Online Behavioral Tracking and Targeting Concerns and Solutions from the Perspective of:

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
The World Privacy Forum

Legislative Primer September 2009

Table of Contents

Executive Summary:

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.

Consumers are increasingly relying 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. At the same time many companies are now engaging in behavioral advertising, which involves the surreptitious tracking and targeting of consumers. Click by click, consumers' online activities – the searches they make, the Web pages they visit, the content they view, the videos they watch and their other interactions on social networking sites, the content of emails they send and receive, how they spend money online, their physical locations using mobile Web devices, and other data – are logged into an expanding profile and analyzed in order to target them with more "relevant" advertising.

This is different from the "targeting" used in contextual advertising, in which ads are generated by a search that someone is conducting or a page the person is viewing at that moment. Behavioral tracking and targeting can combine a history of online activity across the Web with data derived offline 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, the tracking of individuals and the trade of personal or behavioral data raise many concerns.

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 retains critical data on individuals. In the absence of clear privacy laws and security standards these profiles leave individuals vulnerable to warrantless searches, attacks from identity thieves, child predators, domestic abusers and other criminals. Also, despite a lack of accuracy, employers, divorce attorneys, and private investigators may find the information attractive and use the information against the interests of an individual. Individuals have no control over who has access to such information, how it is secured, and under what circumstances it may be obtained.

In order to protect the interests of Americans, while maintaining robust online commerce, we recommend that Congress enact clear legislation to protect consumers' privacy online that 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. Sensitive information should be defined by the FTC and should include data about health, finances, ethnicity, race, sexual orientation, personal relationships and political activity.*

- *No behavioral data should be collected or used from children and adolescents under 18 to the extent that age can be inferred.*

- *There should be limits to the collection of both personal and behavioral data, and any such data should be obtained by lawful and fair means and, where appropriate, 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.*

- *The purposes for which both personal and behavioral data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes, and with any change of purpose of the data the individual must be alerted and given an option to refuse collection or use.*

- *Personal and behavioral data should not be disclosed, made available or otherwise used for purposes other than those specified in advance except: a) with the consent of the individual; or b) by the authority of law.*

- *Reasonable security safeguards against loss, unauthorized access, modification, disclosure and other risks should protect both personal and behavioral data.*

- *There should be a general policy of openness about developments, practices, uses and policies with respect to personal and behavioral data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.*

- *An individual should have the right: a) to obtain from a behavioral tracker, or otherwise, confirmation of whether or not the behavioral tracker has data relating to him; b) to have communicated to him data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and d) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.*

- *Consumers should always be able to obtain their personal or behavioral data held by an entity engaged in tracking or targeting.*

- *Every entity involved in any behavioral tracking or targeting activity should be accountable for complying with the law and its own policies.*

- *Consumers should have the right of private action with liquidated damages; the appropriate protection by federal and state regulations and oversight; and the expectation that online data collection entities will engage in appropriate practices to ensure privacy protection (such as conducting independent audits and the appointment of a Chief Privacy Officer).*

- *If a behavioral targeter receives a subpoena, court order, or legal process that requires the disclosure of information about an identifiable individual, the behavioral targeter must, except where otherwise prohibited by law, make reasonable efforts to a) notify the individual prior to responding to the subpoena, court order, or legal process; and b) provide the individual with as much advance notice as is reasonably practical before responding.*

- *The FTC should establish a Behavioral Tracker Registry.*

- *There should be no preemption of state laws.*

Behavioral Targeting & Online Privacy, Legislative Recommendations

Part I. Findings and Goals

1. Entities that behaviorally target seek to create, compile, and use detailed profiles revealing consumers' interests, activities, and other personal characteristics without limit. A major purpose of behavioral targeting is increasing response rates to advertising. Any economic benefits of behavioral targeting must be measured against the consequences for consumers of the creation and sharing of those profiles. Without controls, profiles can and will be used for commercial, governmental, and other purposes in ways that may harm consumers.

Consumer privacy must be given special and priority consideration when government "measures" the economic benefits related to any data collection activity.

Precedent: The Video Privacy Protection Act limits the compilation of video rental profiles to protect privacy, notwithstanding the loss of advertising capability to industry.

