The Report Committee for Meredith Catherine Whipple
Certifies that this is the approved version of the following report:

Regulating Consumer Profiling: Going Beyond Behavioral Advertising

APPROVED BY
SUPERVISING COMMITTEE:

Supervisor: _____
Jennifer Bussell

_____
Philip Doty

_____
Angela Newell

Regulating Consumer Profiling:
Going Beyond Behavioral Advertising

by

Meredith Catherine Whipple, B.A.

Report

Presented to the Faculty of the Graduate School of

The University of Texas at Austin

in Partial Fulfillment

of the Requirements

for the Degree of

Master of Public Affairs

The University of Texas at Austin

May 2012

Abstract

Regulating Consumer Profiling: Going Beyond Behavioral Advertising

Meredith Catherine Whipple, MPAff

The University of Texas at Austin, 2012

Supervisor: Jennifer Bussell

The following report is an examination of consumer tracking and profiling in the United States. The paper presents perspectives on the current discussion surrounding regulation of consumer tracking. It begins with an explanation of the evolution of tracking technologies and tracking prevention tools. This is followed by a discussion of the outcomes of self-regulatory initiatives, as well as existing regulatory efforts from the Federal Trade Commission (FTC) and standardization initiatives from the World Wide Web Consortium (W3C). This background information is used to examine "specialty consumer reporting agency" Web sites, information brokers that exist solely to create profiles about individuals and sell these profiles online. This research presents a content analysis of privacy policies for 29 of these Web sites. Specifically, the content analysis focuses on the legal language they use in their presentation of Federal Credit Reporting Act (FCRA) disclaimers, the listed sources of their information, and their instructions for users to correct or remove their information. The conclusion from the findings is that many of these Web sites are engaging in deceptive practices as defined by the FTC. As a

solution, the FTC could enforce FCRA requirements on these Web sites by requiring that consumers be able to access this information, dispute inaccurate information, understand how their information is gathered and used, and opt out of having a profile completely. The FTC also can create a centralized Web site where specialty consumer reporting agencies identify themselves to consumers, describe how they collect and use consumer data, and detail the access rights and other choices they provide with respect to the consumer data they maintain. Finally, the paper concludes with a summary of online privacy initiatives in the European Union, and an explanation of the requirements of United States compliance with these policies when taking part in the European marketplace.

Table of Contents

Introduction

Today, it is commonplace for Web sites to track behaviors and collect information about their users, typically in order to provide them with targeted advertisements based on the individual interests of these users. But consumer tracking is not a new phenomenon. For decades, businesses have tracked the customers that come into their store through credit card purchases, coupon use, surveys, mail-in refunds, and received phone calls.[1] Companies have a goal of achieving the best marketing strategy, and by giving their customers advertisements based on their previous purchases, as well as the purchases of other customers similar to them, they are likely to encourage more buying from those customers in the future. It is reasonable to expect that businesses would want to track the purchases of their customers in order to maximize their profits.

In the world of online companies, behavioral tracking of customers has become easier and more prevalent. Web sites are increasingly more interactive, and customers more freely give up personal information in order to use Web sites, so the information these companies have access to has increased greatly. In April 2010, a Wall Street Journal investigative series entitled "What They Know" reported that the 50 most popular U.S. Web sites installed an average of 64 tracking tools onto visitors' computers, usually

---

[1] Charles Duhigg, "How Companies Learn Your Secrets," *The New York Times*, 16 February 2012, <http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?_r=2&pagewanted=1&hp>.

with no warning.[2] This increased awareness of behavioral tracking and resulted in an increase in calls for regulation from the public.

Behavioral tracking is not just used for the purposes of advertising, however. One common use of behavioral tracking that has not received as much attention is for data broker Web sites. These Web sites, known as specialty consumer reporting agencies, collect data on individuals in order to create personal profiles for the purposes of being sold. The following chapters will discuss this use of tracking and the legal questions that arise, particularly violations of the Fair Credit Reporting Act (FCRA). It will examine the potential for discrimination and jeopardized personal safety that arises, and how regulatory efforts can address these concerns.

[2] Julia Angwin, "The Web's New Gold Mine: Your Secrets," 30 July 2010, <http://online.wsj.com/article/SB10001424052748703940904575395073512989404.html>.

Chapter 1: Tracking Tools

Before discussing the regulatory efforts, it is important to understand *how* Web sites track their users. Historically, most Web site tracking has been accomplished through cookies, small files that Web sites can put on a user's hard drive with each Web page visit. This cookie notifies the Web site each time that user returns. A Web site can either store a unique identifier anyplace in the browser, known as tagging, or explore features of the browser until it becomes unique, known as fingerprinting.[3]

Web sites use cookies for a variety of purposes. Some cookies make online shopping efficient, such as through saving a user's selections in a virtual shopping cart for check-out. Web sites also have cookies that allow users to save username information so that they can log in quickly. Web sites often collect anonymous data through cookies for the purposes of analytics, such as data about Web site use that helps them make improvements. Furthermore, many users are not aware that some cookies enable Web sites to prevent fraud and respond to security incidents.

There is also an important distinction between tracking from first-party Web sites and tracking from third-party Web sites. Third-party Web sites are often affiliated through a contract with a first-party Web site for the purpose of advertising implementation, analytical research, fraud prevention, or social network integration. Over

---

[3] Mika D. Ayenson et al., "Flash Cookies and Privacy II: Now With HTML5 And ETag Respawning," *Social Science Research Network* (July 2011), <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1898390>.

time, tracking technologies have evolved, and third-party involvement has increased. As I will describe in Chapter 3 and Chapter 4, regulatory efforts to date are almost entirely focused exclusively on third-party tracking.

In the past few years, tracking has advanced from the use of regular cookies, known as "HTML cookies." Researchers have discovered Web sites using "supercookies," tracking technologies that do not rely on HTML cookies. Supercookies continue tracking even when a user clears his or her HTML cookies, recreating a profile of the information gathered from the user's behavior. Some supercookies can recreate deleted cookies, which are known as "zombie cookies."[4] Two frequently used types of supercookies are Flash cookies and ETags.

Flash cookies, also referred to as "local shared objects," are files used by Adobe Flash developers to store data on users' computers. Flash cookies have many advantages over regular cookies. They can contain up to 100KB of information by default, as opposed to the HTTP cookie storage of 4KB. Flash cookies do not have expiration dates by default, whereas HTTP cookies expire at the end of a session unless programmed to live longer by the domain setting the cookie. Also, the stored location of Flash cookies is different from the location than HTTP cookies, so users may not know what files to

[4] Duhigg.

delete in order to eliminate them. A Flash cookie is typically used with an identical HTML cookie in order to automatically recreate that HTML cookie if it is deleted.[5]

The browser does not control Flash cookies. Therefore, erasing HTTP cookies, clearing history, erasing the cache, or choosing a "delete private data" option within the browser does not affect Flash cookies. "Private Browsing" modes still allow Flash cookies to operate fully and track the user, as does downloading cookies designed to indicate that a user wants to block targeted ads, known as opt-out cookies. However, besides being an excellent tool for gathering consumer data and respawning deleted cookies, Flash cookies also serve another function. They allow a given application to "save state" on a computer, such as through storing the volume level of a Flash video or caching a music file for better performance over an unreliable network connection.[6]

An ETag functions similarly. With HTML cookies, a Web site assigns a version number to a resource. When the browser goes to request the resource (which is what the URL identifies), and the version has not changed, the Web site can tell the browser to use its cached copy. However, instead of a version number, ETags can be stored. ETags generate unique tracking values even when the consumer blocks HTTP, Flash, and HTML5 cookies. In order to block this tracking, the user would have to clear the cache between each Web site visit. Even in private browsing mode, ETags can track the user

---

[5] Ashkan Soltani et al., "Flash Cookies and Privacy," *Social Science Research Network* (August 2009), <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1446862>.

[6] Soltani et al.

during a browser session. Because ETags are cached by the browser, and returned with subsequent requests for the same resource, a tracking server can simply repeat any ETag received from the browser to ensure an assigned ETag persists indefinitely.[7] Privacy policies rarely disclose the use of Flash cookies or of ETags, so users cannot opt out of receiving them.

A team of researchers at the University of California at Berkeley have an ongoing project examining the use of these tools. In a 2009 study, the team surveyed the top 100 Web sites ranked by the company Quantcast on July 1, 2009. Of these, they found 98 using HTTP cookies and 54 using Flash cookies. Thirty-one sites had at least one overlap between an HTTP and a Flash cookie, indicating a third-party advertiser implementing cookie respawning. Thirty-one of the 100 sites had a TRUST-e Privacy Seal, which indicates that the sites are complying with their own privacy policies. However, many of these sites were not. Only four sites mentioned the use of Flash cookies.[8]

Two years later, the UC-Berkeley researchers examined the state of Flash cookies and ETags with a similar study, using the top 100 Web sites based on Quantcast's rankings from July 13, 2011. They detected 5,675 HTTP cookies, a significant increase from their finding of 3,602 cookies in 2009. Third-party companies had placed 4,915 of these cookies. Although the number of Flash cookies decreased, the researchers noted the

[7] Ayenson et al.

[8] Soltani et al.

first appearance of ETags to accomplish respawing of cookies instead.[9] Blocking tools had evolved, but designers of tracking technologies found ways around this.

There have been a series of lawsuits and legal consequences surrounding these advanced cookie technologies. In recent years, Disney, Warner Brothers, MySpace, ABC, and NBCUniversal have all had lawsuits filed against them for zombie cookies. In 2010, the online tracking firm Quantcast paid $2.4 million to settle a class action lawsuit regarding its use of Adobe's Flash plug-in to recreate tracking cookies after users deleted them. The company's Web site clients, including ESPN, Hulu and MTV.com, were sued on the grounds that they violated the federal computer intrusion law.[10] Other class action lawsuits have included large media companies such as the Fox Entertainment Group and Web technology companies such as Clearspring Technologies, charged with not disclosing their use of Flash cookies to users or receiving consent.[11]

The detection of tracking technologies has improved over time as well. In the second study from the UC-Berkeley team, the researchers discovered that Hulu and the tracking company Kissmetrics were using ETags, which resulted in multiple class action lawsuits. They were accused of violating the federal wiretap law and the computer fraud

---

9 Ayenson et al.

10 Ryan Singel, "Online Tracking Firm Settles Suit Over Undeletable Cookies," *Wired*, 5 December 2010, <http://www.wired.com/epicenter/2010/12/zombie-cookie-settlement/>.

