KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

CDT submits the following chart as an addendum to the written testimony of Leslie Harris, President and Chief Executive Officer of the Center for Democracy and Technology before the House Committee on Energy and Commerce, Subcommittee on Commerce, Trade, and Consumer Protection on "The BEST PRACTICES Act of 2010 and Other Federal Privacy Legislation" on July 22, 2010. The chart compares some of the key provisions in both bills, and issues CDT's recommendations about the approach we believe privacy legislation should take. To make comments, or to receive further information, contact Justin Brookman, Senior Resident Fellow at the Center for Democracy & Technology, justin@cdt.org; 202-407-8827.

Issue	Boucher-Stearns Discussion Draft	BEST PRACTICES	CDT Recommendation
Scope. Definition of "covered entities"	Applies to all persons engaged in interstate commerce that collect "covered information," except government agencies or persons who collect covered information from fewer than 5000 individuals in any 12-month period and do not collect "sensitive information." §2(4).	Applies to all persons engaged in interstate commerce that collect or store "covered information" or "sensitive information," except government agencies or persons that (i) store info from 15,000 or less individuals, (ii) collect info from 10,000 or fewer individuals in any 12-month period, (iii) do not collect or store "sensitive information" and (iv) "do not use covered information to study, monitor, or analyze the behavior of individuals as the person's primary business." §2(3). There is a specific	CDT strongly supports both bills' coverage of both online and offline entities. CDT generally endorses the broad definition in the BEST PRACTICES bill, which clearly applies to companies that may not collect data directly from individuals such as data brokers. We also support language exempting small businesses and others who collect information on relatively few individuals. However, §2(3)(B)(iv) of the BEST PRACTICES bill needs to be clarified to exempt news outlets in order to avoid

		exception for entities outside the FTC's jurisdiction, such as banks and credit unions, though common carriers are specifically kept within the bill's scope. §601.	significant First Amendment concerns.
Scope. Definition of "covered information"	Name, contact info, government-issued ID number, financial account number, any unique persistent identifier (including customer number, pseudonym, IP address, and presumably cookie used to collect information from a particular individual or computer), and any information linked to any of the above. §2(5)	Name, contact info, government-issued ID number, financial account number, any unique persistent identifier (including customer number, pseudonym, IP address, and presumably cookie used to collect information from a particular individual or computer), and any information linked to any of the above. §2(4)(A). The bill exempts individuals' employment title and contact info, as well as information collected from employees. §2(4)(B).	CDT supports both bills' robust definitions of covered information, including pseudonymous web identifiers and IP addresses. However, because of technological and marketplace evolution, we believe the FTC should be specifically empowered to modify the definition of "covered information," as the BEST PRACTICES bill currently provides for in the definition of "sensitive information."
Scope. Definition of "sensitive information"	Information relating to medical records or treatment, race or ethnicity, religious beliefs, sexual orientation, financial records and financial accounts, information, and precise geolocation information. §2(10).	Information relating to health or medical history, race or ethnicity, religious beliefs and affiliation, sexual orientation or sexual behavior, financial records and financial accounts, precise geolocation information, biometric data, and SSN numbers. The FTC is empowered to modify the definition in the future. §2(8).	CDT supports enhanced protections for sensitive information, including precise location information. We endorse the more protective definitions included in the BEST PRACTICES bill, especially the broader definition of health information.