2. Americans oppose the collection and sharing of financial, health, and other sensitive personal information for non-essential purposes. Unrestricted, an online profile may include a wide range of sensitive information about the ethnic, racial, financial, and health status of a consumer. Children and adolescents are also subjects of profiling and targeting. The use of sensitive information for behavioral targeting is questionable, harmful, and invasive.

Sensitive information should not be collected or used for behavioral tracking or targeting. Sensitive information should be defined by the FTC and should include data about health, finances, ethnicity, race, sexual orientation, and political activity.

Precedent: Fair Credit Reporting Act. HIPAA Health Privacy Rule.

3. Redlining is the practice of denying or increasing the cost of services such as banking, insurance, access to jobs, access to health care, or even supermarkets to residents in certain, often racially determined, areas. Redlining can discriminate against people based on race, gender, sexual preference, ethnic origin, disability, wealth, income, and other characteristics.

Behavioral targeting can make secret and inappropriate distinctions among consumers based on these characteristics. Some forms of redlining may violate existing law, and some forms of redlining seek to manipulate vulnerable populations.

Use of behavioral targeting for individual redlining activities should be illegal.

Precedent: Equal Credit Opportunity Act

4. Americans support the protection of online information about children. Yet children and adolescents are the focus of a wide range of digital marketing techniques, including behavioral targeting. A decade ago, bi-partisan legislation was enacted (COPPA) designed to protect children under 13 from unfair data collection practices.

However, with recently developed data collection techniques, the targeting of children and adolescents is now a part of their everyday online world. Children are increasingly subjected to a wide array of behavioral targeting practices through social networks, games, mobile services, and other digital platforms that use techniques that evade current legal restrictions.

Scholars in neuroscience and psychology have identified a number of biological and psychosocial attributes that make adolescents particularly vulnerable to behavioral targeting. Existing legislation needs to be updated to cover new threats to privacy from many of the behavioral targeting practices that have emerged since passage of COPPA in 1998.

No behavioral data should be collected or used from children and adolescents under 18 to the extent that age can be inferred.

Precedent: Children's Online Privacy Protection Act (1998).

5. Contextual advertising that does not involve the maintenance of information beyond the current online session within a website or series of websites does not need to be regulated for privacy at this time. Reasonable limitations on behavioral targeting do not threaten the advertising-supported model of Internet availability.

6. Self-regulation for privacy has consistently failed. Self-regulatory efforts for behavioral targeting that are developed without meaningful participation by consumers will not strike a fair balance.

Government must create a baseline that will guarantee protection for consumer privacy and must also provide proper enforcement to ensure that any illegal behavior is prosecuted quickly.

Precedent: Failed self-regulatory efforts include IRSG, NAI, BBO Online, Privacy Leadership Initiative, Online Privacy Alliance.

Part II. Fair Information Practices for Legislation/Regulation

A. Collection Limitation Principle

There should be limits to the collection of both personal and behavioral data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the individual.

BT Implementation Ideas:

1. Any consent for the collection of information for behavioral targeting purposes must be recent (e.g., within three months) and revocable. Once consent has expired or been revoked, information collected with consent must be deleted promptly.

2. No forms of pretexting can be used to obtain user information. For example, a contest

that seeks the collection of consumer information in exchange for the chance to win a prize is a pretext.

B. Data Quality Principle
Personal and behavioral data should be relevant to the purposes for which they are to be used.

BT Implementation Ideas:

1. Websites should only initially collect and use data from consumers for a 24-hour period, with the exception of information categorized as sensitive, which should not be collected at all. Any subsequent use or collection of non-sensitive consumer data must have the affirmative consent of the individual user, including specific consent for any sale or other sharing of the data.

2. Data collected on users who consent must not be retained beyond a period of three months (the new Yahoo standard).

C. Purpose Specification Principle
The purposes for which both personal and behavioral data are collected should be specified not later than at the time of data collection, and the subsequent use limited to the fulfillment of those purposes and with any change of purpose of the data the individual must be alerted and given an option to refuse collection or use.

D. Use Limitation Principle
Personal and behavioral data should not be disclosed, made available or otherwise used for purposes other than those specified in advance except: a) with the consent of the individual; or b) by the authority of law.

BT Implementation Ideas:

1. A behavioral targeter must determine in advance and in writing the purposes for which it plans to use and disclose information about individuals. Those purposes must be explained in a privacy policy that must be publicly available to all on the website of the organization collecting and maintaining user data.