11 Tanzina Vega, "Code That Tracks Users' Browsing Prompts Lawsuits," *The New York Times*, 20 September 2011, <http://www.nytimes.com/2010/09/21/technology/21cookie.html?pagewanted=all>.

law, along with some state laws.[12] In August 2011, a separate team of Stanford researchers discovered Microsoft using zombie cookies—a cache-based cookie and a supercookie together—in their Web sites. Microsoft did this by using a script called wlHelper.js, which they stored along with a cookie in the browser cache. If a user deleted the cookie but did not empty the browser cache, the script recreated the deleted cookie. Once notified, Microsoft responded that they were not aware of the problem, and worked with Mayer to remove the cookies.[13] One of the authors of the UC-Berkeley study, Chris Jay Hoofangle, stated that the recent lawsuits are evidence of a weakness in federal governing of online privacy.[14]

---

12 Wendy David, "KISSmetrics, Hulu Hit with Privacy Suit," *MediaPost News*, 19 September 2011, <http://www.mediapost.com/publications/article/158730/>.

13 Jonathan Mayer, "Tracking the Trackers: Microsoft Advertising" *The Center for Internet and Society*, 18 August 2011, <http://cyberlaw.stanford.edu/blog/2011/08/tracking-trackers-microsoft-advertising>.

14 Tanzina Vega.

Chapter 2: Self-regulatory initiatives

There have been a series of attempts to self-regulate behavioral tracking by the online advertising industry. The main professional association for these businesses is the Digital Advertising Alliance (DAA), a consortium of the leading national advertising and marketing companies. Founded in 2009, the DAA soon succeeded the Network Advertising Initiative (NAI) as the leader of self-regulation efforts. The FTC previously encouraged self-regulation, but regulatory efforts from the NAI and the DAA have largely failed. For example, for over a decade, the NAI has offered users the ability to download an opt-out cookie. However, downloading opt-out cookies only prevents users from seeing targeted ads, which are based on information gathered from tracking. They do not prevent tracking itself. Furthermore, opt-out cookies require manual updating, and they usually expire without the user's knowledge. In fact, at least two other pieces of research have demonstrated significant confusion among users about the function of opt-out cookies and how to implement them.[15]

The NAI also launched a program to include a label on ads that are sent to users based on behavioral tracking data, and give the users the option to block these ads. This is known as the AdChoices label. However, this program has not shown to be successful.

---

15 A. M. McDonald and Lorrie Faith Cranor, "Beliefs and behaviors: Internet users' understanding of behavioral advertising," *Social Science Research Network* (October 2010), <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1989092>; Pedro G. Leon et al., "Why Johnny can't opt out: A usability evaluation of tools to limit online behavioral advertising," *Carnegie Mellon University CyLab* (October 2011), <http://www.cylab.cmu.edu/research/techreports/2011/tr_cylab11017.html>.

Stanford's Computer Science Security Lab conducted a study of the 500 most popular Web sites, as ranked by Alexa.com on August 4, 2011. They found that only 9 percent of the ads they examined (62 out of 627 ads) contained the label.[16] In March 2011, researchers at Carnegie Mellon University examined the document that outlines the DAA principles, "Self-Regulatory Principles for Online Behavioral Advertising," and the level of compliance by Web sites. They looked at the 66 NAI Web sites and found that only 35 percent of ads included the label, whereas industry estimates indicated that 80 percent were targeted ads.[17]

Both of these self-regulatory groups have focused on advertising. As I will discuss in subsequent chapters, the problem of tracking goes well beyond advertising, and yet the public debate seems to be centered there. Media, research, and policymakers often use the term "Online Behavioral Advertising." However, tracking is not simply used for advertising. Some companies use tracking to collect information about individuals and create personal profiles for the purposes of selling them. As previously stated, these companies are known as specialty consumer reporting agencies. Employers, insurers, medical professionals, and creditors all can use this information to deny people jobs,

16 "Tracking the Trackers: The AdChoices Icon," *The Center for Internet and Society*, 18 August 2011, <http://cyberlaw.stanford.edu/node/6714>.

17 Saranga Komanduri et al., "AdChoices? Compliance with Online Behavioral Advertising Notice and Choice Requirements," *Carnegie Mellon University CyLab* (March 2011), <http://www.casos.cs.cmu.edu/publications/papers/CMUCyLab11005.pdf>.

insurance, loans, credit, and more.[18] Although this is illegal under the FCRA, it is unlikely the activity could be traced when it occurs from one's personal computer use. In fact, many of these Web sites specifically market the personal profiles that they sell for these exact purposes.

The focus on advertising from the NAI and DAA leaves out specialty consumer reporting agencies that do not use the information they gather for advertising, but instead sell the information they gather, and often suggest this information be used for investigative purposes. Some research has noted this discrepancy; a team of Princeton researchers currently working on a white paper evaluating self-regulatory measures from the NAI and DAA advocate for use of the term "Consumer Tracking and Profiling", instead of "Online Behavioral Advertising."[19] This recognizes that regulatory efforts aimed solely at advertising ignore other uses of tracking, including one that raises concerns about legal violations. If the NAI and DAA simply regulate advertising, then there is a gap in regulation for when that information is used to create profiles for other purposes. I will discuss this further in Chapter 6.

---

[18] Center for Democracy and Technology, "Complaint and Request for Investigation, Injunction, and Other Relief," *Center for Democracy and Technology*, 30 June 2010, <https://www.cdt.org/files/pdfs/Spokeo.pdf>.

[19] Keyna Chow, Nicholas Petersen & Chris Jay Hoofnagle, "An Evaluation of Self-Regulation of Consumer Tracking and Profiling: Deficiencies and Recommendations for Improvement," *Submission to W3C Workshop on Web Tracking and User Privacy* (March 2011), <http://www.w3.org/2011/track-privacy/papers/Hoofnagle.pdf>.

Chapter 3: Do Not Track and the Consumer Privacy Bill of Rights

There have been regulatory efforts beyond those from the NAI and the DAA. In 2007, Pan Dixon of the World Privacy Forum began campaigning for a Do Not Track law. Dixon explained that the FTC should compile a list of third-party advertisers that consumers could opt out of—similar to a Do Not Call list. However, this initiative remained at a standstill until 2010.[20]

In 2010, the proposition resurfaced when the FTC recommended a Do Not Track (DNT) mechanism in a preliminary report entitled *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*.[21] In 2011, the World Wide Web Consortium (W3C) formed a Tracking Protection Working Group, made up of industry members, privacy advocates and academic experts, to form standards for a universal Do Not Track request tool. However, the W3C does not have enforcement power, so even if the creation of standards is successful, the standards could end up as only symbolic.[22]

Today, most browsers have a Do Not Track list of third-party advertisers that users can subscribe to, as well as a Do Not Track feature that allows users to request that Web sites do not track them. However, Web sites were not required to comply---that is

---

[20] David P. Baron, *Business and its Environment*, 6th ed. (Upper Saddle River, NJ: Pearson Education, 2010), 25.

[21] Federal Trade Commission, *FTC Staff Issues Privacy Report, Offers Framework for Consumers, Businesses, and Policymakers*," 1 December 2010, <http://www.ftc.gov/opa/2010/12/privacyreport.shtm>.

[22] World Wide Web Consortium, *Tracking Protection Working Group*, <http://www.w3.org/2011/tracking-protection/>.

until the DAA announced in February 2012 that all DAA members (about 80 in total) would begin honoring Do Not Track requests from users.[23] Now any DAA member that does not comply will be subject to FTC penalties.

This announcement came the same day as the release of a Consumer Privacy Bill of Rights from the White House and the Department of Commerce. In the Consumer Privacy Bill of Rights, the Administration lists seven rights of online privacy: individual control over data; transparency of privacy practices; respect for context of data use; security of data; access to and accuracy of data; focused collection of data; and accountability of the aforementioned rights. The Administration also states that they will work with Congress to craft privacy legislation and to grant the FTC with enforcement authority. The document also promises open, transparent forums where industry members and consumer advocates can work together to create a reasonable code of conduct that will lead to privacy standards that consumers can easily use and understand. Finally, the Administration plans to work with other countries to encourage global data protection.[24]

There has been little research to date about the recent regulatory efforts aimed at consumer tracking. However, there have been a few papers published about Do Not Track standards. Aleecia M. McDonald and Jon M. Peha looked at user expectations for a

---

[23] Karan Chopra, "Google and the Digital Advertising Alliance Will Support 'Do Not Track,' Agreed On Not To Collect Data About Users," *i2mag*, 23 February 2012, <http://i2mag.com/google-and-the-digital-advertising-alliance-will-support-do-not-track-agreed-on-not-to-collect-data-about-users/>.

[24] The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*," February 2012, <http://www.whitehouse.gov/sites/default/files/privacy-final.pdf>.

Do Not Track tool through a survey of 304 individuals on the crowdsourcing platform Amazon Mechanical Turk. They found that 79 percent of their survey participants expected DNT to limit data collection, and 39 percent expected no data collection at all. About two-thirds of participants expected DNT would stop behavioral profiling, but 40 percent said that they would not be surprised if a DNT tool did not do anything. There is still disagreement among policymakers and stakeholders about what a DNT tool will accomplish, and there are gaps between the expectations of the public and the plans from the W3C and the FTC.[25] This poses difficulties for the process of creating a standard DNT tool. Users need to have trust that this tool is meeting their expectations, or they may avoid Web sites and ads altogether, which will be detrimental to the online economy.