Scope. Affiliates.	Treats disclosures to entities under common control with the covered entity as use by the covered entity, not transfers to third parties. §§2(7)(A)(vi), 2(13).	Treats disclosures to entities under common control and who don't hold themselves out as separate from the corporate entity as use by the covered entity, not transfers to third parties. Directs FTC to issue regulations to clarify and modify the relevant definitions. §2(10).	CDT generally supports the language in the BEST PRACTICES bill, but believes that the definition should explicitly define parties that operate under different brands as third parties for sharing purposes.
Scope. Exception for aggregated or de-identified data.	Exempts aggregate information or information that has been rendered anonymous from the scope of the bill. §5.	Exempts aggregated information and information from which identifying information has been obscured or removed, such that there is no reasonable basis to believe that the information could be used to identify an individual or a computer used by the individual. §501(a).	CDT generally supports the exception for aggregated and de-identified data contained in the BEST PRACTICES bill.
Scope. Prohibition on reidentifying data sets.	No provision.	Provides that reconstructing identifying information for datasets that have been anonymized pursuant to §501(a) is unlawful. §501(c).	§501(c) of the BEST PRACTICES bill should be removed, or revised to allow research and certain other non-commercial uses.
FTC Rulemaking.	Generally empowers the FTC to implement regulations, and specifically directs the FTC to issue regulations in limited instances (see below). §8(a)(3) *et alia.*	Generally empowers the FTC to implement regulations, and specifically directs the FTC to issue regulations in several instances, usually under clear instruction to weigh specific factors in promulgating rules (see below). §602(c) *et alia.*	CDT supports both bills' providing the FTC with general rulemaking authority, and endorses the approach of the BEST PRACTICES bill to specifically refer complex determinations to the FTC under clear and binding

			guidelines for more flexible long-term standards.
Transparency. Elements of notice	Requires privacy notice disclosing detailed information about data collection usage, storage, how to opt out of collection and usage, sharing with third parties, access rights, data retention, how to complain, and how to complain to the FTC. §3(a)(2)(B).	Requires privacy notice disclosing detailed information about data collection usage, storage, how to opt out of collection and usage, sharing with third parties, access rights, data retention, how to complain, and how to complain to the FTC. §101.	CDT supports the language in both bills requiring notice of certain baseline facts about data collection and usage. However, we suggest that the FTC should be empowered to modify the definition over time about what elements should be made available, as they may change as technology evolves.
Transparency. Nature of notice	For information collected over the internet, the notice must be posted in a privacy policy clearly linked from the company's homepage. For collection other than through the internet, covered entities must make available in writing the privacy notice before collecting covered information. §3(a)(2)(A).	Requires the FTC to promulgate regulations on how notice should be made available to consumers in a "concise, meaningful, timely, prominent, and easy-to-understand" fashion, with a special provision allowing the FTC to suggest model notices and require standardized short-form notices that consumers may be more likely to comprehend. §102. Narrow exception for in-person collection for operational purposes or when the entity only collects name and contact info. §102(c)(2).	CDT recommends the flexible approach to notice in the BEST PRACTICES bill given the diversity of modern technologies (including, increasingly, mobile technologies). We support an approach that delegates to the FTC how to best provide notice under different circumstances, including a specific provision for standardized short-form and model notices.
Purpose Specification.	Requires covered entities to list the specific purposes for which they collect and use	Requires covered entities to tell consumers the specific purposes for which they collect	CDT strongly supports clear purpose specification requirements for first-party

	covered information. §3(a)(2)(B)(iv). Requires covered entities to list specific purposes for which covered information or sensitive information may be disclosed to third parties, along with the categories of third parties who may receive such information for each such purpose. §3(a)(2)(B)(ix).	and use covered information and sensitive information, including whether they customize products or services or charge different prices based on such information. §101(3). Requires covered entities to list specific purposes for which covered information or sensitive information may be disclosed to third parties, along with the categories of third parties who may receive such information for each such purpose. §101(4).	and third-party usage. The final bill should require actual purpose specification for third-party sharing, instead of only requiring disclosure of how information may be shared.
Use Limitation.	Does not explicitly limit data usage to the purposes specified in §§3(a)(2)(B)(iv) and (ix), but by requiring covered entities to specifically disclose all purposes for which they collect consumer information, usage is implicitly limited to those purposes.	Does not explicitly limit data usage to the purposes specified in §§101(3) and (4), but by requiring covered entities to specifically disclose all purposes for which they collect consumer information, usage is implicitly limited to those purposes.	CDT believes that the provisions in both bills (along with the FTC Act's prohibition on unfair and deceptive practices) adequately limit usage to specified purposes, as long as the purpose specification requirement is sufficiently strong (see above).
Use Limitation. Changes to privacy policies	Requires covered entities to get express affirmative consent prior to making a material change in privacy policy for information previously collected. §3(a)(4).	Requires covered entities to get express affirmative consent prior to making a material change in privacy policy for information previously collected. §105(a). Requires covered entities to post new privacy policies (that include material changes re collection,	CDT supports the language in both bills requiring affirmative consent before retroactively applying new privacy policies. We also like the additional provision in the BEST PRACTICES bill of requiring companies to post new policies in advance to allow consumers