2. Websites and other online services collecting user data must clearly and prominently provide on their ads—via linked webpages as well as within privacy policies—a consumer-friendly explanation of their data collection practices.

3. A behavioral targeter cannot use or disclose information about an individual in a manner that is inconsistent with its published notice, except where required by law.

4. No behavioral targeting data can be used by any person in any way other than for the advertising purposes for which it was collected. The use of the data for any credit, employment, insurance, or governmental purpose or for redlining should be prohibited.

E. Security Safeguards Principle
Reasonable security safeguards against loss, unauthorized access, modification, disclosure and other risks should protect both personal and behavioral data.

BT Implementation Ideas:

1. A behavioral targeter must (A) establish appropriate administrative, physical, and technical safeguards to ensure the security and confidentiality of information about individuals, and (B) protect against any anticipated threats or hazards to security or integrity that could result in substantial harm, embarrassment, inconvenience, or unfairness to the individual.

F. Openness Principle
There should be a general policy of openness about developments, practices, uses and policies with respect to personal and behavioral data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

BT Implementation Ideas:

1. A behavioral targeter must have a publicly available privacy policy that describes its practices and policies with respect to the collection, maintenance, use, and disclosure of information about an individual used for behavioral targeting. The privacy policy must describe the categories of information collected, the categories of information maintained, the source of the information, the uses of the information, the disclosures of the information, and the sale and distribution methods. A behavioral targeter need not include in its privacy policy any trade secret. The privacy policy must be understandable by the average consumer.

2. In order to change its privacy policy, a behavioral targeter must provide public notice on its website 30 days in advance of the change and, at the same time, specific notice to any person who has requested notice of privacy policy changes.

3. Any change to a privacy policy that has the effect of allowing additional uses or disclosures of information about an individual may apply only to information collected after the effective date of the change.

G. Individual Participation Principle
An individual should have the right:
- *a) to obtain from a behavioral tracker, or otherwise, confirmation of whether or not the behavioral tracker has data relating to him;*
- *b) to have communicated to him data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him;*
- *c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and*

d) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.

BT Implementation Ideas:

1. Individuals should have the right to see, have a copy of, and delete any information about them. If a behavioral targeter is able to use information to target an individual in more than one online session, then the targeter must provide the individual with the opportunity to see, have a copy of, and delete the information about that individual that the targeter maintains.

2. Consumers should always be able to obtain their personal or behavioral data held by a business engaged in tracking or targeting.

3. A behavioral targeter may reject excessive requests for access.

4. If a behavioral targeter receives a subpoena, court order, or legal process that requires the disclosure of information about an identifiable individual, the behavioral target must, except where otherwise prohibited by law, make reasonable efforts to notify the individual prior to responding to the subpoena, court order, or legal process; and provide the individual with as much advance notice as is reasonably practical before responding.

H. Accountability Principle
Every entity involved in any behavioral tracking or targeting activity should be accountable for complying with the law and its own policies.

I. Redress Principle
Consumers should have the right of private action with liquidated damages; the appropriate protection by federal and state regulations and oversight; and the expectation that online data collection entities will engage in appropriate practices to ensure privacy protection (such as conducting independent audits and the appointment of a Chief Privacy Officer).

BT Implementation Ideas:

1. A behavioral targeter must accept and give reasonable consideration to a complaint from any individual who has a reasonable basis for believing that the behavioral targeter has or uses information about the individual. A behavioral targeter must promptly acknowledge the receipt of a complaint, must respond to all complaints within 30 days, and may extend the time for response by an additional 30 days by giving notice in writing or by email to the complainant.

2. Consumers aggrieved by behavioral targeting activities that violate the law or a published policy should have the right of private action that allows for the awarding of liquidated damages, attorney fees, and costs for successful plaintiffs.

3. Federal and state agencies may bring enforcement actions on behalf of consumers for

violations of law or policy.

4. The FTC should maintain an online registry of organizations that engage in behavioral tracking. Behavioral tracking organizations should be required to provide current information to the FTC registry that will, at a minimum:

a) contain technical information required so that consumers can opt out of tracking through tracking cookies, browser settings or extensions, and other methods.
b) appear online in a format so that third parties can develop consumer tools such as browser settings or extensions or tracking cookie management software that will automatically update from the registry.
c) include the name, physical address, and contact information of the BT company doing the tracking, along with information about how to file a complaint about the company or about its opt-out procedures.
d) include a complete description of the categories of consumer information collected, all online and other sources of consumer information, and the countries where the information is stored.