It seems that the DAA has in fact attempted to move past advertising regulation to online tracking regulation as a whole. In November 2011, the association released "Self-Regulatory Principles for Multi-Site Data." These principles include prohibition of the use of third-party Web tracking data for adverse terms or ineligibility for employment, credit, medical treatment, and insurance.[26] However, as Mayer points out, the principles do not prohibit offering favorable terms or determining eligibility from third-party Web

---

[25] Aleecia McDonald & Jon M. Peha, "Track Gap: Policy Implicationsof User Expectations for the 'Do Not Track' Internet Privacy Feature," *Social Science Research Network* (September 2011), <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1993133>.

[26] Digital Advertising Alliance, *Self-Regulatory Principles for Multi-Site Data*, November 2011, <http://www.aboutads.info/resource/download/Multi-Site-Data-Principles.pdf>.

tracking data.[27] Furthermore, regulation regarding the *use* of information from a Web site, as opposed to tracking itself, is difficult to enforce. As I will demonstrate in Chapter 6, the full implementation of these principles has not yet been successful.

[27] Jonathan Mayer, "A Brief Overview of the Supplementary DAA Principles," *The Center for Internet and Society*, 8 November 2011, <http://cyberlaw.stanford.edu/node/6755>.

Chapter 4: The FTC Proposal

In March 2012, the FTC released their final report on online privacy, entitled *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers.* This is an update of their December 2010 preliminary report. The final report calls on Congress to consider enacting privacy legislation and data security legislation. The Commission offers to work with Congress and the DAA to develop standards for behavioral tracking.[28]

The Commission includes three specific updates from the previous report. First, they write that the framework will only apply to businesses that serve 5,000 or more customers per year, so as to avoid unnecessary burdens on small businesses. Businesses that serve fewer than 5,000 customers per year are exempt, provided they do not share data with third parties. Second, companies will not need to provide consumers with a choice when collecting and using their data for practices that are consistent with the context of the transaction, consistent with the company's relationship with the consumer, or as required or specifically authorized by law.

Third, and central to the focus of this report, the Commission recommends that Congress consider enacting legislation to provide greater transparency for, and control over, the practices of information brokers. The framework recommends that companies

---

28 The Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*, March 2012, <http://www.ftc.gov/os/2012/03/120326privacyreport.pdf>.

provide consumers with access to the data that companies maintain about them, proportionate to the sensitivity of the data and the nature of its use. Since the last report, by the FTC's own account, they have done little to address online tracking, besides online protection for children.[29] The one initiative mentioned was that the Commission wrote letters to marketers of six mobile applications in February 2012 to warn them about Fair Credit Reporting Act violations.[30] However, in the report, they still refer to this as an "Online Behavioral Advertising" problem, even though these data are used for problematic purposes beyond advertising, i.e. aggregation and sale by the previously mentioned specialty consumer reporting agencies.

The FTC's framework consists of five action items; implementing a Do Not Track tool, improving privacy disclosures on mobile applications, creating legislation to provide consumers with access to information about them held by a data broker, exploring privacy concerns regarding large platform providers, and promoting enforceable self-regulatory codes. For the portion about data brokers, the report suggests that a centralized Web site be created where data brokers (1) identify themselves to consumers and describe how they collect and use consumer data and (2) detail the access rights and other choices they provide with respect to the consumer data they maintain.

---

[29] Ibid., iii.

[30] "FTC Warns Marketers That Mobile Apps May Violate Fair Credit Reporting Act: Agency Sends Letter to Marketers of Six Apps for Background Screening," The Federal Trade Commission, 7 February 2012, <http://www.ftc.gov/opa/2012/02/mobileapps.shtm>.

However, the paper again states that only data used for marketing purposes needs to be compiled. Creating a Web site like this for specialty consumer reporting agencies could allow for greater oversight over the legal concerns of these Web sites, and also bring awareness to users about their options. However, the framework makes no mention of these Web sites in their recommendations. As demonstrated in Chapter 6, many of these Web sites violate their privacy policies and do not give users the option to control or remove their data. As demonstrated in Chapter 5, this falls into the realm of FTC regulation of deceptive practices. The tools suggested in *Protecting Consumer Privacy in an Era of Rapid Change* could apply to these data broker Web sites in order to assist the FTC with their regulatory enforcement.

Chapter 5: Privacy Policies

Web Finance Inc. defines a privacy policy as a "Statement that declares a firm's or Web site's policy on collecting and releasing information about a visitor. It usually declares what specific information is collected and whether it is kept confidential or shared with or sold to other firms, researchers or sellers."[31] In considering the FTC report, it is important to note that the FTC's role is to prevent business practices that are either "unfair" or "deceptive" under 15 U.S.C. § 45 (Title 15, Section 45 of the *United States Code*). The FTC also has soft power to threaten enforcement, propose legislation, or publicly call on businesses to improve their practices. Since Web tracking standards are so ill-defined at this time, the FTC has not placed prohibitory consequences on Web sites that violate their privacy policies. The FTC does consider privacy policy violations to be a deceptive practice, but they typically respond to violations by issuing consent orders and requiring a small payment, if any.[32]

A potential consequence of this framework is that companies will simply offer less protection in their privacy policies. As Erica Newland from the Center for Democracy and Technology writes in her critique of the FTC report:

> The Commission's focus on 'public commitments' will do little to change an incentive structure that has long encouraged companies to be evasive and vague in

31 "Privacy Policy," Web Finance Inc., <http://www.businessdictionary.com/definition/privacy-policy.html>.

32 Jonathan R. Mayer & John C. Mitchell, "Third-Party Web Tracking: Policy and Technology," *The Center for Internet and Society* (March 2012), <http://cyberlaw.stanford.edu/publications/third-party-web-tracking-policy-and-technology>.

> their notices to users. Companies are most likely to get called out for violating explicit promises to users, so many realize that the less they promise, the less trouble they court. It's not a paradigm that gives consumers much useful information about the privacy practices of the products and services they use.[33]

Most stakeholders agree that more consumer outreach and education about online privacy is needed. Web sites are faced with the challenge of developing a privacy policy that is simple, but also thorough in its promises to users. In February 2012, Google consolidated privacy policies for over 60 of their services into one simple, easier-to-understand policy, explaining that this consolidation was a response to the FTC's request for clearer policies. In response, the media and the public expressed that this change was compromising user privacy too much, and eight members of Congress wrote a letter in complaint. Google responded with a blog post stating that reports and complaints about the change were not based on accurate information. They clarified user rights that were not going to change, including privacy tools for personal data management, and the fact that Google would not sell personal data.[34] This demonstrates the potential for confusion about Web site privacy policies.

Previous research has shown that privacy policies are so complex and densely written that it is unreasonable to expect typical users to read the policy for each Web site they visit. Other research examined the Platform for Privacy Preferences (P3P), a self-

---

[33] Erica Newland, "FTC Once Again Says Privacy Self-Regulation Isn't Enough," *Center for Democracy and Technology*, 27 March 2012, <https://www.cdt.org/blogs/erica-newland/2703ftc-once-again-says-privacy-self-regulation-insufficient>

[34] "Changing our privacy policies, not our privacy controls," *Google Public Policy Blog*, 31 January 2012, <http://googlepublicpolicy.blogspot.com/2012/01/changing-our-privacy-policies-not-our.html>.

regulatory mechanism for Web sites to communicate their privacy policies to user agents so that users do not have to read them. They found that thousands of Web sites were using P3P compact policies to misrepresent their policies.[35] Going forward, it is clear that adequate and comprehendible content in privacy policies will continue to be a struggle for Web companies, regulators, and consumers.

[35] Komanduri 3.

Chapter 6: Specialty Consumer Reporting Agencies

The 1970 Fair Credit Reporting Act (FCRA), under 15 U.S.C. § 1681, regulates credit reporting agencies. There are three credit reporting agencies in the United States--Experian, TransUnion, and Equifax. Under the law, consumers have the right to be told what information the credit organizations have about them, the right to be told if their information has been used against them, the right to ask for a credit score, the right to dispute incomplete or inaccurate information, and the right to have the organization delete inaccurate, incomplete, unverified, or outdated information.[36]

Another lesser-known role of the FCRA is its regulation of specialty consumer reporting agencies, as described in section 603(w) of the law. As described by the FCRA, these are agencies that collect information about individuals from a variety of sources and compile reports for the purposes of selling those data to third parties.[37] The estimated number of these agencies in existence varies from a few dozen[38] to over 180, as listed by Privacy Rights Clearinghouse.[39]

---

36 The Federal Trade Commission, *A Summary of Your Rights Under the Fair Credit Reporting Act*, <http://www.ftc.gov/bcp/edu/pubs/consumer/credit/cre35.pdf>.

37 Center for Democracy and Technology, 17.

38 "Do a Total Background Check on Yourself -- Annual Consumer Reporting Agencies," *Annual Medical Report*, 27 March 2010, <http://www.annualmedicalreport.com/do-a-total-background-check-on-yourself-annual-consumer-reporting-agency/>.

39 "Online Data Vendors: How Consumers Can Opt Out of Directory Services and Other Information Brokers," *Privacy Rights Clearinghouse*, February 2011, <https://www.privacyrights.org/online-information-brokers-list>.

A 2011 paper by researchers from Worchester Polytechnic Institute and AT&T Labs-Research examined the top 120 Web sites, using rankings from Alexa.com, and excluding social networking sites. They found that 56 percent trade or sell private information, which increases to 75 percent when they include user IDs. A few examples of the information that these Web sites most frequently relinquished include searches on healthcare sites, travel itineraries on flight booking sites, age, gender, and ZIP code.[40] While this research does not report on the use of this information, the information itself could certainly be used for more than just advertising purposes. It creates the potential for serious violations of personal privacy and information security, and for the use of discriminatory practices based on this information.

