June 4, 2010

The Honorable Rick Boucher
U.S. House of Representatives
Subcommittee on Communications, Technology and the Internet
2187 Rayburn House Office Building
Washington, DC 20515

The Honorable Cliff Stearns
U.S. House of Representatives
Subcommittee on Communications, Technology and the Internet
2370 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Boucher and Ranking Member Stearns:

In response to your release of a discussion draft of a bill concerning privacy protections for consumers both online and offline, the following organizations offer these comments for your consideration.

Consumers increasingly rely on the Internet and other digital services for a wide range of transactions and services, many of which involve their most sensitive affairs, including health, financial, and other personal matters. Companies are now engaging in behavioral advertising, which involves the surreptitious monitoring of consumers' activities online and offline – just one example of new ways that data is being collected and used. Strong legislation is necessary to protect consumers from consequences that they never imagined or agreed to. Though we believe that the bill you have released has some positive aspects, it must be considerably revised to provide the protection that consumers truly need and garner the support of consumer and privacy groups.

First, we believe that the inclusion of personal identifiers such as Internet Protocol address in definition of "covered information" in the bill is crucial. We are also pleased by the requirement for consumers' express consent when there will be a material change in companies' privacy policies. When consent must be through an opt-in procedure, we think it would be a good idea to clearly and consistently specify that to avoid any confusion about what is intended.

However, we continue to believe that the notice and choice model on which the bill is based promotes bureaucracy but does not promote privacy. A privacy bill that actually creates some privacy will need to set strong rules that directly protect consumer privacy, or at least be based on the Fair Information Practices (FIPs) which have been the foundation of U.S. privacy policy for the past four decades. We believe that the bill should be restructured to follow the FIPs, in much the same way

as we structured the legislative principles that we released last September.[1]

We would also like to challenge the conventional wisdom that privacy legislation that is based on an opt-in approach is not feasible. There is absolutely no reason why an opt-in approach cannot work, and work well. It is ironic that while many in the business community profess to want to offer consumers real and meaningful control over the collection and use of their data, these same companies and associations are unwilling to provide the most effective means of control for consumers – opt-in. We heard similar objections before the wildly popular national "Do Not Call" registry was implemented, and even after when its legality was unsuccessfully challenged. We were told that it would be the end of direct marketing and that consumers would no longer be able to obtain the products and services they wanted at affordable prices. This was nonsense, as the objection to opt-in is nonsense now. Businesses will become more innovative and responsive to consumers' desires concerning the collection and use if their data if they must first ask for their express affirmative consent. We recommend that non-sensitive information should only be allowed to be collected and used for advertising purposes for 24 hours, after which opt-in consent would be required to continue to store and use it.

Of course, we understand that some exceptions will be needed – for instance, for the collection and use of public record data, and for the collection and use of data for operational and transactional purposes. However, we believe that the definitions of transactional and operational in the current draft legislation are too broad, and that the complete lack of any bounds on the retention of this data is inappropriate. We believe that the definition of operational data must be significantly narrowed and that reasonable retention limits should be set for this data.

We are also concerned about the blanket exception for affiliates. We doubt that most consumers could name the affiliates of the companies with which they routinely do business, let alone those of unfamiliar companies. Moreover, sharing consumers' data with affiliates when it is not necessary for transactional or operational purposes does not always provide benefits to consumers and may sometimes be detrimental to them (e.g., passing a consumer's information to an affiliate that charges higher interest rates). We recommend that affiliates should be treated no differently than third parties and that affiliate sharing should only be allowed on an opt-in basis except for transactional and operational purposes.

We believe that the exception for individual managed profiles is also unwarranted. While managed profiles are better than unmanaged profiles, the reality is that there is nothing in the bill that limits such profiles to use for advertising purposes, or that prevents access to them by private detectives, insurers, employers, or others who

---

[1] See Online Behavioral Tracking and Targeting: Legislative Primer, September 2009 at www.democraticmedia.org/doc/privacy-legislative-primer

might make assumptions about individuals based on them. Furthermore, a world in which consumers have dozens or hundreds of "manageable" profiles at sites they've never heard of is not a world in which consumers have any control. Consumers should be asked to opt-in for such profiles, or there must be some way to ensure that consumers have an easy way to opt-out of all such profiling through a federal Do Not Track registry.

