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

Statement of **Leslie Harris**
President and Chief Executive Officer
Center for Democracy & Technology

Before the House Committee on Energy and Commerce,
Subcommittee on Commerce, Trade, and Consumer Protection

THE BEST PRACTICES ACT OF 2010 AND OTHER FEDERAL PRIVACY LEGISLATION

July 22, 2010

Chairman Rush, Ranking Member Whitfield, and members of the Subcommittee:

On behalf of the Center for Democracy and Technology (CDT),[1] I thank you for the opportunity to testify today. Chairmen Rush and Boucher have shown great leadership in putting the issue of consumer privacy legislation back on the Congressional agenda. In a complex global economy, CDT believes a comprehensive set of rules for the collection and use of consumer data is long overdue.

The bills that are being discussed today provide the essential building blocks for a modern and flexible consumer privacy law based on established fair information practices that safeguard consumer privacy and encourage economic growth. Chairman Boucher's draft was a promising and important step on the road to omnibus legislation. Chairman Rush's BEST PRACTICES bill builds on that draft to significantly advance the discussion.

In my remarks today, I will comment on some of the most important building blocks drawn from these bills and offer a few suggestions for improvement. In the next week, CDT will submit a side-by-side analysis of the two bills with additional recommendations to reconcile the two into a final bill that I ask be included in the record.

I. The Need for Baseline Comprehensive Privacy Legislation

Privacy is an essential building block of trust in the digital age. But as the hearing record of both the Subcommittee on Commerce, Trade, and Consumer Protection and the Subcommittee on Communications, Technology, and the

[1] CDT is a non-profit public interest organization dedicated to preserving and promoting privacy, civil liberties, and other democratic values on the internet. CDT is widely recognized as a leader in the policy debate on consumer privacy, and we regularly testify before Congress on legislation and investigations touching on a wide range privacy issues.

Internet have documented, technology and market forces have created fundamental challenges to our assumptions about privacy. Massive increases in data storage and processing power have enabled diverse new business models predicated on the collection, analysis and retention of richly detailed data about consumers and their online — and offline — activities. While these new services and applications are often of great value to consumers, they also present new risks to consumer privacy. Americans turn to search engines to answer sensitive questions about their health. They use smart phone applications to pinpoint their location and obtain directions to a lawyer's or therapist's office. They shop, leaving digital traces of the book stores they browse, credit card numbers, and home and email addresses with "salesclerks" they never meet.

While few consumers fully grasp the extent of this large and growing data trade, both the hearing record and numerous independent studies show that practices such as deep packet inspection, online behavioral advertising, and the merger of online and offline consumer data into profiles undermine consumer trust, the fundamental building block of Internet use.[2] Privacy worries continue to inhibit some consumers from engaging in online shopping,[3] and are a top reason consumers decline to adopt location-based services.[4] A poll conducted by Zogby International in June 2010 found that 88% of Americans are concerned about the security and privacy of their personal information on the internet.[5]

Not only do the collection, sharing, and use of consumer data often clash with consumers' reasonable expectations of privacy, these activities are increasingly

---

[2] *See e.g.,* Scott Cleland, *Americans Want Online Privacy – Per New Zogby Poll*, PUBLIUS' FORUM, June 9, 2010, http://www.publiusforum.com/2010/06/19/americans-want-online-privacy-per-new-zogby-poll; Joseph Turrow, Jennifer King, Chris Jay Hoofnagle, Amy Bleakley & Michael Hennessey, *Contrary to What Marketers Say, Americans Reject Tailored Advertising and Three Activities that Enable It* (Sept. 2009), http://graphics8.nytimes.com/packages/pdf/business/20090929-Tailored_Advertising.pdf. *See also* Alan F. Westin, *Majority Uncomfortable with Websites Customizing Content Based Visitors Personal Profiles: Level of Comfort Increases when Privacy Safeguards Introduced,* HARRISINTERACTIVE, April 10, 2008, http://www.harrisinteractive.com/vault/Harris-Interactive-Poll-Research-Majority-Uncomfortable-with-Websites-Customizing-C-2008-04.pdf (in which majority of respondents said they were not comfortable with online companies using their browsing behavior to tailor ads and content to their interests even when they were told that such advertising supports free services); John B. Horrigan, *Use of Cloud Computing Services*, PEW INTERNET & AMERICAN LIFE PROJECT, September 2, 2008, http://www.pewinternet.org/~/media//Files/Reports/2008/PIP_Cloud.Memo.pdf.pdf (showing that 68% of users of cloud computing services say they would be very concerned if companies that provided these services analyzed their information and then displayed ads to them based on their actions).