Specialty consumer reporting agency Web sites function solely as data aggregators and sellers of personal information. This information can include name, phone numbers, addresses, occupations, names of affiliated people, religion, ethnicity, gender, political affiliation, financial wellbeing, and criminal record, among other personal data. Studies have shown that the information these Web sites report is not always accurate. Furthermore, correcting it can be difficult if not impossible, and usually requires payment. Usually, users can request that their information be taken off a

40 Balachander Krishnamurthy, Konstantin Naryshkin, & Craig E. Wills, "Privacy leakage vs. Protection measures: the growing disconnect," *Web 2.0 Security and Privacy Workshop* (May 2011), <http://web.cs.wpi.edu/~cew/papers/w2sp11.pdf>.

particularly site, but that process can also be difficult, and the companies are able to create a new profile for that consumer in the future.[41]

In January 2012, researchers at Fox News conducted an experiment with Spokeo, one of the largest specialty consumer reporting agencies. They asked 15 people to search for themselves on Spokeo.com. Ten of the 15 reported inaccuracies in their information. Of those, three said the information was mostly inaccurate, while others noted only minor discrepancies, such as an incorrect address or the wrong number of people in their household. There is no way to correct one's information on Spokeo.com, but users tried to follow the opt-out instructions to block their names from searches. However, this was unsuccessful.[42] A CBS affiliate in New York conducted a similar study with their staff and found errors in important information in the majority of the profiles. The staff of the nonprofit organization Center for Democracy and Technology conducted the same tests and found errors in important information in every profile.[43] On all specialty consumer reporting agency Web sites, purchasers of profiles have no way of telling if there are inaccuracies in the personal information, and users face difficulty in changing inaccurate information.

---

41 Anita Ramasastry, "Can We Stop Zabasearch--and Similar Personal Information Search Engines?: When Data Democratization Verges on Privacy Invasion," *FindLaw*, 12 May 2005, <http://writ.news.findlaw.com/ramasastry/20050512.html>.

42 John Brandon, "Spokeo a Growing Threat to Internet Privacy, Cyber Security Experts Warn," *Fox News*, 19 January 2011, <http://www.foxnews.com/scitech/2011/01/19/spokeo-cyber-security-warn-threat-privacy/>.

43 Center for Democracy and Technology, 11-12.

I looked at 29 Web sites that fit into the category of specialty consumer reporting agencies and analyzed their privacy policies (see Appendices). For the table in Appendix A, I examined the cost of personal profiles and the listed sources of information about individuals. Most Web sites had multiple tiers of profiles that could be purchased, with more information given for a higher cost. Examples of some of the categories of information include Credit Score, Wealth Level, Mortgage Value, Relationship Status, Lifestyle and Interests, Occupation, Political Affiliation, Ethnicity, Residence, Family Members, and Criminal Record. For the table in Appendix B, I examined the language of the legal disclaimers explaining the prohibited uses of the information under the FCRA. I also looked at the language of the instructions on how to change one's information or opt out of the Web site completely.

I found that eight of the 29 Web sites did not have legal disclaimers explaining FCRA restrictions on their Web sites at all. Seven of the 29 Web sites had FCRA disclaimers, but claimed on their Web site to be a service specifically for FCRA-prohibited decisions, such as those related to employment, housing, or insurance. Three of the 29 Web sites have an FCRA disclaimer, but, when one enters a search query, the site redirects to PeopleFinders.com. PeopleFinders.com markets itself as a Web site for employers, which violates FCRA regulations, and contradicts the FRCA disclaimers of the original Web sites.

The Web sites that did have disclaimers ranged in comprehensiveness. Some explained that it is illegal to use the information to make decisions about credit, employment, insurance, loans, housing, scholarships, etc., based on FCRA restrictions. However, others were more vague, including the following;

- "You agree to use the Services only for purposes that are permitted by any applicable law, regulation, or generally accepted practices or guidelines."
- "By placing an order for services with us, you confirm that: you are ordering information about yourself, not about anyone else."
- "Crimcheck.com is FCRA Certified by CDIA."
- "You should consult state and federal laws before using this information in making decisions on hiring or firing of employees."

Other Web sites explicitly promoted FCRA violations, including the following;

- "We provide Fair Credit Reporting Act compliant, multilayer, in-person/real-time reports that include criminal record checks, permissible-purpose credit reporting and driving records. These services […] can help you reduce employee turnover and shrinkage, decrease training costs and increase productivity.
- While EasyBackgroundChecks.com attempts to provide a quality product, these instant checks may not comply with local, state or federal employment laws such as the Fair Credit Reporting Act.

Furthermore, many of the Web sites listed only few sources of their information, and often used undescribed terms including "partners, affiliates, and third-parties" and "cookies." Seven Web sites listed no sources at all. Two Web sites gave instructions for how to change one's information, although one required payment to do so. Twelve offered instructions for users to remove their information from the Web site. Some of these Web sites required personal information to do so, such as a copy of a driver's

license or ID card. Two Web sites warned that even with successful deletion of a personal profile, it could reappear on their Web site at a later time. Fourteen Web sites did not list instructions for opting out of the Web site or disputing personal information.

Chapter 7: Interoperability and the European Union

One of the recommendations in the Consumer Privacy Bill of Rights is global operability. Based on comments received after the previous draft, they conclude:

> Consistency between different privacy regimes reduces companies' costs, promotes international competitiveness, and increases compliance with privacy standards. Such interoperability is better for consumers, whose data will be subject to more consistent protection wherever it travels, and more efficient for businesses by reducing the burdens of compliance with differing, and sometimes conflicting rules.[44]

The report explains that as a result, the U.S. framework is consistent with the nine privacy principles in the 2004 Asia-Pacific Economic Cooperation (APEC) Privacy Framework, which intends to create cross-border privacy rules to facilitate data transfers among the 21 APEC members. The Consumer Privacy Bill of Rights also recognizes the 2011 reissuing of the Organization for Economic Cooperation and Development Privacy Guidelines, which had not be altered since their release in 1980. The report recommends that Congress and the FTC keep these initiatives a focus of their regulatory efforts going forward.[45]

One timely example of how the United States is affected by privacy laws abroad is the European Union (EU). For years, policymakers in Europe have debated the interpretation of existing regulations and the need for different regulations, resulting in many evolutions of the law. There are two legal frameworks for online tracking in

---

[44] The White House, 31.

[45] Ibid.

Europe. The first is the European Data Protection Directive, which regulates the collection, processing, storage, and transfer of personal data. It sets forth basic principles for both online and offline data collection and use, including notice, consent, proportionality, purpose limitation, and retention periods. The second is the European e-Privacy Directive, which regulates data privacy on communication networks, and includes protections for confidentiality of communications, spam, traffic and location data, and the use of cookies.[46]

Over a series of amendments to the e-Privacy Directive, the standards for tracking have developed. Policymakers updated the original 1995 Privacy Directive in 2002 to include electronic communications. The 2002 version included an opt-out rule that allowed users to refuse cookies after they had been delivered. This also required Web sites to include instructions for disabling or rejecting cookies in their privacy policies. The opt-out rule was changed in 2009 to an opt-in rule, meaning that users needed to give consent in order to receive a cookie. However, Web sites send dozens of cookies to users during each Web site visit, so instead of users giving consent for each individual cookie, users can opt in once through their browser settings.[47]

In June 2012, the Article 29 Working Party, the group of European privacy regulators charged with interpreting and enforcing the law, reevaluated this interpretation

---

46 Omar Tene and Jules Polonetsky, "To Track or 'Do Not Track': Advancing Transparency and Individual Control in Online Behavioral Advertising," *Social Science Research Network*, 31 August 2011, 19, <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1920505>.

47 Ibid, 20-21.

of opting in through browser settings. They concluded that in order for user consent through browser settings to be sufficient, consent must occur periodically, users should be able to easily revoke their consent, and all browsers should have a default setting of rejecting cookies. The United Kingdom government responded to these conclusions by rejecting the use of browser settings as a form of consent.[48]

In February 2012, the European Commission proposed a new set of revisions to the EU data protection law. Recommendations include giving people easier access to their personal data, enabling users to delete data if there are no legitimate grounds for retaining them, and increasing penalties for violations to up to two percent of revenue. The document developed their consent regulations based on the Article 29 Working Party feedback.[49] However, EU directives are not laws, but frameworks for each member state to develop into internal laws.[50]

These developments are significant to the United States due to the US-EU Safe Harbor Privacy Principles, which were part of the original 1995 Privacy Directive, and continue to exist in the latest version. The Safe Harbor prohibits the transfer of personal data to non-European countries that do not meet the EU standards for privacy protection.

---

[48] Ibid, 22.

[49] "Commission proposes a comprehensive reform of data protection rules to increase users'' control of their data and to cut cots for businesses," *Europa*, 25 January 2012, <http://europa.eu/rapid/pressReleasesAction.do?reference=IP/12/46>.

[50] Christine Fretten and Vaughne Miller, "The European Union: a guide to terminology, procedures and sources," *United Kingdom House of Commons Library*, 21 July 2005, 8, <http://www.w4mp.org/html/library/standardnotes/snia-03689.pdf>.

This applies to all member states. Companies in the U.S. have the option to comply if they wish to be active in the EU market and offer their services to EU citizens. The standards with which Web sites must comply include providing users the following: notification about the uses of the data they collect, the ability to opt out of having their personal information disclosed, the ability to opt in to having sensitive data shared for a purpose other than the original stated purpose, and the ability to access the information held about them.[51] The Web sites in the U.S. that are not complying with these standards do not get to participate in the online economy of Europe, which is detrimental to the U.S. as a whole.

51 "U.S.-EU Safe Harbor Overview," *Export.gov*, 26 April 2012, <http://export.gov/safeharbor/eu/eg_main_018476.asp>.

Chapter 8: Conclusion

Despite a lack of success with self-regulatory initiatives, it appears that the NAI and the DAA have attempted to respond to online privacy concerns. The DAA Transparency Principle requires that companies "give clear, meaningful, and prominent notice on their own Web sites that describe their Online Behavioral Advertising data collection and use practices." According to the principles, companies must disclose the type of data they collect, the use of those data, how long they are retained, offer users the ability to dispute information, and offer users the ability to opt out of having their information included on the Web site.[52] However, this information is limited to data used for targeted advertising. It does not cover tracking for other purposes.