Even opt-in does not adequately protect consumers when there is the potential that their sensitive data could be used for purposes other than for transactions they decide to make. First, we believe that the bill's definitions of what constitute "sensitive information" are too narrow. For example, "sensitive information" under the bill includes "medical records, including medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional." However, this would not cover situations such as when a consumer researches cancer or another disease online. As that search is not part of "medical records," the information may be collected and used to make judgments about the consumer for any purpose, including employment and insurance. We recommend using different language adapted from the HIPAA definition of "health information."

But even with the required notice and opt-in, consumers may not be able to fully appreciate how information about their health, finances, race or ethnicity, sexual orientation, religious beliefs, political beliefs and data about their location might be accessed and used, for purposes they never anticipated. For instance, a consumer searching for mortgage information is unaware that she is being tracked as she searches for the best deal online and that her "profile" may contain information about her race, ethnicity, financial condition, health concerns, where she travels, and other sensitive information which can influence the kinds of offers and products that she may receive. It is unclear what "other financial" information means and whether it would encompass this. We recommend a broader definition that includes income and credit score, as well as Social Security number.

We also note that storing and sharing sensitive information puts consumers at risk of identity theft and other crimes. To truly protect consumers, the bill should prohibit sensitive data from being collected or used for any purposes other than for the transactions for which they have provided it.

Another concern is that other than for managed profiles, the bill sets no time limit for data retention (and 18 months for managed profiles is far too long). Furthermore, there is no right to access, correct or delete one's data in the current draft bill.

We suggest that the bill should provide the Federal Trade Commission with the authority and flexibility to develop the definitions further and to provide for reasonable notice and access requirements and data retention time limits.

To make clear that the legislation in no way erodes consumers' privacy under the

Electronic Communications Privacy Act, we recommend that this should be explicitly stated.

We are very concerned about the sweeping preemption in the current draft of the legislation. The bill preempts state or local laws or regulations that include "requirements for the collection, use, or disclosure of covered information." This is incredibly broad and could block existing or new measures on the state level to limit the use of certain types of information, such as Social Security numbers, to notify consumers of data breaches, to protect health data, and to extend other needed privacy protections to consumers. Rather than a broad preemption, we recommend that the bill set minimum standards for privacy protection and allow states to create stronger laws and regulations to safeguard consumer data against misuse and abuse if necessary. The stronger the final bill is, the less likely that there will be any significant gaps that states will feel compelled to fill.

We are also dismayed by the fact that the bill would block consumers from taking legal action to enforce their rights. As you know, federal and state agencies play important roles in protecting the public, but they cannot and do not take action to resolve every situation in which consumers' rights have been violated. It is essential for individuals to be able to enforce their privacy rights and stop egregious practices. A private right of action must be provided to help ensure a level playing field and incentivize companies to respect and protect consumers' privacy.

Finally, we believe that there should be a strong findings section at the beginning of the bill and we are attaching suggested language in this regard. We urge you to carefully review our suggestions, as we are working toward the same goal: to protect the interests of Americans while maintaining and increasing robust commerce. In fact, providing meaningful protection for consumers' data is necessary in order to ensure their confidence in our increasingly complex marketplace. The argument that we must choose between privacy or access to a broad array of reasonably attainable goods and services is false. American business can deliver both, and we should demand no less.

We are committed to working with you to achieve real privacy protection for consumers. Thank you for considering our views.

Sincerely,

Jeff Chester
Executive Director
Center for Digital Democracy

Susan Grant
Director of Consumer Protection
Consumer Federation of America

Lee Tien
Senior Staff Attorney
Peter Eckersley
Senior Staff Technologist
Electronic Frontier Foundation

Linda Sherry
Director of National Priorities
Consumer Action

Beth Givens
Director
Privacy Rights Clearinghouse

John M. Simpson
Consumer Advocate
Consumer Watchdog

Pam Dixon
Executive Director
World Privacy Forum

Ed Mierzwinski
Consumer Program Director
USPIRG

Melissa Ngo
Publisher
Privacy Lives

Evan Hendricks
Publisher
Privacy Times

Enclosure: suggested findings language