		use, and disclosure of covered and sensitive information) 30 days in advance before collecting information pursuant to those policies. §105(b).	and consumer advocates an opportunity to digest and consider changes before they go into effect.
Data Minimization.	Only imposes data retention requirements on companies that participate in the safe harbor provision that allows opt-out permission for sharing covered information with third parties. For those companies, the bill requires covered entities to delete or anonymize covered information within 18 months of when it was collected. §3(e)(2).	Requires that covered entities that use covered information or sensitive information shall retain such data only as long as is necessary to fulfill a legitimate business purposes or comply with a legal requirement. §303.	CDT generally supports the flexible approach of the BEST PRACTICES bill. However, the FTC should be directed to implement regulations to establish meaningful standards that can be tailored to different industry segments as appropriate.
Data Quality and Integrity.	Requires each covered entity to establish reasonable procedures to assure the accuracy of covered information it collects. §4(a).	Requires each covered entity to establish reasonable procedures to assure the accuracy of covered information and sensitive information it collects, assembles, or maintains, and directs the FTC to promulgate implementing regulations, balancing costs and benefits of ensuring accuracy. §201(a). Provides exceptions for fraud databases and for publicly available information if such information reflects what is available to the general public. §201(b)-(c).	CDT endorses a general provision such as in the Boucher-Stearns draft bill with a referral to the FTC for more precise definitions. The Fair Credit Reporting Act does not make an exception in its accuracy provisions for publicly available information, and we are not convinced a blanket exception for publicly available information is appropriate here.

Individual Participation. Notice and consent for first-party use of covered information.	Requires covered entities to always offer a persistent opt-out consent for first-party secondary uses of covered information, such as marketing, advertising, or selling. §§3(a)(3), 3(a)(5). No provision about whether a covered entity may condition service to a consumer based on that consumer not opting out of secondary usage.	Requires covered entities to always offer a persistent opt-out for first-party secondary uses of covered information. §103(a)-(e). However, entities may explicitly condition service to a consumer based on that consumer not opting out of secondary usage. §103(f).	CDT supports the language in both bills offering consumers an opportunity to opt out of secondary uses of their data by companies. We suggest removing the blanket authority to deny service for parties who opt out in the BEST PRACTICES bill, as we believe this should be allowed only in robust market environments where consumers have multiple options.
Individual Participation. Notice and consent for sensitive information.	Requires covered entities to get express affirmative consent for the collection or disclosure of sensitive information. §3(c).	Requires covered entities to get express affirmative consent for the collection, use, or disclosure of sensitive information. §104(b). Covered entities must offer reasonable means for consumer to withdraw consent at any time. §104(e).	CDT endorses the provisions in the BEST PRACTICES bill.
Individual Participation. Notice and consent for disclosure of covered information to third parties.	Requires covered entities to get express affirmative consent for sharing covered information with third parties for non-operational purposes. §3(b)(1). Covered entities must offer reasonable means for consumer to withdraw consent at any time. §3(b)(2). HOWEVER, covered entities	Requires covered entities to get express affirmative consent for sharing covered information with third parties for non-operational purposes. §104(a)(1). Covered entities must offer reasonable means for consumer to withdraw consent at any time. §104(e). HOWEVER, covered entities	CDT endorses the general opt-in/opt-out framework of both bills: opt-in for sharing as a default, with the opportunity to share on an opt-out basis by meeting certain safe harbor requirements. For the reasons discussed below, we support the flexible FTC-approved Choice Program put forward in