The U.S. Congress passed the FCRA in 1970 as a response to a pattern of abuse and misinformation by the consumer reporting industry. In addition to highly inaccurate reports, Congress was concerned that data brokers were reporting conclusions about consumers' lifestyle. Congress concluded four points;

- Inaccurate credit reports directly impair the efficiency of the banking system, and unfair credit reporting methods undermine the public confidence which is essential to the continued functioning of the banking system.

---

[52] Komanduri 5.

- An elaborate mechanism has been developed for investigating and evaluating credit worthiness, credit standing, credit capacity, character, and general reputation of consumers.
- Consumer reporting agencies have assumed a vital role in assembling and evaluating consumer credit and other information on consumers.
- There is a need to insure that consumer reporting agencies exercise their grave responsibilities with fairness, impartiality, and a respect for the consumer's right to privacy.[53]

The FCRA was the response from Congress to ensure that protection, fairness, and integrity would remain in place. The World Wide Web has made these goals more difficult to achieve. Information is easier to access. It is impossible for individuals to know what data each Web site has about them and the details of their respective privacy practices. It is difficult to detect when online data about an individual are used for discriminatory practices. Information is less secure, and the potential for fraud, identity theft, and other security threats is high. The FCRA regulations cannot be ignored.

Many specialty consumer reporting agencies are directly violating the FCRA by promoting their services for the use of decisions about employment, insurance, credit, and loans. Those Web sites that do warn of FCRA violations have no way of knowing how the information they sell is being used, so the regulations cannot be enforced.

---

[53] Center for Democracy and Technology, 15-16.

Furthermore, changing or removing one's information from these Web sites is usually difficult, if not impossible, even if the information is inaccurate.

The FTC has a responsibility to step in to prevent deceptive practices and to ensure the safety of the online marketplace. As set forth by the FCRA, users need free access to their information, the ability to get inaccurate or irrelevant information removed, and the ability to opt out of a having profile. To increase consumer awareness, the FTC can implement their proposal of a centralized Web site where data brokers identify themselves, their data collection and use, and options available to users. However, they should begin with a centralized Web site specifically for specialty consumer reporting agencies.

The FTC must improve their efforts to uncover and penalize violations of privacy policies. Researchers are working on solutions to improve understanding of privacy policies. In fact, researchers at Carnegie Mellon and Rutgers University have launched an app that allows users to see simple interpretations of privacy policies that have been crowsourced to workers on Amazon Mechanical Turk.[54] While previously mentioned research has concluded the difficulty of this, there is a responsibility on the users to understand the privacy policies of the Web sites they visit, as they are essentially entering into a contract with the Web site with each visit. However, it is the responsibility of the FTC to prevent deceptive and unfair practices, of which privacy policy violations are one.

---

[54] David Talbot, "Using Crowdsourcing to Protect Your Privacy," *Technology Review*, 3 April 2012, <http://www.technologyreview.com/communications/40036/page1/>.

It is deceptive to consumers when specialty consumer reporting agencies do not explicitly state Fair Credit Reporting Act violations on their Web site. It is also deceptive for these Web sites to include unclear or false information about the source of the data they aggregate and the data management options for the user.

Self-regulatory efforts from the DAA and NAI have largely failed, and their efforts have focused almost entirely on advertising. The DAA and the NAI can expand their privacy protection efforts to include specialty consumer reporting agencies, or these data brokers could create their own industry representative. However, considering the patterns of DAA and NAI efforts, policymakers should stay involved and work with these representatives to create laws that clarify individual online privacy rights and ensure the enforcement of existing laws. Lastly, as demonstrated by the differences in the EU online privacy laws and the Safe Harbor Privacy Principles, the formation of U.S. policies will be important for U.S. involvement in the international online marketplace going forward.

Appendices

APPENDIX A: COST OF USER PROFILES AND LISTED SOURCES OF USER INFORMATION

The following table shows information taken directly from each Web site about the cost of purchasing an individual profile and the sources of the information used in individual profile.

Web site	Cost to order record	Listed sources of their information about users
Intelius.com	$4.99 for phone check, $50 for full record report	Intelius provides online access to public records such as real estate deeds, lawsuit filings, liens, professional licensing records, and other information filed by individuals and businesses with local, state and federal agencies. Intelius is not a consumer credit reporting agency, and we do not compile mailing lists or consumer marketing data. Additionally, we do not maintain any databases of non-public individual financial data, such as individual credit reports, tax records, employment information or bank information. Intelius also does not have any individual's medical records, and Intelius does not collect or distribute any information about your race, religious preference, medical history, lifestyle, political preference or friends to any customers. Finally, although Intelius does offer access to "white pages" telephone directories, your telephone number is not available in these databases if you have a non-published telephone number. All of the information contained in our databases is available from many other sources, such as the public records custodians and private data compilers. For example, home addresses are available from county land records, tax assessor files, and telephone directories. Additionally, many companies retrieve and publish public records, and many government agencies and private information vendors now make their records available electronically and over the Internet. Public Records are compiled by various public offices and agencies with the intent and for the purpose of being made publicly available. Examples of public records include real estate records, lien filings, business entity filings (such as corporate registrations), lawsuit information and court dockets, court decisions, and birth, marriage, divorce and death records. Publicly Available Information generally originates with the individual himself or herself and is provided in the course of routine business transactions, such as ordering telephone service, placing catalog orders, making retail purchases, and joining book clubs. Published telephone numbers, household demographics, street addresses, and church and school alumni directory information all fall within the category of publicly available information. Information contained in newspapers and magazines (such as news reports and birth, death and marriage notices) is also considered to be publicly available.

Acxiom.com	$5 for your own info	The data in Acxiom's marketing products comes from several different types of sources including public records, publicly available data and nonpublic sources where the consumer has been provided notice of how their data will be used, and offered a choice as to whether to allow those uses. The data includes public record and publicly available data from such sources as telephone directories, website directories and postings, real property recorder and assessor files, and government licenses. Data from other providers includes demographic data, surveys and questionnaires, and summarized or aggregated purchase data.
MyLife.com	Must buy monthly plan, min one month $17.95 w/ autorenewal	In addition to tens of millions of Member Profiles, MyLife also has a database of public domain information about more than 200 million adults in the United States, which visitors and members can search. A Public Profile is one that has been created by us using public-domain information, which we have licensed from third party sources (for display and resale on the internet). People can search on MyLife.com by various parameters for people from their past. If people search for you on the internet, for example at a search engine such as Google or Yahoo, the search results delivered by the third party search engine may include links to your public profile at MyLife.com. If you are a Member, they will see your Member Profile as well. Your Member Profile may also include additional public domain information, which MyLife.com will make available to you to add to your existing Member Profile.
ZabaSearch.com	Free but reports produced by Intelius.com where you have to pay	Online data aggregator, doesn't list sources--Public records are available from the official public records custodian or repository to anyone who requests them. In order for any database of public records to be useful, the databases must contain all of the information in the public records offices. Our data files must accurately reflect the underlying public records, and we do not remove or suppress any information that is both accurate and publicly available. There are exceptions to this rule, as a courtesy we allow law enforcement, certain government officials or employees, and individuals with court protection orders the option to opt out their information.

center.Spoke.com	Spoke is free but Reports are actually USSearch.com	Spoke offers an online directory that is available at http://center.spoke.com ("the Spoke Directory"). The Spoke Directory contains information about businesses and business contacts that is collected, aggregated and assembled from various sources, including: * Publicly available information: Information that is available to the general public, including via the Internet. * Published information: Information that has been privately collected by an entity other than Spoke, which is then made available for redistribution by that entity. * Contributed information: Information contributed by registered or unregistered users of the Spoke Services, including names, titles, and company affiliations of individuals.
BeenVerified.com	$19.95	All of the information we share at BeenVerified is public record and comes from numerous sources of publicly available information, opt-in databases, and vendors. After aggregating these massive amounts of public information, we apply our proprietary technology that gives you the ability to perform instant searches, all within an easy to use application.
PeekYou.com	Free but reports like to other sites	Search engine aggregator: PeekYou can find only what Google, Bing, and Yahoo are also able to find. If these traditional search engines cannot find a piece of information, then PeekYou cannot either. But whereas traditional search engines might bury certain kind of personal information as not relevant to a search, PeekYou cleans it up, organizes it, and presents it in useful form.
USSearch.com	$19.95 when you purchase another search -- "Self Background Check (Click here for details) Great Savings! Get a search credit to run an Advanced Background report on yourself. This offer is only available with a purchase."	Advanced Background reports provide details pulled from US Search's entire network of public record databases. The information includes, when available: current address and history; aliases; phone numbers; relatives, neighbors and associates; bankruptcies and tax liens; small claims civil judgments; property ownership; home value; marriage and divorce records; and a state criminal search.(from report itself)…. Also elsewhere this...In addition to public records, personal information may be publicly or commercially available. Publicly available information consists of online and offline information that is generally available but is not maintained by a government agency, such as names, addresses and telephone numbers of individuals and businesses, professional licensing and trade organization information, press releases and newspaper articles and content from blogs or social networking sites. Commercial records consist of information that is maintained by enterprises and is available for purchase, such as marketing and telemarketing lists, phone connect and disconnect information, and business profile data.

