

Behavioral Tracking and Targeting -- September 2009

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. Today, electronic information from consumers is collected, compiled, and sold; all done without reasonable safeguards.

People increasingly rely on the Internet for a wide range of transactions and services, many of which involve their health, finances, and other sensitive matters. At the same time, technology enables information about people's activities online to be tracked over time and analyzed for many purposes, including targeting them with advertising that may be more relevant. Data derived offline can be combined with online data to create even more detailed profiles. The data that is collected through behavioral tracking can, in some cases, reveal the identity of the person, but even when it does not, tracking and using such data raises serious concerns.

Tracking people's every move online is an invasion of privacy. Online behavioral tracking is even more distressing when consumers aren't aware who is tracking them, that it's happening, or how the information will be used. Often consumers are not asked for their consent and have no meaningful control over the collection and use of their information, often by third parties with which they have no relationships.

Online behavioral tracking and targeting can be used to take advantage of vulnerable consumers. Information about a consumer's health, financial condition, age, sexual orientation, and other personal attributes can be inferred from online tracking and used to target the person for payday loans, sub-prime mortgages, bogus health cures and other dubious products and services. Children are an especially vulnerable target audience since they lack the capacity to evaluate ads.

Online behavioral tracking and targeting can be used to unfairly discriminate against consumers. Profiles of individuals, whether accurate or not, can result in "online redlining" in which some people are offered certain consumer products or services at higher costs or with less favorable terms than others, or denied access to goods and services altogether.

Online behavioral profiles may be used for purposes beyond commercial purposes. Internet Service Providers (ISPs), cell phone companies, online advertisers and virtually every business

on the Web retain critical data on individuals. In the absence of clear privacy laws these profiles leave individuals vulnerable to warrantless searches, attacks from identity thieves, child predators, domestic abusers and other criminals.

Right now, individuals have little to no control over who has access to their online information, how it is secured, and under what circumstances it may be obtained.

To protect the interests of Americans, while maintaining robust online commerce, Congress must enact clear legislation to protect consumers' privacy online which implements Fair Information Practices. While these recommendations are not exhaustive, they do represent areas in which the leading organizations concerned with consumer privacy are in consensus. Consumer privacy legislation should include these main points (for more detailed recommendations, please see the Legislative Recommendations Primer):

- *Individuals should be protected even if the information collected about them in behavioral tracking cannot be linked to their names, addresses, or other traditional "personally identifiable information," as long as they can be distinguished as a particular computer user based on their profile.*
- *Sensitive information should not be collected or used for behavioral tracking or targeting.*
- *No behavioral data should be collected or used from children and adolescents under 18 to the extent that age can be inferred.*
- *The ability of websites and ad networks to collect and use behavioral data should be limited to 24 hours, after which affirmative consent should be required.*
- *Behavioral data should not be retained for more than 3 months.*
- *Pretexting should not be used to obtain personal or behavioral data from individuals.*
- *Behavioral trackers and targeters should adopt policies, as relevant, for the types of data that will be collected and how that information will be maintained and used, and clearly explain those policies on their websites.*
- *Personal and behavioral data should not be used or disclosed in a manner that is inconsistent with published policies, except where required by law.*
- *Behavioral data shouldn't be used in any way other than for the advertising purposes for which it was collected.*
- *Ads based on behavioral data should contain links to consumer-friendly explanations and controls.*
- *A targeter or tracker that has personal or behavioral data should not use the data or compiled profile in a manner that could affect an individual's credit, education, employment, insurance, access to government benefits or resources.*
- *Neither personal nor behavioral data should be used in any way that would unfairly discriminate against an individual.*
- *Reasonable security safeguards against loss, unauthorized access, modification, disclosure and other risks should protect both personal and behavioral data.*
- *Individuals should have the right to confirm whether a data controller has their personal or behavioral data, request such data, and delete it.*

- *Each organization involved in any behavioral tracking and targeting should be accountable for complying with the law and its own policies.*
- *Consumers should have the right of private action with liquidated damages.*
- *Data collected for behavioral tracking or targeting should be protected by the constitutional safeguards that rule evidence collection.*
- *The FTC should establish a Behavioral Tracker Registry.*
- *There should be no preemption of state laws.*

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