Sec. 2(10)(ii).

Title I. Transparency, Notice, and Individual Choice

Rep. Rush's bill would establish a transparency framework in which "covered entities" that collect "covered information" or "sensitive information"³ from individuals would be required to provide notice of the entities' information privacy practices and choice with respect to those practices.⁴ Sec. 101. The term "covered information" would refer to various information that identifies individuals, and equates less-sensitive identifiers such as names with traditionally more sensitive identifiers such as credit card numbers. More specifically, the term refers to any of the following: (1) a first name or initial and last name; (2) a postal address; (3) email address; (4) a phone or fax number; (5) a tax identification number, passport number, driver's license number, or any other unique government-issued identification number; (6) a financial account number, or credit card or debit card number, or any required security code, access code, or password that is necessary to permit access to an individual's financial account, (7) *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 to create or maintain a *preference profile*; or (8) *any other information* collected, stored, used, or disclosed in connection with any covered information described above. Sec. 2(4) (emphasis added). The unique persistent identifier provision of Rush's bill is narrower than Boucher's and would not capture weblogs, serving advertisements, or contextual advertisements. Also unlike the Boucher draft, the definition in Rush's bill excludes business information, such as employees' business email addresses and information collected about employees by employers that relates to the employment relationship. Sec. 2(a)((B).

Explanation of Choices and Options

Covered entities that collect covered information or sensitive information from individuals, would be required to provide an explanation of the choices and options available to the individuals. In addition, the bill would require a covered entity to make available a very prescriptive list of information to the individuals.⁵ Sec. 102(1)-(13).

³ The term "sensitive information" would include information that is associated with covered information of an individual that relates directly to that individual's: (1) medical history, physical or mental health, or the provision of health care to the individual; (2) race or ethnicity; (3) religious beliefs and affiliation; (4) sexual orientation or sexual behavior; (5) income, assets, liability, or financial records, and other financial information associated with a financial account; or (6) precise geolocation information and information about the individual's activities and relationships associated with the geolocation. Sec. 2(8)(A)(i). Unique biometric data and Social Security numbers would also be captured within the definition of "sensitive information." Sec. 2(8)(A)(ii).

⁴ See Appendix for key defined terms.

⁵ The bill would require covered entities to provide: (1) the covered entity's identity; (2) a description of the covered information or sensitive information collected or stored; (3) the purposes for collection, use, or disclosures of such information; (4) when such information may be disclosed to a "third party" ; (5) choice for limiting collection, use, and disclosure of such information; (6) a description of the information to which an individual has access and how the individual may request the access; (7) how such information may be merged, linked, or combined with other information about the person from third parties; (8) the retention schedule of such information; (9) whether individuals may delete the information; (10) a reasonable means to contact the covered entity; (11) the covered entity's process for notifying individuals of material changes to policies; (12) a hyperlink or listing of the FTC's

Provision of Notice

The bill would require covered entities to provide concise, meaningful, timely, prominent, and easy-to-understand notice before collecting, using, or disclosing covered information or sensitive information. Sec. 102(a). The FTC would have authority to authorize use of short notices or limited disclosures. Sec. 102(b)(2). The bill also anticipates that the Commission could issue model notices. Sec. 102(b)(4).

The bill provides a limited exclusion from the notice requirements for collection of information for an “operational purpose.” The term “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 a product or service, and defending the rights or property of a covered entity against fraud.⁶ Notably, however, the term “operational purpose” specifically excludes “the use of covered information for marketing or advertising purposes, or any use of or disclosure of covered information to a third party for such purposes,” as well as the use of information for purposes a person acting reasonably would not expect. Sec. 2(5)(B). Thus, the “operational purpose” exemption from the notice requirement would not apply to the collection, use, or disclosure of covered information for marketing or advertising purposes. Sec. 102(c)(2). Because many covered entities collect covered information precisely for marketing or advertising purposes, many entities would not be in a position to use this exemption. The Boucher bill addresses the above concept in its definitions of “operational purpose” and “transactional purpose.”

Exclusion from Notice for In-Person Transactions

The bill would not require covered entities to provide notice when the collection of covered information takes place *in-person* so long as the information is collected for an

complaint form or toll-free number to the FTC’s Consumer Response Center; and (13) the privacy notice’s effective date. Sec. 102(1)–(13).