	may share covered information on an opt-out basis if they adhere to the narrow safe harbor requirements in §3(e). (See "Safe Harbor," below)	may share covered information on an opt-out basis if they adhere to the more flexible safe harbor requirements in §§401-04. (See "Safe Harbor," below)	the BEST PRACTICES bill. (See "Safe Harbor," below)
Individual Participation. Access and correction.	No access or correction requirements for non-safe harbor participants. HOWEVER, covered entities that take advantage of the safe harbor program (in order to share covered information with third parties on an opt-out basis) are required to make available for review, modification, or deletion a list of information, categories of information, or preferences associated with the individual or computer or device used by the individual. §3(e).	Requires covered entities to offer reasonable access to and opportunity to correct data that may be used for an adverse decision against the individual, such as the denial of a right, benefit, or privilege. §202(a). For other covered information, covered entities must make available (undefined) "personal profiles" that are stored in the normal course of business, and must offer access and correction rights for behavioral preference profiles. §202(b). HOWEVER, safe harbor participants are exempted from §202(b)'s access and correction rights for information that could not result in an adverse decision, and need only make available the types of information available it typically collects about individuals, or a representative sample. §§202(b)(3), 202(c). Detailed rules governing access	CDT believes that access and correction rights are fundamental elements of the Fair Information Practices, and disagrees that they should only be required of safe harbor participants (as in the Boucher-Stearns draft) or that safe harbor participants can sometimes avoid these obligations (as in the BEST PRACTICES bill). We believe a privacy bill should generally require covered entities to make available to consumers the covered information possessed about them along with a reasonable method of correction. We believe the precise rules and exemptions for access should be implemented by FTC regulations.

		and correction when required by the bill. §§202(d)-(j).	
Security.	Requires covered entities that collect covered information to adopt reasonable security safeguards that the FTC deems necessary to protect the information. §4(b). Prohibits the FTC from prescribing specific products or technologies. §8(a)(3).	Requires covered entities to adopt reasonable security measures. Directs the FTC to promulgate implementing regulations taking into account, *inter alia*, nature of covered entities and cost of security safeguards. §301. Prohibits the FTC from prescribing specific products or technologies. §602(c)(3).	CDT supports the security requirements in the BEST PRACTICES bill.
Accountability and Auditing.	No specific provisions for internal accountability and auditing.	Requires covered entities to establish a process for individuals to make complaints about privacy policies and procedures. §302(a). Requires covered entities to conduct Privacy Risk Assessments of potential risks to individuals if information about more than 1,000,000 individuals likely to be collected. §302(b). Requires covered entities to conduct periodic review of whether collected data remains necessary for disclosed purposes, and whether collection practices serve legitimate business purpose. §302(c).	CDT supports the accountability provisions contained in the BEST PRACTICES bill.

Safe Harbor.	Covered entities may get opt-out (instead of opt-in) consent for the disclosure of covered information. In order to take advantage of the safe harbor, they (1) offer a persistent opt-out of data collection, (2) delete or anonymize covered information within 18 months, (3) place a symbol or seal on all behavioral ads placed by the entity, and allow consumers to access and modify their behavioral profiles, and (4) have ad networks to which the entity discloses information under the safe harbor agree to not share the information with other parties without the consumer's express affirmative (opt-in) consent. §3(e).	Covered entities may get opt-out (instead of opt-in) consent for the disclosure of covered information, are exempted from the private right of action, and do not have to offer individuals access to "personal profiles" (consumer profiles such as behavioral advertising profiles that will not be used in a way that could result in an adverse decision against the individual, such as the denial of a right, benefit, or privilege). In order to take advantage of the safe harbor, they must join and be in compliance with an FTC-approved private Choice Program that (1) provides individuals with a global opt-out for third-party information sharing and/or communication and advertising settings for all Choice Program company participants, (2) establishes additional guidelines for protections of covered information and sensitive information, (3) requires testing and review of Choice Program participants, and (4) has consequences for failure to adhere to Choice Program	CDT generally supports the FTC-approved Choice Program safe harbor in the BEST PRACTICES bill as a vehicle for promoting best practices, while allowing compliant companies to share data on an opt-out basis and protection from a private right of action. We believe that a flexible, private safe harbor program with meaningful government oversight offers the most effective means to implement the Fair Information Practices over a wide range of companies that collect and use personal information. However, as noted above, CDT does not support an exemption from access requirements for covered information for Safe Harbor participants; the opt-out and protection from the private right of action offer sufficient incentive for companies to join a safe harbor program.