PeopleFinders.com	$0.95 for people search report, 14.95 for monthly membership, $39.95 for background report	Info provided to website, widgets, partners/affiliates/third parties, info collected from browser, cookies, pixel tags
PeopleLookup.com	On- time $1.49, 24-hour pas $9.95, background check $54.95	Throughout the page, they mention that information can be collected by an individual sharing it while using the website; through cookies; through information aggregated from online ads; through public records; through publicly available information like online and offline information that is generally available but is not maintained by a government agency, such as names, addresses and telephone numbers of individuals and businesses, professional licensing and trade organization information, press releases and newspaper articles and content from blogs or social networking sites; through commercial records that is maintained by enterprises and is available for purchase, like marketing and telemarketing lists, phone connect and disconnect information, and business profile data.
PeopleSmart.com	Contact report $1.95, background report $39.95	We collect Personal Information about you when you voluntarily register with us, when you use the Website and/or our products or services and your browser interacts with us, when you visit the Website pages or the pages of certain of our partners, and when you enter third party Personal Information to conduct certain searches. We may combine information that we have about you with information we obtain from business partners or other companies, such as data providers and billing companies. We automatically receive and record information on our server logs from your browser, including your IP address, our cookie information, search activity, and the pages you request. We may collect, create, use and disclose, in our discretion, any data that does not permit the identification of an individual (e.g., aggregated data or data in which we exclude information, such as your name, email, and address, that makes the data personally identifiable to you).
PrivateEye.com	Links to PeopleFinders.com. All info the same.	Website use, cookies, aggregated info from public records
WhitePages.com	Links to PeopleSmart.com	**None listed**

USA-People-Search.com	"People records" $0.95, Premium membership (24 hours $14.95, 7 days $19.95, 30 days $39.95), Extreme background check ($29.95 + $10 for business ownership and $10 for criminal records)	**None listed**
Spokeo.com	$4.95/month autorenew min three months	Spokeo is a search engine specialized in aggregating people-related information from phone books, social networks, marketing lists, business sites, and other public sources. Unfortunately, we do not have information to the specific sources we pull data from, as there are more than 50 of them. We apologize, and will alert Spokeo users if a source-revealing feature becomes available.
PublicRecordsNow.com	Links to PeopleFinders.com. All info the same.	**None listed**
DOBSearch.com	People Finder Report $3.99, 24-hour pass $8.99	Info from website use, info from browser, cookies, public records or publicly available information, proprietary database repositories, or governmental databases from the municipal, county, State or Federal levels
Radaris.com	Links to PeopleFinders.com. All info the same.	**None listed**
efindoutthetruth.com	Basic background check $10, Extensive background check $45	**None listed**

identitypi.com	Complete background check $34.95, National Criminal Search $15.99, People Search $9.99, National Sex Offender $5.99, Tenant Screening $24.95	
backgroundpi.com	$34.95	Website use, cookies, ClickTale (mouse clicks) analytics
easybackgroundchecks.com	Instant Database Background Check $17.95, Investigator Assisted Background Check $79.95	**None listed**
crimcheck.com	$79.95 for your own report, no price listed for business use until you register	Brower info, cookies, website use
knowx.com	$24.95	Public records
backgroundchecks.com	National Criminal Background Check $39.95, National Criminal Report with Annual Monitor $73.35, National Criminal Report with one-month monitor $44.90, all have $9.95 fee for emailing report to you	Cookies, website use

publicbackgroundchecks.com	People Records $1.95, 24 hour People Search Membership $14.95, Background Report $39.95	Information provided by you. We may collect, sell, or share any personal information you enter on our web site or provide to us in some other manner, including through e-mail marketing by us, and our partners and affiliates. This includes identifying information, such as your name, address, e-mail address, and telephone number, and, if you transact business with us, financial information such as your payment method (valid credit card number, type, expiration date or other financial information). (Please see "How we protect your personal information", below); **Information provided by third party sources.** Periodically we may acquire - from partners, affiliates or other third parties - personal and/or non-personal information about you. We add it to other information we have collected.; Cookies; Website Use
iamscreened.com	"Silver Package" $49, "Gold Package" $89.95, "Platinum Package" $124.95	Website use; "We may also periodically obtain both personal and non-personal information about you from our partners and affiliates, and other third parties, and add it to our account information or other information we have collected"; cookies; pixel tags; online ads
BackgroundsOnline	**Not listed** without sign-up	Info from site use, cookies
PublicPeopleFinder.com	Basic results $39.99, Advanced Results $59.99	**None listed**

APPENDIX B: OPT-OUT INSTRUCTIONS AND FCRA LEGAL DISCLAIMERS

The following table shows information taken directly from each Web site. It includes the explanation of how users can opt out of having their information on the Web site, and the wording of their FCRA legal disclaimer, if any, about illegal users of the user profile information.

Web site	Opt-out/correction requirements	Disclaimer Language for FCRA
Intelius.com	As a courtesy we can 'opt out' your specific information from the Intelius People Search service. What this means is that your name as it appears in a particular record and the associated identifying information such as your address and phone number will be suppressed if you request this in the manner described below. However, please note that any time your identifying information appears in a public record in a manner which is different from the record you opted out, it will again appear in our system. (For example, if your address or area code changes your new information will again appear unless you opt out the new record.) There also are many other public records search services which are not owned by Intelius and your request that we opt out your information will not prevent your information from appearing on these other services. In order for Intelius to 'opt out' your public information from being viewable on the Intelius website, we need to verify your identity and require you to complete the online opt out request or send a faxed proof of identity. Proof of identity can be a state issued ID card or driver's license. If you are faxing a copy of your driver's license, we require that you cross out the photo and the driver's license number. We only need to see the name, address and date of birth. Please fax to 425-974-6194 and allow 4 to 6 weeks to process your request.	FCRA Restrictions. Intelius is not a consumer reporting agency as defined in the Fair Credit Reporting Act ("FCRA"), and the information in the Intelius databases has not been collected in whole or in part for the purpose of furnishing consumer reports, as defined in the FCRA. You shall not use any of our information as a factor in (1) establishing an individual's eligibility for personal credit or insurance or assessing risks associated with existing consumer credit obligations, (2) evaluating an individual for employment, promotion, reassignment or retention (including employment of household workers such as babysitters, cleaning personnel, nannies, contractors, and other individuals), or (3) any other personal business transaction with another individual (including, but not limited to, leasing an apartment).

Acxiom.com	Acxiom offers access to and correction of information in our directory products and fraud detection and prevention products. Access to information about you in our directory and fraud detection and prevention products will be provided in the form of a U.S. Reference Information Report that is available for a processing fee of $5. Below is a link to our U.S. Reference Information Report Request Form. You must separately mail your $5.00 personal check, made payable to Acxiom at the following address: Acxiom, Consumer Advocate, P.O. Box 2000, Conway, AR 72033 After you have submitted your U.S. Reference Information Report request and your check has been received and processed, your report will be sent to you. Acxiom will perform certain additional validation procedures to verify your identity and the authenticity of your request prior to generating your U.S. Reference Information Report.	We provide *Fair Credit Reporting Act* (*FCRA*)–compliant, multilayer, in-person/real-time reports that include criminal record checks, permissible-purpose credit reporting and driving records. These services—in combination with the other checks such as drug testing, education and professional license verifications—can help you reduce employee turnover and shrinkage, decrease training costs and increase productivity.

MyLife.com	To continue deleting your account, please call this toll-free number: **1-888-704-1900**	You shall not use the Service in any manner contrary to local, state, or federal law. For example, because MyLife is not a "Consumer Reporting Agency" as that term is defined in the federal Fair Credit Reporting Act (15 U.S.C. 1681, et seq.), information provided on the website do not constitute Consumer Reports. Accordingly, information found on the website may not be used in whole or in part as a factor in determining eligibility for credit, insurance, employment or another purpose in connection with which a consumer report may be used under the Fair Credit Reporting Act. You hereby certify that you will not use any of the information you receive through your subscription to determine, in whole or in part an individual's eligibility for any of the following products, services or transactions: (1) credit or insurance to be used primarily for personal, family or household purposes; (2) employment purposes; (3) a license or other benefit granted by a government agency; or (4) any other product, service or transaction in connection with which a consumer report may be used under the Fair Credit Reporting Act or any similar state statute, including without limitation apartment rental, check-cashing, or the opening of a deposit or transaction account.

ZabaSearch.com	ZabaSearch is a search engine like Google, and it scours various data sources for its results. Because ZabaSearch does not maintain a database of records, it is not possible to change the information it finds from various public records sources. Nor can ZabaSearch remove persons or information it finds because ZabaSearch has no control to add, modify or delete public information owned, operated and/or maintained by those sources. What ZabaSearch can offer is to create a filter that will block the information from appearing when someone runs a search. Please note this WILL NOT remove your information from the information sources. There may be multiple results for one individual due to the way the information was entered at the source. Even the slightest variation in a name, such as a period after a middle initial or a spelling of a street name, will result in a separate record.	Links to USSearch.com: The Service is intended for personal use only, and is not intended for commercial use. You will not use any information provided to you by US Search or its employees to determine an individual consumer's credit worthiness, eligibility for insurance, housing, any license or other benefit, employment screening any business transaction initiated by that person, or any other purpose covered by the Fair Credit Reporting Act, 15 U.S.C. sec. 1681 et seq., ("FCRA"), Federal Trade Commission interpretations of the FCRA, and similar state statutes. If you use the Service for any of the aforementioned reasons, you may be violating the law. Also: Like Google, ZabaSearch is a search engine, not a database and does not house, create or manage the information in the search results.
center.Spoke.com	**None listed**	Links to USSearch.com: The Service is intended for personal use only, and is not intended for commercial use. You will not use any information provided to you by US Search or its employees to determine an individual consumer's credit worthiness, eligibility for insurance, housing, any license or other benefit, employment screening any business transaction initiated by that person, or any other purpose covered by the Fair Credit Reporting Act, 15 U.S.C. sec. 1681 et seq., ("FCRA"), Federal Trade Commission interpretations of the FCRA, and similar state statutes. If you use the Service for any of the aforementioned reasons, you may be violating the law.