⁶ The activities that the bill identifies as being for an “operational purpose” include: “(i) providing, operating, or improving a product or service used, requested, or authorized by an individual, including the ongoing provision of customer services and support; (ii) analyzing data related to use of the product or service for purposes of improving the covered entity’s products, services, or operations; (iii) basic business functions such as accounting, inventory and supply chain management, quality assurance, and internal auditing; (iv) protecting or defending the rights or property, including intellectual property, of the covered entity against actual or potential security threats, fraud, theft, unauthorized transactions, or other illegal activities; (v) preventing imminent danger to the personal safety of an individual or group of individuals; (vi) complying 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 (vii) any other category of operational use specified by the Commission by regulation that is consistent with the purposes of this Act.” Sec. 2(5)(A). The term “operational purpose” specifically excludes “the use of covered information for marketing or advertising purposes, or any use of or disclosure of covered information to a third party for such purposes,” as well as the use of information for purposes a person acting reasonably would not expect. Sec. 2(5)(B).

“operational purpose” or when the entity is only collecting certain information (name, address, email, phone, or fax) and does not share the information with third parties or use it to acquire more information about the person from third parties. Sec. 102(c)(2).

Opt-Out Consent for First-Party Collection and Use of Covered Information

The bill would generally impose an obligation on first parties to provide an opt-out before collecting and using covered information for their own purposes, including marketing. Sec. 103(a). Pursuant to the bill, a covered entity would be deemed to have obtained the requisite consent if the entity provides the individual: (1) notice; (2) a means to opt-out; and (3) the individual affirmatively grants consent by not opting out. Sec. 103(a)(1)-(2). The bill notes that the opt-out requirement would not apply to covered information collected for “operational purposes.” Sec. 103(e). The duration of an individual’s opt-out would be permanent unless directed otherwise by the individual. Sec. 103(b). The bill specifies that a covered entity would be required to provide an individual with a reasonable means to decline consent or revoke previously granted consent at any time. Sec. 103(c).

Conditioning Service

In a significant change from the Boucher draft, the bill would permit covered entities to condition the provision of a service or other benefit on requiring the collection and use of personal information. Sec. 103(f). An entity could impose such a condition so long as: (1) the entity has a direct relationship with the person, (2) the personal information is not shared with a third party without express affirmative consent, (3) the entity provides a disclosure describing the purposes for which the information may be used, (4) the person provides consent, and (5) the option remains for the person to later withdraw their consent. Sec. 103(f).

Express Affirmative Consent

The bill would require *prior express affirmative consent* for an entity to disclose personal information to a third party. Sec. 104(a). In another improvement from the Boucher draft, such consent would not be required for joint marketing provided that the covered entity enters into a contractual arrangement prohibiting the joint marketer from disclosing or using the information except as necessary to carry out the arrangement. Sec. 104(a)(2). Additionally, the bill would require express affirmative consent for the collection, use, or disclosure of sensitive information. Sec. 104(b).

Express affirmative consent would also be required for the use of hardware or software to monitor all or substantially all of a person’s Internet browsing or other Internet or computer activities, and for the collection, use, or disclosure of such information. Sec. 104(c).

The bill provides that a third party that receives covered information or sensitive information that was collected after a covered entity obtained express affirmative consent may

only use that information for the purposes originally authorized by the individual when that person granted the consent. Sec. 104(d).

The bill would require covered entities to provide persons an opportunity to withdraw the express affirmative consent at any time. Sec. 104(e). Unlike the Boucher bill, if a person later revoked consent, the Rush bill would not prohibit a covered entity from using the previously collected information.

Material Changes to Privacy Practices

The bill addresses material changes to privacy practices in the context of retroactive and prospective applications. This is another improvement from the Boucher draft and reflects current law as outlined in FTC enforcement actions. For retroactive applications, the bill would require a covered entity to obtain express affirmative consent before making a material change to information collected previously under a privacy policy. Sec. 105(a). For prospective applications, the bill would require a covered entity to provide 30 days notice before the effective date of the material change and to obtain consent to the material change or to permit the person to terminate the relationship with the covered entity in circumstances where the change would necessitate an opt-out or opt-in described above. Sec. 105(b).

Exceptions

The bill details various scenarios where the opt-out and express affirmative consent requirements would not apply. For instance, these consent requirements would not apply to the disclosure of such information to service providers performing services on behalf of and at the instruction of covered entities so long as the covered entity obtained the initial requisite consent, a contractual agreement prohibiting the service provider from disclosing the information for purposes other than to carry out the agreement, and the covered entity remains responsible for the protection of the information. Sec. 106(1). Unlike the Boucher draft, the exception would also apply to service providers that subsequently disclose information to other service providers to perform functions on behalf of a covered entity. Sec. 106(1)(B). The bill would also provide an exemption for the collection, use, or disclosure of “publicly available information,”⁷ provided that a covered entity would not be permitted to use that information about an individual for marketing purposes if the person had opted out of the covered entity’s use of covered or sensitive information for marketing purposes. Sec. 106(5). This public record exception does not appear in the Boucher bill and appears to be modeled on the Gramm-Leach-Bliley Act. Additionally, the bill provides exemptions for fraud detection,⁸ imminent danger, and compliance with federal, state or local law. Sec. 106(2)-(4).