[3] *See* John B. Horrigan, *Online Shopping*, PEW INTERNET & AMERICAN LIFE PROJECT, February 13, 2008, http://www.pewinternet.org/~/media//Files/Reports/2008/PIP_Online%20Shopping.pdf.pdf.

[4] Janice Y. Tsai, Patrick Gage Kelley, Lorrie Faith Cranor, & Norman Sedeh, *Location-Sharing Technologies: Privacy Risks and Controls*, CYLAB USABLE PRIVACY & SECURITY LABORATORY 18 (2010), http://cups.cs.cmu.edu/LBSprivacy/files/TsaiKelleyCranorSadeh_2009.pdf.

[5] This poll also found that 80% of Americans are concerned about companies recording their online activities and using this data to advertise and turn a profit. *See* Scott Cleland, *Americans Want Online Privacy – Per New Zogby Poll*, PUBLIUS' FORUM, June 9, 2010, http://www.publiusforum.com/2010/06/19/americans-want-online-privacy-per-new-zogby-poll.

outside of consumers' control. Online, even very savvy consumers are being thwarted in their efforts to take technological steps to protect their privacy and are seeing the privacy decisions they make directly overridden.[6]

The lack of consumer trust in the Internet also threatens to undermine the American economy. As the FCC wrote in the National Broadband Plan, a networked, "high-performance America" will require a policy framework that ensures the protection of consumers' privacy:

> As aspects of individuals' lives become more "digitized" and accessible through or gleaned from broadband use, the disclosure of previously private, personal information has made many Americans wary of the medium. Innovation will suffer if a lack of trust exists between users and the entities with which they interact over the Internet. Policies therefore must reflect consumers' desire to protect sensitive data and to control dissemination and use of what has become essentially their "digital identity." Ensuring customer control of personal data and digital profiles can help address privacy concerns and foster innovation.[7]

The Department of Commerce — in a recent Notice of Inquiry,[8] and the Federal Trade Commission — in a recent series of roundtables,[9] have both emphasized that privacy protections provide a foundation for e-commerce and the full realization of the potential benefits of the networked world. Yet the United States still has no comprehensive law that spells out consumers' privacy rights in the commercial marketplace. Instead, a confusing patchwork of distinct standards has developed over the years, with highly uneven results and many gaps in coverage. For example, while there is a strong privacy law for cable viewing and video records, the collection and use of purchasing data, search data, and location data held by smart phone applications are subject only to the FTC's general Section 5 authority.

---

[6] Consumers who use their browser controls to block or delete traditional tracking cookies may have their choices overridden by advertising networks that simply use a new technology, such as Flash cookies or browser fingerprinting to track their online behavior. *See* Ashkan Soltani, Shannon Canty, Quentin Mayo, Lauren Thomas & Chris Jay Hoofnagle, *Flash Cookies and Privacy*, SOCIAL SCIENCE RESEARCH NETWORK, August 10, 2009; Peter Eckersley, *How Unique is Your Web Browser?*, ELECTRONIC FRONTIER FOUNDATION, https://panopticlick.eff.org/browser-uniqueness.pdf; Wendy Davis, *ClearSight Launches Targeting Platform Tying IP Address to Offline Data*, MEDIAPOSTNEWS, June 28, 2010, http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=131044.

[7] FEDERAL COMMUNCIATIONS COMMISSION, CONNECTING AMERICA: THE NATIONAL BROADBAND PLAN 7-12, 52-57, http://download.broadband.gov/plan/national-broadband-plan.pdf.