BeenVerified.com	Please send an email to support@beenverified.com and supply the following information.* Your name as shown on our site * Your Age * Current address (City, State, Zip) * Previous addresses * Listed Relatives. We send out a monthly update to our data providers.	We are not a credit reporting agency for purposes of the Fair Credit Reporting Act ("FCRA"). As such, the additional protections afforded to consumers, and obligations placed upon credit reporting agencies, are not contemplated by, nor contained within, these terms and conditions. You may not use any information obtained from BeenVerified™ including, without limitation, the BeenVerified™ Checks, in connection with determining a prospective candidate's suitability for: Health insurance or any other insurance, Credit and/or loans, Employment, Education, scholarships or fellowships, Housing or other accommodations, Benefits, privileges or services provided by any business establishment
PeekYou.com	Simple web form here http://www.peekyou.com/about/contact/optout/	You agree to use the Services only for purposes that are permitted by (a) the Terms and (b) any applicable law, regulation, or generally accepted practices or guidelines in the relevant jurisdictions. You understand that all information and Content is presented to you as is, and PeekYou makes no guarantees regarding quality, integrity or accuracy.
USSearch.com	http://www.ussearch.com/consumer/ala/landing.do?did=590	The Service is intended for personal use only, and is not intended for commercial use. You will not use any information provided to you by US Search or its employees to determine an individual consumer's credit worthiness, eligibility for insurance, housing, any license or other benefit, employment screening any business transaction initiated by that person, or any other purpose covered by the Fair Credit Reporting Act, 15 U.S.C. sec. 1681 et seq., ("FCRA"), Federal Trade Commission interpretations of the FCRA, and similar state statutes. If you use the Service for any of the aforementioned reasons, you may be violating the law.

PeopleFinders.com	Fill out and mail this form: http://www.peoplefinders.com/optout-form.pdf	A person is authorized to use information disclosed on this Site only to protect a person at risk. Except to protect a person at risk or as authorized under any other law, use of any information disclosed on this web site for purposes relating to any of the following is prohibited: Health insurance, Insurance, Loans, Credit, Employment, Education, scholarships, or fellowships, Housing or accommodations, Benefits, privileges, or services provided by any business establishment. **Source:** California Penal Code Section 290.46 (j) (1), (2); California Penal Code Section 290.46 (k) (2). You agree that you are only authorized to visit, view, and retain a copy of pages of this Site for your own personal use; except with the Company's written permission, you shall not duplicate, download, publish, modify, or otherwise distribute the material on this Site for any commercial use, or for any purpose other than as described in these Terms. You cannot automate, script, scrape, or otherwise take data from the Site in an automated fashion to re-use or display in any way. You acknowledge that we are not providing you with a consumer report, and you are certifying that you will not use information obtained from us for any purpose covered under the Fair Credit Reporting Act (15 U.S.C. §1681, et seq.). You acknowledge that the Company owns and retains all proprietary materials contained on the Site, including trademarks, content, and other proprietary content.

PeopleLookup.com	As a courtesy we allow you to opt out your personal information from our Website. What this means is that your name as it appears in a particular record and the associated identifying information such as your address and phone number will be suppressed if you request this in the manner described below. However, please note that any time your identifying information appears in a public record or in a publicly or commercially available manner, in a way that is different from the particular record you opted out, it will again appear on our Website. For example, if your address or area code changes, your new information -- including other associated identifying information -- will again appear unless you opt out the new record. Similarly, if the way in which your name or address appears in a record differs from a record you opted out (e.g., "Michael" instead of "Mike," or "1212 Second AVE NE" instead of "1212-2nd Avenue Northeast"), we may include the differing record. In addition to this Website, there are many other companies offering public records search services, and your request that we opt out your information from this Website will not prevent your information from appearing on these other services. In order for PeopleLookup to suppress or opt out your personal information from appearing on our Website, we need to verify your identity. To do this, we require faxed proof of identity. Proof of identity can be a state issued ID card or driver's license. If you are faxing a copy of your driver's license, we require that you cross out the photo and the driver's license number. We only need to see the name, address and date of birth. We will only use this information to process your opt out request. Please fax to 425-974-6194 and allow 4 to 6 weeks to process your request.	FCRA Restrictions. PeopleLookup is not a consumer reporting agency as defined in the Fair Credit Reporting Act ("FCRA"), and the information in the PeopleLookup databases has not been collected in whole or in part for the purpose of furnishing consumer reports, as defined in the FCRA. You shall not use any of our information as a factor in (1) establishing an individual's eligibility for personal credit or insurance or assessing risks associated with existing consumer credit obligations, (2) evaluating an individual for employment, promotion, reassignment or retention (including employment of household workers such as babysitters, cleaning personnel, nannies, contractors, and other individuals), or (3) any other personal business transaction with another individual (including, but not limited to, leasing an apartment).

PeopleSmart.com	If you would like to remove your name and address from appearing in the results of searches done at PeopleSmart.com, please complete and submit the form on our Opt-Out page. PeopleSmart.com will use good faith efforts to comply with properly completed Opt-Out requests. Opt-Out requests apply to the display of personal information in search results for living persons displayed on PeopleSmart.com and other sites operated by Inflection LLC. PeopleSmart.com may still make available details which are not specific to you (e.g. the city associated with an area code of a phone number). Third Party Databases. Opting-Out does not remove your name and address from data sources we do not control such as public records, or lists maintained by marketing companies. Anonymous Data. We and our partners reserve the right to make available anonymous search data that does not identify you individually (for example, the number of times a particular name was searched for). Other Consent. We may show results that include your information if a third party has provided documentation that you have consented to a disclosure by us. Hard Copy Vital Records, On-Site County Court Records Search, and Similar Services. We may show results that include your information in response to a hard copy vital records search, on-site county court records search, and similar services, that provide direct access to official government records. Pre-employment screening services, while currently not available, are also exempt from opt-out if added in the future.	We are not a consumer reporting agency as defined in the Fair Credit Reporting Act ("FCRA"), and the information in the databases has not been collected in whole or in part for the purpose of furnishing consumer reports, as defined in the FCRA. You shall not use our services as a factor in (1) establishing an individual's eligibility for personal credit or insurance or assessing risks associated with existing consumer credit obligations, (2) evaluating an individual for employment, promotion, reassignment or retention (including but not limited to employment of household workers such as babysitters, cleaning personnel, nannies, contractors, and other individuals), or (3) any other personal business transaction with another individual (including, but not limited to, leasing an apartment).
PrivateEye.com	Fill out and mail this form: http://www.usa-people-search.com/optout-form.pdf	**None listed**
WhitePages.com	**None listed**	**None listed**

USA-People-Search.com	http://www.usa-people-search.com/optout-form.pdf	We only deal in publicly available information. We are not a consumer credit reporting agency and do not compile financial information, tax records, credit reports, or any other non-public information.
Spokeo.com	http://www.spokeo.com/privacy	You may not use Spokeo.com or any information acquired from Spokeo.com: to engage in activities that would violate applicable local, state, national or international law, or any regulations having the force of law, including the laws, regulations, and ordinances of any jurisdiction from which You access Spokeo.com; for any commercial purpose including use in connection with marketing or sales activities; to send any type of spam, junk mail, or unsolicited communications; to evaluate a consumer's eligibility for credit or insurance to be used primarily for personal, family, or household purposes, to evaluate a person's eligibility for employment purposes, to evaluate a person's eligibility for a government license or benefit, to evaluate a person for renting a dwelling property, or for any other purpose specified in the Fair Credit Reporting Act (15 U.S.C. § 1681b); in any manner that may violate any local, state, federal, or international privacy law to which You may be subject on the basis of Your location or the location of the person searched.
PublicRecordsNow.com	**None listed**	**None listed**

DOBSearch.com	In order for us to “opt out” your public information from being viewable on the public DOBsearch People Finder search results, we need to verify your identity and require **faxed proof of identity**. Proof of identity can be a state issued ID card or driver's license, or notarized letter. If you are faxing a copy of your driver's license, you may cross out the photo and the driver's license number. We only need to see the name, address and date of birth. Please fax to **516-717-3012** and allow 4 to 6 weeks to completely process your request. It is your responsibility to ensure legibility of your document.	Concert Technologies Inc. is not a consumer reporting agency. Information retrieved from DOBsearch.com shall not be deemed a "consumer report" as defined in the federal Fair Credit Reporting Act (F.C.R.A.). Information retrieved from DOBsearch.com shall not be a factor used to determine creditworthiness, for pre-employment screening, for tenant screening, or for any purpose regulated by the Fair Credit Reporting Act.
Radaris.com	**None listed**	**None listed**
efindoutthetruth.com	**None listed**	**None listed**
identitypi.com	**None listed**	In the event of using this service for criminal or civil background checks, you should not assume that this data provides a complete or accurate history of any person's criminal or civil history. You should consult state and federal laws before using this information in making decisions on hiring or firing of employees. IDentityPi Inc cannot offer legal advice on how to use the information contained in criminal or civil background reports, and is not responsible for any action taken by the customer based on this information. Customers should use extreme caution when interpreting the results of a criminal or civil background search for any type of personal verification. Positive or false matches in criminal or civil searches may not provide confirmation of an individual's criminal or civil background. Proper use of these reports is the responsibility of you, the customer.

backgroundpi.com	**None listed**	4. FCRA Restrictions. IDentityPi Inc is not a consumer reporting agency as defined in the Fair Credit Reporting Act ("FCRA"), and the information in the IDentityPi Inc databases has not been collected in whole or in part for the purpose of furnishing consumer reports, as defined in the FCRA. You shall not use any of our information as a factor in (1) establishing an individual's eligibility for personal credit or insurance or assessing risks associated with existing consumer credit obligations, (2) evaluating an individual for employment, promotion, reassignment or retention (including employment of household workers such as babysitters, cleaning personnel, nannies, contractors, and other individuals), or (3) any other personal business transaction with another individual (including, but not limited to, leasing an apartment).
easybackgroundchecks.com	**None listed**	While EBC attempts to provide a quality product, these instant checks may not comply with local, state or federal employment laws such as the Fair Credit Reporting Act.
crimcheck.com	**None listed**	Crimcheck.com™ is FCRA Certified by CDIA
knowx.com	**None listed**	"I agree that I, and the organization I represent if applicable, will NOT use the information accessed through this search in whole or in part for the purpose of serving as a factor in establishing a consumer's eligibility for CREDIT or INSURANCE, EMPLOYMENT purposes, or for any other purpose(s) authorized under section 604 of the federal Fair Credit Reporting Act (15 U.S.C. Sec 1681 et seq.) ('FCRA") or similar state statute. KnowX is not a consumer reporting agency and KnowX reports do not constitute consumer reports as such terms are defined in the FCRA, and accordingly these reports may not be used for the purposes provided for in the FCRA. As this information is compiled from individual sources, KnowX LLC does not guarantee the comprehensiveness or accuracy of

		these records, nor that they are a complete history of activity."
backgroundchecks.com	If you do not want to receive promotional information from backgroundchecks.com, you can opt out by unchecking the appropriate box on your online registration form. If you did not opt out when you registered, and later decide that you are not interested in receiving this information, you can opt out at any time by sending an email to info@backgroundchecks.com. Please note that if you opt out of receiving promotional material from backgroundchecks.com, you still may receive such material from our worldwide subsidiaries, third party content providers, affiliates and other parties to whom we provide your information in the course of doing business, as explained above. If you would like to review or revise information you previously provided on an online form, or believe that what we currently have on record is incorrect, you may update your information in the Account section of this website.	By placing an order for services with us, you confirm that: you are ordering information about yourself, not about anyone else.