⁷ “Publicly available information” is defined as any covered or sensitive information that the entity has a “reasonable basis to believe is lawfully made available to the general public” from government records, widely distributed media, or legally-required disclosures to the general public. Sec. 2(7).

⁸ The “fraud detection” provision would exclude the following from the consent requirements: “Collection, use, or disclosure necessary to protect or defend the rights or property, including intellectual property, of the covered entity

Title II. Accuracy, Access, and Dispute Resolution

Rep. Rush's legislation would establish requirements for accuracy, access and dispute resolution for covered entities that do not participate in a Commission-approved self-regulatory program. Rep. Boucher's circulated bill does not contain such requirements.

Requirement to Assure Accuracy

The bill would generally require covered entities to establish "reasonable procedures to assure the accuracy" of covered or sensitive information that the entity "collects, assembles, or maintains." Sec. 201(a). The Commission would be tasked with issuing implementing regulations that take into account the costs and benefits of ensuring accuracy, the sensitivity of information, the purposes of information, and the harms of misuse. Sec. 201(a).

However, the legislation includes limited exceptions from this accuracy requirement for fraud databases and "publicly available information."⁹ Secs. 201(b)-(c). Entities would not be required to verify independently the accuracy of publicly available information as long as the entity has reasonable procedures to ensure that the information it assembles or maintains accurately reflects the information available to the public. Sec. 201(c). The legislation also includes an exemption from the accuracy requirement when information is collected or maintained solely for the purpose of indicating a "discrepancy or irregularity" in the information associated with an individual and is used for identification or to protect against or investigate fraud or "other unlawful conduct." Sec. 201(b).

Individual Access and Dispute Resolution Rights

For any covered or sensitive information that "may be used for purposes that could result in an adverse decision against" an individual, the bill would require covered entities to give individuals, upon request, reasonable access to their information that the entity retains for more than 30 days, and a way to dispute the accuracy or completeness of such information. Sec. 202. The bill does not define what constitutes as "adverse decision." If an entity declined to correct or amend the information when requested, the entity would be required to note that the information is disputed, including the individual's statement on the matter; take reasonable steps to verify the accuracy of the information; and, if the information was obtained from a third party or is publicly available, provide the individual with certain details about requesting correction from the information source. Sec. 202(h)

against actual or potential security threat, fraud, theft, unauthorized transactions, or other illegal activities." Sec. 106(2).

⁹ "Publicly available information" is defined as any covered or sensitive information that the entity has a "reasonable basis to believe is lawfully made available to the general public" from government records, widely distributed media, or legally-required disclosures to the general public. Sec. 2(7).

The legislation also appears to treat marketing information as a special category that triggers individual access and correction rights. The legislation would require covered entities to provide individuals with reasonable access to any “personal profile” stored in a manner that makes it accessible in the normal course of business. Sec. 202(b). The scope of this provision is unclear because the term “personal profile” is not defined. However, the legislation also appears to require an entity to provide an individual with “access and correction” rights to marketing-related “preference profile”¹⁰ and allow an individual to review and change the preference information associated with a unique persistent identifier. Sec. 202(b)(2). This provision could be interpreted as requiring any company to provide individuals with access to all marketing data. As discussed above, an entity that participates in a Commission-approved self-regulatory program would be exempt from these requirements. Sec. 202(b)(3).

For information that would not reasonably result in an adverse decision against the individual and is not a personal profile, entities would merely be required to provide, upon request, a general notice or representative sample of the information typically stored or collected. Sec. 202(c). Unlike specific access, this type of general description of how information is used is more reasonable.

In addition, a covered entity could deny an individual’s access request if, and to the extent that, the entity reasonably believes:

- The requestor’s identity cannot be verified;
- Access is limited by law or legally recognized privilege;
- Information is used for a governmental or fraud prevention purpose that would be compromised by providing access;
- A request is frivolous or vexatious;
- A request would violate the privacy or other rights of other persons; or
- Proprietary or confidential information, technology, or business processes would be revealed. Sec. 202(d)(1).