[8] Information Privacy and Innovation in the Internet Economy, 75 Fed. Reg. 21226 (April 23, 2010).

[9] *Exploring Privacy: A Roundtable Series*, FEDERAL TRADE COMMISSION (2009-2010), http://www.ftc.gov/bcp/workshops/privacyroundtables.

For many companies, the growth of cloud computing is also bringing new urgency to the call for privacy legislation. As American companies continue to innovate and expand their markets overseas, they are finding that America's weak privacy framework is bad for business. Without adequate privacy protections in place, individuals, companies, and governments in other countries do not feel comfortable — or in many cases are legally restricted from — taking advantage of U.S.-based cloud computing services.[10] With our advanced technology and infrastructure, U.S. companies and the U.S. economy are poised to lead adoption of this hugely important new generation of cloud-based services. But to do so, Congress must move quickly to put a robust privacy framework in place.

II. Scope

CDT strongly supports the enactment of a uniform set of baseline rules for personal information collected both online and off-line. Both the Boucher draft and the Rush BEST PRACTICES bill take this comprehensive approach. Modern data flows often involve the collection and use of data derived and combined from both online and offline sources, and the rights of consumers and obligations of companies with respect to consumer data should apply to both as well. CDT also supports both bills' robust definitions of covered information, which go beyond traditional identifiers to include unique pseudonyms and persistent identifiers such as internet protocol (IP) addresses, and other information that could be reasonably be associated with an individual. The BEST PRACTICES bill currently empowers the FTC to update the definition of "sensitive information" in Section 2(8)(B). We agree with that approach and urge that the FTC also be empowered to adjust the definition of "covered information" as well to respond to technological and marketplace evolution.

CDT appreciates the heightened protections in both bills for sensitive information, including precise location information. In our comments on Chairman Boucher's draft bill, we argued for some expansion of the definition of "sensitive information," especially health information, and we think the new definitions in the BEST PRACTICES bill are close to the mark.

CDT is concerned, however, with the potential breadth of the affiliate exception in Section 2(11) of Chairman Boucher's draft bill and strongly urges that the sharing

[10] Article 25 of the EU Data Protection Directive states that the personal information of EU citizens may not be transmitted to nations outside of the EU unless those countries are deemed to have "adequate" data protection laws. The Article 29 Working Party does not consider U.S. law "adequate" (in part because the U.S. has no comprehensive data protection law), and thus in general personal information about EU data subjects may not be transferred to the U.S. for storage or other processing. While there are several compliance mechanisms, such as the U.S.-EU "Safe Harbor" agreement, that allow U.S. companies to process personal information from the EU, each comes with its own compliance challenges. For an in-depth discussion of these compliance challenges, *see Comments of the Center for Democracy and Technology on Information Privacy and Innovation in the Internet Economy*, CDT (2010), http://www.cdt.org/files/pdfs/20100613_doc_privacy_noi.pdf.

of consumer information among affiliates for advertising, marketing, and other non-operational purposes be limited to entities under common branding with the covered entity — entities that a consumer would reasonably understand to be under common control. Otherwise this exception could be used to swallow the rule. We generally support the BEST PRACTICES bill's referral of this issue to the FTC for more precise definition.

Finally, CDT is pleased to see that both bills have specific rules for covered entities that collect "all or substantially all" or certain categories of a consumer's internet activity. CDT has long been concerned about companies such as internet service providers who have the ability to monitor all of a consumers' online activity through deep packet inspection for advertising or other purposes.[11] We agree that this particularly invasive level of monitoring merits special rules, and should only be done on an opt-in, affirmative consent basis. However, we recognize that the term "all or substantially all" may not give companies sufficient clarity as to which practices are covered, nor does it prohibit narrow interpretations that would render this exception meaningless. CDT recommends that the scope of this definition be specifically referred to the FTC for further clarification.