publicbackgroundchecks.com	**None listed**	The reports we provide are not to be confused with consumer reports, the purposes of which are governed by the Fair Credit Reporting Act (15 U.S.C. ¤1681, et seq.).
iamscreened.com	**None listed**	Each product meets the legal obligations of your potential employer as outlined in the Fair Credit Reporting Act (FCRA).
BackgroundsOnline	**None listed**	Backgrounds Online enhances and streamlines the process with: Detailed reports consisting of current, relevant and complete information and Ongoing compliance with the Federal Fair Credit Reporting Act (FCRA) and the ICRAA in California
PublicPeopleFinder.com	**None listed**	**None listed**

References

Aleecia McDonald & Jon M. Peha, "Track Gap: Policy Implications of User Expectations for the 'Do Not Track' Internet Privacy Feature," *Social Science Research Network* (September 2011), <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1993133>.

A. M. McDonald and Lorrie Faith Cranor, "Beliefs and behaviors: Internet users' understanding of behavioral advertising," *Social Science Research Network* (October 2010), <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1989092>.

Anita Ramasastry, "Can We Stop Zabasearch--and Similar Personal Information Search Engines?: When Data Democratization Verges on Privacy Invasion," *FindLaw*, 12 May 2005, <http://writ.news.findlaw.com/ramasastry/20050512.html>.

Ashkan Soltani et al., "Flash Cookies and Privacy," *Social Science Research Network* (August 2009), <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1446862>.

Balachander Krishnamurthy, Konstantin Naryshkin, & Craig E. Wills, "Privacy leakage vs. Protection measures: the growing disconnect," *Web 2.0 Security and Privacy Workshop* (May 2011), <http://web.cs.wpi.edu/~cew/papers/w2sp11.pdf>.

Center for Democracy and Technology, "Complaint and Request for Investigation, Injunction, and Other Relief," *Center for Democracy and Technology*, 30 June 2010, <https://www.cdt.org/files/pdfs/Spokeo.pdf>.

"Changing our privacy policies, not our privacy controls," *Google Public Policy Blog*, 31 January 2012, <http://googlepublicpolicy.blogspot.com/2012/01/changing-our-privacy-policies-not-our.html>.

Charles Duhigg, "How Companies Learn Your Secrets," *The New York Times*, 16 February 2012, <http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?_r=2&pagewanted=1&hp>.

Christine Fretten and Vaughne Miller, "The European Union: a guide to terminology, procedures and sources," *United Kingdom House of Commons Library*, 21 July 2005, 8, <http://www.w4mp.org/html/library/standardnotes/snia-03689.pdf>.

"Commission proposes a comprehensive reform of data protection rules to increase users'' control of their data and to cut cots for businesses," *Europa*, 25 January 2012, http://europa.eu/rapid/pressReleasesAction.do?reference=IP/12/46>.

David P. Baron, *Business and its Environment*, 6th ed. (Upper Saddle River, NJ: Pearson Education, 2010), 25.

David Talbot, "Using Crowdsourcing to Protect Your Privacy," *Technology Review*, 3 April 2012, <http://www.technologyreview.com/communications/40036/page1/>.

Digital Advertising Alliance, *Self-Regulatory Principles for Multi-Site Data*, November 2011, <http://www.aboutads.info/resource/download/Multi-Site-Data-Principles.pdf>.

"Do a Total Background Check on Yourself -- Annual Consumer Reporting Agencies," *Annual Medical Report*, 27 March 2010, <http://www.annualmedicalreport.com/do-a-total-background-check-on-yourself-annual-consumer-reporting-agency/>.

Erica Newland, "FTC Once Again Says Privacy Self-Regulation Isn't Enough," *Center for Democracy and Technology*, 27 March 2012, <https://www.cdt.org/blogs/erica-newland/2703ftc-once-again-says-privacy-self-regulation-insufficient>.

The Federal Trade Commission, *A Summary of Your Rights Under the Fair Credit Reporting Act*, <http://www.ftc.gov/bcp/edu/pubs/consumer/credit/cre35.pdf>.

The Federal Trade Commission, *FTC Staff Issues Privacy Report, Offers Framework for Consumers, Businesses, and Policymakers*," 1 December 2010, <http://www.ftc.gov/opa/2010/12/privacyreport.shtm>.

The Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*, March 2012, <http://www.ftc.gov/os/2012/03/120326privacyreport.pdf>.

"FTC Warns Marketers That Mobile Apps May Violate Fair Credit Reporting Act: Agency Sends Letter to Marketers of Six Apps for Background Screening," The Federal Trade Commission, 7 February 2012, <http://www.ftc.gov/opa/2012/02/mobileapps.shtm>.

John Brandon, "Spokeo a Growing Threat to Internet Privacy, Cyber Security Experts Warn," *Fox News*, 19 January 2011, <http://www.foxnews.com/scitech/2011/01/19/spokeo-cyber-security-warn-threat-privacy/>.

Jonathan Mayer, "A Brief Overview of the Supplementary DAA Principles," *The Center for Internet and Society*, 8 November 2011, <http://cyberlaw.stanford.edu/node/6755>.

Jonathan Mayer, "Tracking the Trackers: Microsoft Advertising" *The Center for Internet and Society*, 18 August 2011, <http://cyberlaw.stanford.edu/blog/2011/08/tracking-trackers-microsoft-advertising>.

Jonathan Mayer, "Tracking the Trackers: Self-Help Tools," *The Center for Internet and Society*, 13 September 2011, <http://cyberlaw.stanford.edu/blog/2011/09/tracking-trackers-self-help-tools>.

Jonathan R. Mayer & John C. Mitchell, "Third-Party Web Tracking: Policy and Technology," *The Center for Internet and Society* (March 2012), <http://cyberlaw.stanford.edu/publications/third-party-web-tracking-policy-and-technology>.

Julia Angwin, "The Web's New Gold Mine: Your Secrets," 30 July 2010, <http://online.wsj.com/article/SB10001424052748703940904575395073512989404.html>.

Karan Chopra, "Google and the Digital Advertising Alliance Will Support 'Do Not Track,' Agreed On Not To Collect Data About Users," *i2mag*, 23 February 2012, <http://i2mag.com/google-and-the-digital-advertising-alliance-will-support-do-not-track-agreed-on-not-to-collect-data-about-users/>.

Keyna Chow, Nicholas Petersen & Chris Jay Hoofnagle, "An Evaluation of Self-Regulation of Consumer Tracking and Profiling: Deficiencies and Recommendations for Improvement," *Submission to W3C Workshop on Web Tracking and User Privacy* (March 2011), <http://www.w3.org/2011/track-privacy/papers/Hoofnagle.pdf>.

Mika D. Ayenson et al., "Flash Cookies and Privacy II: Now With HTML5 And ETag Respawning," *Social Science Research Network* (July 2011), <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1898390>.

Omar Tene and Jules Polonetsky, "To Track or 'Do Not Track': Advancing Transparency and Individual Control in Online Behavioral Advertising," *Social Science Research Network*, 31 August 2011, <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1920505>.

"Online Data Vendors: How Consumers Can Opt Out of Directory Services and Other Information Brokers," *Privacy Rights Clearinghouse*, February 2011, <https://www.privacyrights.org/online-information-brokers-list>.

"'Other' Consumer Reports: What You Should Know about 'Specialty' Reports," *Privacy Rights Clearinghouse*, April 2012, <https://www.privacyrights.org/fs/fs6b-SpecReports.htm#2>.

Pedro G. Leon et al., "Why Johnny can't opt out: A usability evaluation of tools to limit online behavioral advertising," *Carnegie Mellon University CyLab* (October 2011), <http://www.cylab.cmu.edu/research/techreports/2011/tr_cylab11017.html>.

"Privacy Policy," *Web Finance Inc.*,

<http://www.businessdictionary.com/definition/privacy-policy.html>.

Ryan Singel, "Online Tracking Firm Settles Suit Over Undeletable Cookies," *Wired*, 5 December 2010, <http://www.wired.com/epicenter/2010/12/zombie-cookie-settlement/>.

Saranga Komanduri et al., "AdChoices? Compliance with Online Behavioral Advertising Notice and Choice Requirements," *Carnegie Mellon University CyLab* (March 2011), <http://www.casos.cs.cmu.edu/publications/papers/CMUCyLab11005.pdf>.

Tanzina Vega, "Code That Tracks Users' Browsing Prompts Lawsuits," *The New York Times*, 20 September 2011, <http://www.nytimes.com/2010/09/21/technology/21cookie.html?pagewanted=all>.

"U.S.-EU Safe Harbor Overview," *Export.gov*, 26 April 2012, <http://export.gov/safeharbor/eu/eg_main_018476.asp>.

Wendy David, "KISSmetrics, Hulu Hit with Privacy Suit," *MediaPost News*, 19 September 2011, <http://www.mediapost.com/publications/article/158730/>.

The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*," February 2012, <http://www.whitehouse.gov/sites/default/files/privacy-final.pdf>.

World Wide Web Consortium, *Tracking Protection Working Group*, <http://www.w3.org/2011/tracking-protection/>.