Center for Digital Democracy
Consumer Action
Consumer Federation of America
Consumers Union
Consumer Watchdog
Electronic Frontier Foundation
Privacy Lives
Privacy Rights Clearinghouse
Privacy Times
U.S. Public Interest Research Group
The World Privacy Forum

May 3, 2010

Dear Representative,

We write to support principles for shaping strong privacy legislation. The tracking and targeting of consumers online have reached alarming levels. Companies engaged in behavioral targeting routinely monitor individuals, the searches they make, the Web pages they visit, the content they view, their interactions on social networking sites, the content of their emails, and the products and services they purchase. Further, when consumers are using mobile devices, even their physical location is tracked. This data is compiled, analyzed, and combined with information from offline sources to create even more detailed profiles.

This tracking is an invasion of privacy. Marketers claim that the goal of this unprecedented surveillance is simply to make the online experience more "personalized" and "convenient" by providing consumers with more "relevant" advertising—sales pitches more aligned, that is, to their particular needs and interests. But consumers now rely on the Internet and other digital services for many purposes. Some of their online activities involve sensitive matters such as health and finances. In these contexts, tracking people's every move online is not simply a matter of convenience or relevance. It presents serious risks to consumers' privacy, security and dignity.

Consumers have rights, and profiling should have limits. Behavioral tracking and targeting can and has been used to take advantage of vulnerable individuals, and to unfairly discriminate against people. The potential misuse of health or financial information is especially troubling. The assumptions that can be made about people based on behavioral tracking – such as sexual orientation or medical diagnosis – may have detrimental consequences for them, including loss of a job or health insurance. Online profiles may also be obtained by government agencies, private investigators, and other entities for purposes that go far beyond advertising.

As you well know, privacy is a fundamental right in the United States. For four decades, the foundation of U.S. privacy policies has been based on Fair Information Practices: collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability.

Those principles ensure that individuals are able to control their personal information, help to protect human dignity, hold accountable organizations that collect personal data, promote good business practices, and limit the risk of identity theft. Developments in the digital age urgently require the application of Fair Information Practices to new business practices. As Congress moves ahead in this area, we trust that the following principles and goals will be incorporated in new online privacy legislation.

Principles for Shaping Legislation

- Robust Fair Information Practices are the key to legislation concerning online privacy.
- Notice and choice are inadequate to protect consumers. Transparency is not enough if consumers have no real understanding or control.
- Self-regulation for privacy will not protect consumers.
- Law enforcement access to personal data should require a warrant.

The following goals should also be addressed in the new legislation:

Specific Goals to Protect Consumers

- The privacy of individuals should be protected even if the information collected about them in behavioral tracking cannot be linked to their names, addresses, or other overt identifiers. As long as consumers can be distinguished based on IP addresses, cookies, or other characteristics, their privacy interests must be protected.

- The ability of websites and ad networks to collect or use behavioral data should be limited to 24 hours, after which affirmative consent (opt-in) should be required.

- Websites should not collect or use sensitive information for behavioral tracking or targeting. The FTC should be tasked with defining sensitive information, which must include data about health records, financial records, ethnicity, race, sexual orientation, personal relationships, and political activity.

- Personal data should be obtained only by lawful and fair means and, unless unlawful or impossible, with the knowledge or consent of the individual.

- Personal and behavioral data should be relevant to the purposes for which they are to be used.

- Websites should specify the purposes for which they collect both personal and behavioral data not later than the time of data collection. Websites should not disclose or use personal

and behavioral data for purposes other than those specified in advance except: a) with the consent of the individual; or b) when required by law.

- Websites should be responsible for providing reasonable security safeguards for personal and behavioral data, including protection against unauthorized access, modification, disclosure and other risks.

- Websites should disclose their practices, uses, and policies for personal and behavioral data.

- An individual should have the right to: a) be told by behavioral tracker whether the behavioral tracker has data relating to the individual; b) obtain a copy of the data within a reasonable time, at a reasonable charge, and in a form that is readily intelligible to a consumer; and c) correct the data or, if requested, have all the data removed from the behavior tracker's database within a week.

We look forward to working with you and your staff on this important issue. Please contact any of these representatives if we can provide further information: Jeff Chester, Center for Digital Democracy at 202-494-7100; Pam Dixon, World Privacy Forum at 760 470 2000; John Simpson, Consumer Watchdog at 310-392-0522 ext. 317; or, Ed Mierzwinski of U.S. PIRG at 202-461-3821.

Sincerely,

Center for Digital Democracy
Consumer Action
Consumer Federation of America
Consumers Union
Consumer Watchdog
Electronic Frontier Foundation
Privacy Lives
Privacy Rights Clearinghouse
Privacy Times
U.S. Public Interest Research Group
The World Privacy Forum