III. Fair Information Practices

As both bills recognize, Fair Information Practices (FIPs)[12] must be the foundation of any comprehensive privacy framework. FIPs have been embodied to varying degrees in the Privacy Act, Fair Credit Reporting Act, and other sectoral federal privacy laws that govern commercial uses of information online and offline. While some have discussed moving away from FIPs in the past, new sets of protections created always revolve around the same basic eight ideas just using new terminology. The most recent government formulation of the FIPs offers a robust set of modernized principles that should serve as the foundation for any discussion of consumer privacy legislation. These principles, as described by the Department of Homeland Security in 2008, include:[13]

---

[11] *See What Your Broadband Provider Knows About Your Web Use: Deep Packet Inspection and Communications Laws and Policies: Hearing Before the Subcomm. on Telecomm. and the Internet of the H. Comm. on Energy and Commerce*, 110th Cong., 1st Sess. (2008) (statement of Alissa Cooper, Chief Computer Scientist, Center for Democracy & Technology); *The Privacy Implications of Deep Packet Inspection: Hearing Before the Subcomm. on Commc'ns, Tech. and the Internet of the H. Comm. on Energy and Commerce*, 111th Cong., 1st Sess. (2009) (statement of Leslie Harris, President and Chief Executive Officer, Center for Democracy & Technology).

[12] The first set of FIPs was released in 1973 by the Health, Education, and Welfare Department. Since that time, various versions of the FIPs have been used by federal agencies internally and externally; each agency adopts and abides by its own set of Fair Information Principles, and these principles are reflected to some extent in the various U.S. sectoral privacy laws. FIPs additionally appear, with some variation, in many international frameworks, including the OECD guidelines of 1980, the Council of Europe data privacy convention, and the EU Data Protection Directive.

[13] U.S. Department of Homeland Security, *Privacy Policy Guidance Memorandum, The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security* (December 2008), http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

- **Transparency.** *Entities should be transparent and provide notice to the individual regarding their collection, use, dissemination, and maintenance of information.*
- **Purpose Specification.** *Entities should specifically articulate the purpose or purposes for which personal information is intended to be used.*
- **Use Limitation.** *Personal information should be used solely for the purpose(s) specified in the notice. Sharing of personal information should be for a purpose compatible with the purpose for which it was collected.*
- **Data Minimization.** *Only data directly relevant and necessary to accomplish a specified purpose should be collected, and data should only be retained for as long as is necessary to fulfill a specified purpose.*
- **Data Quality and Integrity.** *Entities should, to the extent practicable, ensure that data is accurate, relevant, timely, and complete.*
- **Individual Participation.** *Entities should involve the individual in the process of using personal information and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of this information. Entities should also provide mechanisms for appropriate access, correction, and redress regarding their use of personal information.*
- **Security.** *Entities should protect personal information through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.*
- **Accountability and Auditing.** *Entities should be accountable for complying with these principles, providing training to all employees and contractors who use personal information, and auditing the actual use of personal information to demonstrate compliance with the principles and all applicable privacy protection requirements.*

While both bills make significant headway toward the integration of the Fair Information Practice principles into U.S. privacy law, the BEST PRACTICES bill intelligently incorporates much of the feedback from Chairman Boucher's draft bill and puts forward strong FIPs-based privacy protections that go beyond notice and consent to a full set of substantive privacy protections.

Transparency

Both Section 3(a)(2)(B) of Chairman Boucher's draft and Section 101 of the BEST PRACTICES bill require that covered entities entities make available detailed information about the collection, storage, and use of covered information. While the required information is important, privacy policies are notoriously difficult for consumers to understand, and striking the right balance

between readability and comprehensiveness has proven elusive. Given this challenge, we recommend that rather than mandating such detailed specific elements of notice, the FTC should be empowered to institute a rulemaking on the issue. Given the wide and ever-changing variety of mediums through which people communicate and share information, including increasingly mobile devices, we strongly support the approach of Section 102(b) of the BEST PRACTICES bill to delegate to the FTC to determine how this notice should be presented to consumers. We also support that provision's explicit direction to the FTC to develop model short form notices that companies can adapt to make notice and consent more meaningful to consumers.