5. A behavioral targeter must provide privacy training to all appropriate staff annually.

6. A behavioral targeter must conduct an independent audit of its operations for compliance with this law, and it must make the results of that audit public.

7. A behavioral targeter must designate a Chief Privacy Officer to supervise implementation of and compliance with its privacy policy.

8. There should be no preemption of state laws.

Part III. Definitions

1. Behavioral Targeting: The practice of collecting and compiling data from and about an individual's activities, interests, preferences, behaviors, or communications for interactive advertising and marketing targeted to the individual, including but not limited to the use of a profile that may be stored or linked to a browser cookie, IP address, or any other persistent user identifiers or tracking methods. Behavioral targeting does not include contextual advertising.

2. Individual: An individual includes any

a) individual identified by name, address, account number, or other identifying particular assigned to the individual; and
b) user of any online service or facility who is targeted (1) based on information obtained in more than a single transaction, online encounter, or other online activity; (2) notwithstanding the absence of a name, address, account number, or other identifying particular about the user known to the behavioral targeter; and (3) when the behavioral targeter has any reason to believe that the user being targeted is a particular user about whom the behavioral targeter obtained information in the past or from another source, including the use of IP addresses, browser cookies, and other persistent user identifiers or tracking methods.

3. Contextual Advertising: Contextual advertising is online advertising that does not involve the maintenance or storage of information about an individual beyond the current online session with a website or series of websites.

4. Profile: Data stored electronically containing information about an individual's online activities and behaviors, whether or not the name or other identifier of the individual is included in the profile, and whether or not the data include information obtained from offline sources.

5. Behavioral Targeter: Any organization, including its agents, affiliates, and partners, engaging in behavioral targeting (for commercial, non-profit, or governmental purposes).

6. Financial information: Any information, regardless of source, about an individual's income, wealth, investments, or bank or other financial accounts.

7. Health information: Any information, regardless of source, that relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; and the past, present, or future payment for the provision of health care to an individual.

About the members of the coalition:

Center for Digital Democracy: The Center for Digital Democracy (CDD) is dedicated to ensuring that the public interest is a fundamental part of the new digital communications landscape. URL: http://www.democraticmedia.org

Consumer Federation of America: Since 1968, the Consumer Federation of America (CFA) has provided consumers a well-reasoned and articulate voice in decisions that affect their lives. URL: http://www.consumerfed.org

Consumers Union: Consumers Union is a nonprofit membership organization chartered in 1936 under the laws of the State of New York to provide consumers with information, education and counsel about goods, services, health, and personal finance.
URL: http://www.consumersunion.org

Consumer Watchdog: Consumer Watchdog (formerly The Foundation for Taxpayer and Consumer Rights) is a consumer group that has been fighting corrupt corporations and crooked politicians since 1985. URL: http://www.consumerwatchdog.org

Electronic Frontier Foundation: When freedoms in the networked world come under attack, the Electronic Frontier Foundation (EFF) is the first line of defense. URL: http://www.eff.org

Privacy Lives: Published by Melissa Ngo, the Website chronicles and analyzes attacks on privacy and various defenses against them to show that privacy lives on, despite the onslaught. URL: http://www.privacylives.com

Privacy Rights Clearinghouse: The Privacy Rights Clearinghouse is a consumer organization with a two-part mission: To raise consumer awareness about privacy and to advocate for privacy rights in policy proceedings. URL: http://www.privacyrights.org

Privacy Times: Privacy Times is the leading Subscription-only newsletter covering privacy & Freedom of Information Law and policy. Since 1981, Privacy Times has provided its readers with accurate reporting, objective analysis and thoughtful insight into the events that shape the ongoing debate over privacy and Freedom of Information. URL: http://www.privacytimes.com

U.S. Public Interest Research Group: The federation of state Public Interest Research Groups (PIRGs) stands up to powerful special interests on behalf of the public, working to win concrete results for our health and our well-being. URL: http://www.uspirg.org

The World Privacy Forum: WPF is focused on conducting in-depth research, analysis, and consumer education in the area of privacy. Areas of focus include health care, technology, and the financial sector. URL: http://www.worldprivacyforum.org