Comments of the Center for Democracy & Technology on the Staff Discussion Draft of Consumer Privacy Legislation

The Center for Democracy & Technology (CDT) submits these comments on the staff discussion draft ("the draft") of consumer privacy legislation released May 3, 2010 by Chairman Boucher and Ranking Member Stearns. The Internet and new technologies have created powerful new ways for consumers to live their lives online and for industry to gather, store, share and use personally identifiable information. In today's increasingly complex information environment, CDT believes that it is crucial to enact a flexible baseline consumer privacy law that would protect consumers from inappropriate collection and misuse of their personal information, both online and offline. We appreciate the Chairman's leadership on this issue and are committed to working with the Committee to enact a bill that will protect privacy while providing sufficient flexibility to support technological innovation.

I. **The scope of the bill**: CDT is pleased that the draft covers personal information collected both online and off-line, with a uniform set of baseline rules. There is no longer a bright line between the online and offline world. Modern data flows often involve collection and use of data derived and combined from both, and the rights of consumers and obligations of companies with respect to consumer data should apply to both as well.

II. **Fair Information Practices**: CDT believes that federal privacy legislation should be grounded in a comprehensive set of fair information practices ("FIPs") including the following[1]:

    a. **Transparency.** *Entities should be transparent and provide notice to the individual regarding their collection, use, dissemination, and maintenance of information.*
    b. **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.*
    c. **Purpose Specification.** *Entities should specifically articulate the purpose or purposes for which personal information is intended to be used.*

[1] This formulation of Fair Information Practices is based on those adopted by the Department of Homeland Security in 2008. *See* 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* (Dec. 2008), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf ("DHS FIPs").

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 FIP principles and FIPs principles are reflected 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 (DPD). The Asia-Pacific Economic Cooperation (APEC) Privacy Framework also incorporates some of the FIPs.

d. **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.*
e. **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.*
f. **Data Quality and Integrity.** *Entities should, to the extent practicable, ensure that data is accurate, relevant, timely, and complete.*
g. **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.*
h. **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.*

The discussion draft addresses portions of the "individual participation" principle in the notice and choice provisions as well as requirements for accuracy and data security, but stops short of adopting a full FIPS framework that would impose substantive obligations on companies to minimize collection, use and retention of consumer data. While CDT generally agrees with the draft's basic framework for notice and choice, including its opt-in and opt-out structure, we are concerned that the strong reliance on consent places the entire burden for privacy protection on consumers to navigate an increasingly complex data environment. In most instances, very little privacy protection is achieved by reliance on this narrow set of protections. We urge that the draft include all of the FIPs in order to meet the privacy challenges posed by the vast array of 21st-century technology and business practices.

III. **Covered Information:** CDT generally supports the draft's robust definition of covered information, which goes beyond traditional identifiers to include biometrics, persistent identifiers such as Internet protocol (IP) addresses, preference profiles and other information that could reasonably be associated with an individual (Sec. 2(5)). However, as technologies change, some types of information may become more sensitive and "personally identifiable" while some types may become less so. For example, it has become increasingly easy for companies to collect and combine discrete pieces of information from consumers into rich profiles and to associate those profiles with a specific individual or a device. But situations may also arise in which the collection or monitoring of dynamically assigned IP addresses may not create data that poses privacy risks. In this context of rapidly changing technologies and advances in online data collection, we recommend empowering the FTC to clarify and update the definition of covered information to take account of new developments.

IV. **Sensitive information**: CDT appreciates the heightened protection in the draft bill for sensitive information (Sec. 2(10)), including precise location information (Sec. 2(10)(F)). As the accuracy of location data improves and the expense of calculating and obtaining it declines, location is beginning to pervade the online

experience, making way for exciting new applications and services while also prompting significant privacy concerns. The draft's provisions for location information provide important protections for this increasingly prevalent type of data. We urge, however, that the provision on "medical information" (Sec. 2(10)(A)) be redesignated "health information" and the definition broadened in order to reach health data generated by users online. Part two of the definition of "health information" in HIPAA may prove a useful model.[2]

V. **Affiliates of the covered entity:** While CDT agrees that covered entities will often need to share consumer data for operational purposes, we believe the phrase "affiliate of the covered entity" (Sec. 2(7)(vi)) and the definition of unaffiliated party (Sec. 2(13)) require further clarification to ensure that they align with the reasonable expectations of consumers and not provide an overbroad exception from the requirements of the staff draft. We suggest that the term "affiliate of the covered entity" be limited in scope to entities under common branding with the covered entity, entities that a reasonable consumer would understand is under common control. It may be appropriate to explicitly require that the FTC define the term "affiliate of the covered entity" in a rulemaking (Sec. 8(3)).[3]

VI. **Improving Notice and Choice**: Privacy policies are difficult for consumers to understand and striking the right balance between readability and comprehensiveness has proven elusive. Given this challenge, we recommend that the bill refrain from mandating the specific elements of notice and instead provide the FTC with the authority to institute a proceeding on the issue. We also recommend that the FTC be empowered to develop a model short form notice that companies can adapt to make notice and consent more meaningful to consumers.

VII. **Ensuring technology neutrality and flexibility**: CDT believes that regulatory flexibility aimed at accommodating different business models and technologies over time is an essential element of successful consumer privacy legislation. While the FIPs are well-suited to the task of providing a cross-industry framework for privacy-protective practices, writing specific requirements into legislation will likely prove a Sisyphean task. Because business practices and processes may vary significantly between "brick and mortar" companies and those online, a single set of specific practices that apply to all covered entities will be ill-fitting for some. Further, privacy protections enshrined in law must be able to respond to rapid changes in technology. There is a significant risk that highly prescriptive mandates, such as the specific time period for data retention (Sec. 3(e)(2)) or the specific technological approach to access to profile data (Sec. 3(e)), to name a few, may inadvertently "freeze" today's practices into law and discourage future innovation. For this reason, we strongly urge that requirements be set out at a

[2] 45 CFR 160.103.