Purpose Specification

CDT is pleased that both bills have strong language requiring that companies clearly specify the purposes for which they collect and use consumer information. Sections 101(3), 101(4) and 102(a) of Chairman Rush's bill require that covered entities disclose the specific purposes for which consumer data is being collected in a "concise, meaningful, timely, prominent, and easy-to-understand" fashion. Similarly, Section 3(a)(2)(B)(iv) of Chairman Boucher's bill requires notice of the specific purposes for which covered entities collect and use covered information.

Use Limitation

Neither bill explicitly states that a covered entity can only collect or use covered information for the purposes specified to the consumer. However, by mandating that covered entities affirmatively specify the purposes for which they collect or use personal information, we believe use limitation is implicitly incorporated into both bills by the sections cited above under "Purpose Specification."

CDT generally supports the provisions in both bills preventing companies from revising their privacy policies retroactively to apply to previously collected information. These provisions are consistent with the manner in which the FTC has applied its authority under Section 5 to such "material changes,"[14] but it is certainly preferable to have the principle spelled out explicitly in a privacy statute. We also endorse the provision in Section 105 in the BEST PRACTICES bill that requires covered entities to post new privacy policies for thirty days before they take effect so that consumers have ample opportunity to notice and assess the changes.[15]

---

[14] Consent Decree, In re Gateway Learning Corp., FTC No. C-4120 (July 7, 2004), http://www.ftc.gov/os/caselist/0423047/0423047.shtm.

[15] While CDT does not expect that ordinary consumers will be checking the privacy policies of all the websites they interact with on a monthly basis, privacy advocates do pay attention. As one telling example, last month, Apple made a change to its privacy policy regarding location tracking and behavioral targeting. Within a matter of days, bloggers and other tech writers immediately publicized the changes, to the extent that Apple eventually received a letter of inquiry from Congressmen Markey and Barton about the new policies.

Data Minimization

CDT supports the language contained in Section 303 of the BEST PRACTICES bill that sets forth appropriate and well-considered high level requirements for data minimization. Data minimization must be an obligation of all companies that collect covered information, not just for those companies that take advantage of the individually managed profile exception, as is currently the case with Chairman Boucher's draft bill. While we agree with Chairman Boucher that companies should not retain consumer data for longer than needed to fulfill the purpose for which it was collected, we are not comfortable setting a specific time limit for data retention in law as in Section 3(e)(2) of the draft bill. CDT believes that a consumer privacy law should avoid such highly prescriptive mandates, which may inadvertently freeze today's practices into law and discourage future innovation. Having said that, we also believe that Section 303 of the BEST PRACTICES bill would be improved if it specifically directed the FTC to issue regulations implementing this section. Given that the current framework has utterly failed to require or even encourage companies to adopt data minimization procedures, we believe that a direct provision requiring FTC implementation regulations is appropriate.

Data Quality and Integrity

CDT likes the broad but flexible language of both bills requiring that covered entities establish reasonable procedures to assure the accuracy of the information they collect about consumers. The only material difference between Section 201 of the BEST PRACTICES bill and Section 4(a) of Chairman Boucher's draft bill is that the former requires the FTC to issue regulations to implement and interpret this section, while the latter merely permits such regulation (through the general rulemaking powers in implementing the bill granted in Section 8(3)). Both approaches have merit. However, we believe that greater direction to covered entities would be useful to set flexible but meaningful baseline standards. We believe a directive to the FTC to adopt implementing regulations is appropriate.

Individual Participation

In general, CDT approves of the opt-out/opt-in choice framework of both bills: covered entities must offer a persistent opt-out for first-party data collection and use, and must get opt-in affirmative consent for the collection and use of sensitive information. For the sharing of covered information with third parties, as a default, covered entities must get opt-in consent, although both bills offer safe harbor provisions that allow companies to only offer an opt-out if they meet certain conditions (see *infra* Section IV, "Safe Harbor"). Obviously, "notice and choice" alone has proven insufficient to protect consumers, as that model places the entire burden for privacy protection on consumers to navigate an increasingly complex data environment. That is why a modern consumer privacy framework must incorporate all of the other FIPs in order to meet the privacy challenges posed by the vast array of 21st-century technology and business practices.