		requirements. §403.	
Enforcement. By the FTC.	The FTC can enforce the act as a violation of a trade regulation under Section 5 of the FTC Act, meaning the FTC is entitled to statutory penalties of $16,000 per violation. §8(a), 15 U.S.C. §45(m).	The FTC can enforce the act as a violation of a trade regulation under Section 5 of the FTC Act, meaning the FTC is entitled to statutory penalties of $16,000 per violation. §602, 15 U.S.C. §45(m).	CDT supports vesting the FTC with the primary authority to enforce a privacy law. However, we believe FTC penalty authority should mirror that given to state Attorneys General (see below).
Enforcement. By state Attorneys General.	Allows state Attorneys General to bring civil action for injunctive relief, damages, restitution, and other relief on behalf of state citizens. §8(b)(1). FTC has the right to intervene in such actions, and no state may bring an action while an FTC action is pending. §8(b)(2).	Allows state Attorneys General to bring civil action for injunctive relief. For violations of the notice-and-consent provisions, state AGs can also get penalties of up to $11,000 per affected person. For violations of accuracy, access, security, accountability, and data minimization provisions, state AGs can get penalties of up to $11,000 per day the entity is out of compliance. An entity's total liability for any related series of violations is capped at $5,000,000. The $11,000 per person/day figures are indexed for inflation; the $5 million cap is not. FTC has the right to intervene in such actions, and no state may bring an action while an FTC action is pending. §603.	CDT strongly supports giving state Attorneys General the right to enforce any privacy bill, and we endorse an approach that gives state AGs the ability to get statutory penalties. CDT suggests Title II and III penalties should be based on the number of individuals affected (as Title I currently is), perhaps with a lesser maximum amount per affected person. The $11,000 per person should be increased to $16,000 per person (at least for Title I violations) to mirror FTC trade regulation penalties and should remain indexed to inflation; the $5,000,000 cap should be indexed to inflation as well.
Enforcement. Private right of	Explicitly prohibits any private right of action. §9.	Allows private right of action for willful violation of notice-	CDT supports the inclusion of a strong private right of action

action.		and-consent provisions. Exempts entities that participate in and are compliance with Choice Program safe harbor. Seems to require plaintiffs to demonstrate actual damages in order to recover (damages are limited to between $100 and $1000 per individual). Plaintiffs can also recover punitive damages at the court's discretion, and reasonable costs and attorneys' fees. §604.	in any privacy bill. The private right of action in the BEST PRACTICES bill should include a provision for reasonable liquidated damages and should be extended to the full range of FIPs, not just notice-and-consent. We do not object, however, to the exemption for compliant safe harbor participants, as we believe this provides an important incentive to companies to enroll in those programs.
Preemption. State laws.	Provides very broad field preemption of any state privacy laws, arguably including state consumer protection laws and data breach notification laws. §10.	Preempts any state law that expressly requires covered entities to implement requirements with regard to the collection, use, or disclosure or covered or sensitive information, however, state consumer protection laws, state data breach laws, state financial and health privacy laws, and state trespass, contract, tort, and fraud laws are specifically preserved. §605.	CDT generally supports the preemption language in the BEST PRACTICES bill, provided that the final bill ultimately provides appropriate nationwide implementation of all the Fair Information Practices. Federal preemption of state laws is only appropriate when the federal statute gives consumers as much protection as the best state laws.