Requests to correct or amend information could be declined for the same reasons, and could also be declined if correction or amendment would be incompatible with another legal obligation. Sec. 202(d)(3).

Entities would be permitted to charge a reasonable fee for individual information access. Sec. 202(e). Entities would be required to respond to any access, correction, or amendment

¹⁰ A “preference profile” is defined as a list of preferences, information categories, or interests that is: (1) associated with an individual or an individual device; (2) either supplied by the individual or inferred from an individual’s behavior or device use; and (3) compiled and maintained for marketing, advertising or sales purposes. Sec. 2(6).

request within 30 days of receipt, and would be limited to certain permitted types of responses.¹¹ Sec. 202(f). While the bill would require notices to disclose where a person has a right to delete personal information, Sec. 101(9), the bill does not require covered entities to offer individuals such a right to have their information deleted. Sec. 202(g). The bill also stipulates that the individual rights provided in this section would not obligate a covered entity to retain, maintain, reorganize, or restructure information. Sec. 202(i).

The Commission would be charged with issuing implementing regulations within 18 months of enactment, and the legislation specifically states that the Commission may set forth additional circumstances in which a covered entity may limit access to information. Sec. 202(k).

Title III. Data Security, Data Minimization, and Accountability

Data Security

The bill would require covered entities and service providers to establish, implement, and maintain reasonable and appropriate administrative, technical, and physical safeguards to--

- ensure the safety, security, and confidentiality of “covered information” or “sensitive information” it collects, assembles, or maintains;
- protect against any anticipated threats, reasonably foreseeable vulnerabilities, or hazards to the security or integrity of such information; and
- protect against unauthorized access to or use of such information and loss, misuse, alterations, or destruction of such information.

The Commission would be authorized to issue regulations concerning reasonable and appropriate safeguards. The bill sets forth several factors for the Commission to consider as it promulgates rules. Sec. 301.

Accountability

The bill would obligate a covered entity to: (1) provide a process for individuals to make complaints concerning the covered entity’s policies and procedures, (2) perform privacy risk assessments, and (3) undertake periodic evaluations of its practices. In particular, a covered entity that collects covered information or sensitive information from or about more than 1,000,000 individuals would be required to assess the risks to individuals raised by the collection, use, and disclosure of this information prior to the implementation of commercial

¹¹ Specifically, an entity could respond with one or more of the following: (1) the requested information, (2) the general notice permitted as an alternative to access for certain information, (3) instructions for using an automated mechanism to complete the request, (4) a confirmation that the correction or amendment request has been completed, (5) a notification that the entity is declining to correct or amend the information and the reasons for the decline, (6) a request to resubmit if the request was deficient in certain respects, or (7) a notification that additional time is needed up to 30 more days. Sec. 202(f).

projects, marketing initiatives, business models, applications, and other products or services that use such information. Sec. 302. A covered entity would also be required to conduct periodic assessments to evaluate whether the covered information or sensitive information collected remains necessary for the purposes disclosed at the time of collection and whether the ongoing collection practices are and remain necessary for legitimate business purpose. Sec. 302.

Data Minimization Obligations

The bill would require a covered entity that uses covered information or sensitive information for any purpose to retain such data as long as necessary to fulfill a legitimate business purpose or comply with a legal requirement. Sec. 303.

Title V. Exemptions

Rep. Rush's bill would include two general exemptions. First, the legislation states that nothing in the legislation would preclude a covered entity from collecting using, or disclosing (1) aggregate information or (2) covered information or sensitive information from which identifying information has been "obscured or removed using reasonable and appropriate methods" such that there is no reasonable basis to believe that the information could be used to identify a specific individual or "a computer or device that is owned or used by a specific individual." Sec. 501(a). It is not clear from this language whether information that identifies a specific device, without associating the device with an individual, would qualify for the exemption.

If a covered entity disclosed such aggregate or de-identified information to a third party, the entity would still be required to take reasonable steps to protect the information, including obtaining reasonable assurance that the third party will not attempt to reconstruct the information and not disclosing the algorithm or other mechanism used to de-identify the information. Sec. 501(b). The legislation would generally prohibit reconstructing or revealing the information that has been removed or obscured from de-identified data if an entity claims the benefit of the exemption, but directs the Commission to promulgate rules within 18 months to establish exemptions from this rule against re-identifying information. Sec. 501(c).