The BEST PRACTICES bill includes very detailed provisions for granting consumers access and rights of correction for covered information. While we believe these provisions to be carefully considered, we are hesitant to recommend embedding such detailed provisions into law. Instead, we suggest that the Subcommittee consider referring some or all of this section to the Federal Trade Commission for implementing regulations. To the extent the BEST PRACTICES bill exempts safe harbor participants from certain access obligations (and the Boucher draft bill requires that only safe harbor participants grant consumers access), we recommend instead that reasonable access to stored covered information be treated as a universal obligation for all companies who collect and store covered information about consumers (see *infra* Section IV, "Safe Harbor,").

Security

CDT endorses the standards set forth by Section 301 of the BEST PRACTICES bill and Section 4(b) of Chairman Boucher's bill that require covered entities to enact reasonable safeguards to protect the security of covered information. Companies should be held to an objective standard while having the freedom (and indeed, the responsibility) to innovate creatively to best protect consumers' data. If the legislation does refer the question of security to the FTC for implementing regulations, it should also include the language of Section 602(c)(3) of the BEST PRACTICES bill, which prohibits the FTC from specifically prescribing particular technologies or products in regulations for security or other components of the bill.

Accountability and Auditing

Finally, we strongly applaud the inclusion in Section 302 of the BEST PRACTICES bill of a requirement for companies to conduct Privacy Impact Assessments before collecting and using the data of large numbers of consumers, and to conduct periodic reviews of its privacy practices. American companies have played a leadership role in identifying and implementing accountable practices that safeguard privacy. In the absence of baseline privacy law, many companies have moved ahead with the appointment of privacy officers to guide internal privacy decision-making and to engage in privacy risk assessment and privacy by design.[16] And just last week the European Union's Article 29 Working Party released an opinion that was devoted entirely to an exploration of promising accountability frameworks and that recommended adoption of new accountability mechanisms by companies that handle consumer data.[17] As we noted in our comments on Chairman Boucher's draft, the inclusion

[16] For more information on how accountability measures can be incorporated into the product development cycle, *see* Marty Abrams, Ann Cavoukian, and Scott Taylor, *Privacy by Design: Essential for Organizational Accountability and Strong Business Practices* (Nov. 2007); http://www.ipc.on.ca/images/Resources/pbd-accountability_HP_CIPL.pdf.

[17] Article 29 Working Party, "Opinion 3/2010 on the principle of accountability,'" 00062/10/EN WP 173 (July 2010). http://www.huntonfiles.com/files/webupload/PrivacyLaw_Accountability_WP29.pdf.

of accountability provisions in the legislation, is a way to encourage a culture of responsibility and accountability within covered entities.[18] Doing so will also support the development of a global standard on accountability.

IV. The Safe Harbor Framework

CDT strongly supports the inclusion of a safe harbor provision in the BEST PRACTICES Act. CDT has long supported the use of a flexible safe harbor framework as the most effective tool to implement the Fair Information Practice principles over a wide range of industries that collect and use personal information.[19] Given the necessary disparity in practices among varying groups such as behavioral advertisers, data brokers, small offline businesses, and multinational online retailers, a one-size-fits-all approach that narrowly prescribes all data practices is likely to unfairly favor certain industries while stifling innovation and development in others. A carefully crafted safe harbor program — backed up by a rigorous internal compliance regime — that gives industries and industry segments flexibility to develop tailored privacy solutions that are consistent will the law, is the best way to accommodate differences between industries, create certainty for companies (because following approved practices would be deemed compliance with the privacy statute), encourage privacy innovation over time, and reward the adoption of accountable practices.[20]

Finding the right balance between industry self-regulation, encouraging new technologies and business practices that protect privacy, and government oversight is obviously the key challenge in defining the parameters of a reasonable safe harbor. In designing a safe harbor, it is important to strike a balance between strong incentives to participate in a safe harbor with meaningful regulatory oversight. We believe that the BEST PRACTICES bill generally meets that test. We disagree, however with the approach of the BEST PRACTICES bill to the extent that it grants exemption from access requirements to covered entities which participate in an approved safe harbor (*see supra*, Section IV ("Individual Participation")). A safe harbor should not free participants from engaging in any particular Fair Information Practice. Rather, it should simply free them to develop alternative means to meet the requirement.