[3] The FTC has already conducted extensive research into the question of how to define affiliates in the behavioral advertising space. *See* Federal Trade Commission Staff Report, *Self-Regulatory Principles For Online Behavioral Advertising: Behavioral Advertising Tracking, Targeting & Technology* (Feb. 2009), *available at* http://www.ftc.gov/opa/2009/02/behavad.shtm.

more general level with the details left to FTC rulemaking. Inclusion of a safe harbor provision (discussed below) may also encourage best practices over time and ensure that legislation acts as a floor rather than a ceiling on privacy practices.

VIII. **Promoting flexibility and accountability through a safe harbor:** CDT urges the drafters to consider inclusion of a safe harbor provision to encourage innovation in privacy protection and industry-specific best practices. As Professor Ira Rubenstein (who also serves on the CDT Board) explains in comments submitted on the discussion draft:

> A safe harbor is a regulatory strategy under which a federal statute explicitly recognizes differences in performance by treating safe harbor participants more favorably than non-participants. In other words, safe harbors shield or reward regulated firms if they engage in desirable behavior as defined by statute. Favorable treatment for better performing firms might include immunity from liability, protection from certain penalties, exemptions from certain requirements, and permission to engage in certain desired behaviors. The key point to emphasize here…is that eligibility for the benefits conferred by a safe harbor should be limited to firms meeting a high standard of performance that exceeds what is otherwise required of firms covered by the relevant statute.[4]

We believe that a carefully crafted safe harbor framework, giving industries or industry segments flexibility to develop tailored privacy solutions with FTC oversight, is the best way to accommodate differences between industries, create certainty for companies (because following approved practices would be deemed compliance with the statute), encourage privacy innovation over time, and reward adoption of accountable practices.

IX. **Private right of action:** CDT believes that baseline privacy legislation should provide consumers with a private right of action. Without such a provision, individuals whose privacy rights are violated must rely entirely on enforcement decisions by government authorities to vindicate their rights, yet neither the FTC nor state attorneys general have the capacity to litigate every violation of the statute. One successful model for a private right of action can be found in the Telephone Consumer Protection Act (TCPA), which provides for a private right of action for liquidated damages for violations of the Act.[5] In any event, even if the drafters choose not to include a private right of action, the current language in Section 9 precluding actions in state court is seriously overbroad. It would not only preclude a private civil action arising from the violations of the bill itself, but all relevant civil actions commenced under any state laws, including common law. Section 6(b) of H.R. 2221 offers a model for a more appropriately targeted approach, precluding a state law action "if such action is premised in whole or in part upon the defendant violating any provision of this Act."

---

[4] Letter to Chairman Rick Boucher from Professor Ira Rubenstein, June 1, 2010.
[5] 47 U.S.C. sec. 227(b)(5).

X. **Effect on federal laws**: CDT has long argued that the confusing patchwork of federal privacy laws in this country has resulted in highly uneven protections for user data and many gaps in coverage. This draft represents an important recognition of the limitations of the sectoral privacy framework that has arisen over the years. CDT does, however, believe that the existing sectoral laws have an important role to play in any new privacy framework. While many important federal laws are explicitly preserved in the draft (Sec. 11), others – such as the Video Privacy Protection Act, the Genetic Information Nondiscrimination Act, and the health privacy provisions in the American Recovery and Reinvestment Act of 2009 – would be preempted. We urge you to ensure that all federal sectoral laws are preserved in the draft. If however the intent of the drafters is to preempt any existing federal privacy law, that fact should be expressly stated in the draft.

XI. **Preemption of state laws:** 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. The states have been the engine of innovation with respect to privacy and CDT recognizes that while the diversity of state privacy laws may be burdensome for some companies, particularly in the online environment, preemption must be approached cautiously. The preemption clause in the draft (Sec. 10) appears to provide sweeping "field" preemption of all state privacy laws including those that address disclosure of specific health information and state-level consumer protection laws. If broadly interpreted, the draft could even be read to preempt successful state data breach notification laws, which have been adopted by 46 states, the District of Columbia, Puerto Rico, and the Virgin Islands.[6] We recommend looking to H.R. 2221 for a model of a narrowly tailored preemption provision.

XII. **Accountability:** CDT encourages the drafters to consider including accountability requirements in the bill that encourage companies to assess and manage privacy risk on an ongoing basis**.** Developing products that are privacy protective requires attention to privacy from the very beginning of the product development cycle. Accountability measures might include a requirement, for example, to conduct a Privacy Impact Assessment (PIA) prior to the implementation of new products, services or marketing initiatives, which involve the collection, use, and disclosure of, covered data. PIAs are mandated by law in government agencies and are standard practice in some companies.[7]

---

[6] *See* National Conference of State Legislatures, *State Security Breach Notification Laws* (April 12 2010), *available at* http://www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/SecurityBreachNotificationLaws/tabid/13489/Default.aspx.

[7] The process of integrating privacy considerations into business models, product development cycles, and new technologies is often referred to as "Privacy by Design." For more information, *see* Anne Cavoukian, *Privacy by Design: The 7 Foundational Principles* (August, 2009)*, available at* http://www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf.

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). *Available at* http://www.ipc.on.ca/images/Resources/pbd-accountability_HP_CIPL.pd