Other than as expressly provided, the legislation would have no effect on activities covered by the following federal privacy laws:

- Title V of the Gramm-Leach-Bliley Act;
- Fair Credit Reporting Act;
- Health Insurance Portability and Accountability Act (HIPAA);
- Part C of title XI of the Social Security Act;
- Children's Online Privacy Protection Act;
- CAN-SPAM Act of 2003;

- Electronic Communications Privacy Act;
- Video Privacy Protection Act; and
- Communications Act of 1934 provisions on the protection of personally identifiable information acquired by cable operators (Section 631) and of customer proprietary network information (Section 222). Sec. 502.

Title VI. Application and Enforcement

Scope of Authority

The requirements of Rep. Rush's legislation would apply to persons over which the Commission has authority pursuant to Section 5(a)(2) of the Federal Trade Commission Act. In addition, the bill would provide the Commission with jurisdiction over "common carriers," as defined in the Communications Act of 1934, for purposes the Act. Sec. 601. Violations of Titles I-III would be treated as unfair and deceptive acts or practices in violation of a trade regulation rule, thereby empowering the Commission to seek civil penalties.¹² Sec. 602(a). The legislation would not grant civil penalty authority for violations of title V, and thus the Commission would be limited to injunctive relief for such violations.

In addition to the specific grants of rulemaking authority discussed above, the Commission would also receive general authority to issue regulations necessary to carry out the law, including additional exemptions consistent with the purposes of the law. Sec. 602(c). However, the Commission would not be able to require the deployment or use of any specific products or technologies. Sec. 602(c)(3).

Private Right of Action

Notably, unlike Rep. Boucher's circulated legislation, Rep. Rush's bill would establish a private right of action against any covered entity that willfully fails to comply with Section 103 (opt-out consent for first-party collection or use) or Section 104 (express affirmative consent for disclosure to third parties) of the bill. Sec. 604. Covered entities that participate in and are in compliance with a Commission-approved Choice Program are exempt from such liability. Sec. 604(a). Individuals may seek actual damages of \$100-\$1000, punitive damages as allowed by the court, and legal costs. Sec. 604(a). A two-year statute of limitations would apply. Sec. 604(b).

Enforcement by State Authorities

The law would also be enforceable by state attorneys general or other state authorities with reason to believe that residents' interests have been or are threatened or adversely affected by a violation. Sec. 603. Such state authorities may seek to enjoin further violations or to compel compliance. Sec. 603(a). In a change from the Boucher draft, the state authorities could also

¹² 15 U.S.C. § 45(m).

obtain civil penalties for violations of Titles I-III. Sec. 603(a). Civil penalties for a violation of Title I would be available up to \$11,000 per day of noncompliance or number of individuals for whom consent was not obtained (subject to automatic adjustments for inflation), up to a maximum total of \$5 million. Sec. 603(b). Civil penalties for a violation of Title II would be available up to \$11,000 per day of noncompliance (subject to automatic adjustments for inflation), up to a maximum total of \$5 million. Sec. 603(b). These caps are similar to those found in the H.R. 2221 bill passed by the House. In calculating civil penalties, a court may take into account an entity's participation in a Choice Program and whether the entity cures an alleged violation of Titles I or II in a reasonable period of time. Sec. 603(b)(4).

State authorities would be required notify the Commission of any action against an alleged violator, and the Commission would have the right to intervene in the case. Sec. 603(c)(1). Moreover, state authorities would not be permitted to bring an action while a Commission case is pending against the same defendant. Sec. 603(c)(2).

Preemption

The legislation would preempt state laws or rules that expressly require covered entities to implement requirements with respect to the collection, use or disclosure of covered information. Sec. 605(a). The legislation would also prevent civil actions premised on a violation of the law except state authorities and individuals as permitted by the law. Sec. 605(b)(1). However, it would not limit enforcement of state consumer protection laws by state authorities, nor would it preempt state laws on health and financial data; breach notification; trespass, contract or tort; or fraud. Sec. 605(b)(2); Sec. 605(c).

The legislation would not be construed to limit or affect the Commission's authority, or to expand or limit the duty or authority of a covered entity, service provider, or third party to disclose covered or sensitive information to a government entity. Secs. 605(d)-(e).

Title VII. Miscellaneous Provisions

The legislation would require the Commission to review and report to Congress on the law's implementation and effect within five years. Sec. 701.

The Commission would be tasked with conducting a consumer education campaign to inform individuals of their rights under the legislation and the steps they could take to consent or decline consent to the collection, use and disclosure of information, as well as to provide compliance guidance to businesses. Sec. 702.

The legislation would take effect two years after enactment, but the Commission would be permitted to stay enforcement as determined necessary to allow for the establishment of and participation in approved Choice Programs. Sec. 703.

* * *

Please contact us with questions.