---

[18] *Comments of the Center for Democracy and Technology on the Staff Discussion Draft of Consumer Privacy Legislation*, CDT (2010), *available at* http://www.cdt.org/files/pdfs/20100604_boucher_bill.pdf.

[19] As noted by Ira Rubinstein in his comments to the Boucher draft bill, when Congress last considered online privacy legislation, several bills included provisions for a comprehensive self-regulatory safe harbor modeled on COPPA, including Rep. Markey's Electronic Privacy Bill of Rights Act of 1999 (H.R.3321, 106th Cong. § 4 (1999)); Sens. Burns and Wyden's Online Privacy Protection Act of 1999 (S. 809, 106th Cong. § 3 (1999)); Rep. Stearns' Consumer Privacy Protection Act of 2002 (H.R. 4678, 107th Cong. §106 (2002)); and Sen. Hollings' Online Personal Privacy Act (S. 2201, 107th Cong. § 203 (2002)).

[20] *See also* Letter to Chairman Rick Boucher from Professor Ira Rubinstein, June 1, 2010.

V. Enforcement

Baseline privacy legislation needs strong enforcement measures to give teeth to FIPs-based privacy protections, and the FTC does not need to go it alone. State attorney generals have brought a number of important online consumer protection cases in recent years, and they have a right and obligation to protect their citizens' interests. Therefore CDT supports the approach in both bills to give enforcement to both the Federal Trade Commission and state Attorneys General. We also support the statutory penalty provision in Section 603 of the BEST PRACTICES bill, though we believe that these penalties should be available to the Federal Trade Commission as well as the states. As we have testified previously, we believe the FTC should be empowered to sue for statutory penalties for all Section 5 violations and already operates at a disadvantage vis-à-vis state attorneys general;[21] there is no need to create a parallel FTC disadvantage for violations of privacy legislation.

CDT has long supported the inclusion of a strong private right of action in any privacy legislation. We are pleased Chairman Rush has included a private right of action in the BEST PRACTICES bill, but we think it could be strengthened by providing for liquidated damages instead of requiring that plaintiffs prove actual damages, and by extending the private right of action to all the Fair Information Practice principles, not just notice and choice.

However, CDT does not object to compliant participants in safe harbor programs from being exempted from the private right of action. Companies need to have some degree of assurance that meeting the standards approved by the FTC will insulate them from legal attack. If companies are in fact meeting those goals, they should not be subject to any legal action — either from government enforcers or private litigants.

VI. Preemption

CDT believes that preemption of state law in federal privacy law should be narrowly tailored to reach only those state laws that expressly cover the same set of covered entities and same set of requirements. Even then, CDT would only supports preemption if the federal law provides as much protection as the best state laws. CDT has previously objected to the overly broad preemption language contained in Chairman Boucher's draft bill, which arguably provides for sweeping field preemption of all state privacy laws. We are gratified that the preemption language in the BEST PRACTICES bill aligns closely with our suggested language, which we think is narrowly tailored to reach only those state laws that expressly cover the same set of covered entities, while allowing states to specify additional protections on sensitive areas such as health and financial information.

---

[21] Ari Schwartz, Testimony of Ari Schwartz before the Senate Committee on Commerce, Science, and Transportation Subcommittee on Interstate, Trade, and Tourism, "Reauthorization of the Federal Trade Commission," September 12, 2007, www.cdt.org/privacy/20070912schwartz-testimony.pdf.

VII. Conclusion

CDT would like to thank Chairman Rush for the introduction of the BEST PRACTICES Act and for holding this important hearing. Today, we have taken an important step forward toward enactment of the baseline privacy legislation that consumers strongly support and that businesses increasingly need to compete in the global economy. We look forward to working closely with the Committee on this legislation. Thank you again for the opportunity to testify.

For more information, contact Leslie Harris, lharris@cdt.org, or Justin Brookman, justin@cdt.org at (202) 637-9800.