Foxes Guarding the Henhouse: An Assessment of Current Self-Regulatory Approaches to Protecting Consumer Privacy Interests in Online Behavioral Advertising

by Madolyn Orr

Table of Contents

Introduction

This paper examines the efficacy of the Federal Trade Commission's February 2009 staff report, "Self-Regulatory Principles for Online Behavioral Advertising" (FTC SRP), and the online advertising industry's July 2009 response, "Self-Regulatory Principles for Online Behavioral Advertising" (Industry SRP) in protecting consumer data privacy. In the FTC SRP, Federal Trade Commission (FTC) staff "attempted to balance the potential benefits of behavioral advertising against the privacy concerns" of consumers, specifically "the invisibility of the data collection to consumers; the shortcomings of current disclosures about the practices; the potential to develop and store detailed profiles about consumers; and the risk that data collected for behavioral advertising…could fall into the wrong hands or be used for unanticipated purposes."[1] Unfortunately, the self regulatory schema proposed by the FTC SRP and Industry SRP will not, on their own, sufficiently resolve these consumer privacy concerns.

The online behavioral advertising (OBA) practices addressed herein do not fall under the scope of any extant federal privacy laws. [2] That is, this paper begins from the premise that the FTC's authority to regulate "unfair or deceptive acts or practices" under Section 5 of the F.T.C. Act is the only basis upon which most OBA can currently be federally regulated.[3] The FTC has indicated that "the Commission will find deception if there is a representation, omission or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the

[1] FTC SRP p. ii

[2] *See, e.g.*, Children's Online Privacy Protection Act (COPPA), 15 U.S.C.A. § 6501 *et seq.*; Title V of the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 – 6809; Health Insurance Portability and Accountability Act (HIPAA), P.L. 104-191, 110 Stat. 1936 (1996), codified in part at 42 U.S.C. §§ 1320d *et seq.*; Video Privacy Protection Act of 1988, 18 U.S.C. § 2710. Whether the Electronic Communications Protection Act, 18 U.S.C. §§ 2510-2522, would prohibit some of the methods of data collection and use for OBA described here is open to debate. *See generally*, Center for Democracy & Technology, An Overview of the Federal Wiretap Act, Electronic Communications Privacy Act, and State Two-Party Consent Laws of Relevance to the NebuAd System and Other Uses of Internet Traffic Content from ISPs for Behavioral Advertising, July 8, 2008, http://www.cdt.org/privacy/20080708ISPtraffic.pdf.

[3] 15 U.S.C. § 45.

consumer's detriment."[4] Regarding unfairness, the FTC has indicated that they normally:

> expect the marketplace to be self-correcting, and…rely on consumer choice – the ability of individual consumers to make their own private purchasing decisions without regulatory intervention – to govern the market. [The FTC] anticipate[s] that consumers will survey the available alternatives, choose those that are most desirable, and avoid those that are inadequate or unsatisfactory. However,… certain types of sales techniques may prevent consumers from effectively making their own decisions, and… corrective action may then become necessary. Most of the Commission's unfairness matters are brought under these circumstances. They are brought, not to second-guess the wisdom of particular consumer decisions, but rather to halt some form of seller behavior that unreasonably creates or takes advantage of an obstacle to the free exercise of consumer decisionmaking[sic].[5]

As will be described in detail below, the methods of data collection and use that are currently practiced in relation to OBA are likely to mislead a reasonable consumer, to the detriment of his ability to protect his privacy interests. Similarly, the surreptitious nature of data collection and use for the OBA market and the difficulty of preventing such collection and use arguably constitute a form of seller behavior that unreasonably creates and takes advantage of an obstacle to free consumer decision making.

Nevertheless, the FTC has recently confirmed that it prefers a self-regulatory approach to protecting consumers' privacy interests from the risks inherent in OBA, rather than creating binding administrative rules or seeking further authority from Congress to directly regulate the practice.[6] After publishing draft guidelines in 2007[7] and providing time for public comment, in

---

[4] James C. Miller III, Chairman, FTC, FTC Policy Statement on Deception, appended to *Cliffdale Associates, Inc.*, 103 F.T.C. 110, 174 (1984).
[5] Michael Pertschuk, Chairman, FTC, FTC Policy Statement on Unfairness, appended to *International Harvester Co.*, 104 F.T.C. 949, 1070 (1984).
[6] *Privacy Implications of Online Advertising Before the S. Committee Commerce, Science, and Transportation*, 111th Cong. 1 (July 9, 2008) (Prepared statement of the F.T.C., delivered by Lydia Parnes, Director, Bureau of Consumer Protection, F.T.C.), *available at* http://commerce.senate.gov/public/_files/LydiaParnesFTCOnlinePrivacyTetimony.pdf ("At this time the Commission is cautiously optimistic that the privacy concerns raised by behavioral advertising can be addressed effectively by industry self-regulation").
[7] FTC Staff, Online Behavioral Advertising: Moving the Discussion Forward to Possible Self-Regulatory Principles (Dec. 20, 2007), http://www.ftc.gov/os/2007/12/P859900stmt.pdf.

February 2009 the FTC published the FTC SRP,[8] which outlines the FTC's most recent suggestions for industry improvements. In an accompanying statement, FTC Commissioner Jon Leibowitz, who was later named FTC Chairman by President Barack Obama in March 2009,[9] noted that "[i]ndustry needs to do a better job of meaningful, rigorous self-regulation or it will certainly invite…a more regulatory approach by our Commission. Put simply, this could be the last clear chance to show that self-regulation can – and will – effectively protect consumers' privacy in a dynamic online marketplace."[10] In response, several industry associations – the American Association of Advertising Agencies (4As), Association of National Advertisers (ANA), Council of Better Business Bureaus (BBB), Direct Marketing Association (DMA), and Interactive Advertising Bureau (IAB) – developed and published their own "Self-Regulatory Principles for Online Behavioral Advertising" (Industry SRP)[11] in order to "apply consumer-friendly standards to online behavioral advertising across the Internet."[12] Self-regulation of OBA *won't* effectively protect consumers' privacy interests unless it *can* do so. This paper therefore examines whether the recently proposed self-regulatory schema can sufficiently protect consumers' privacy interests.

Consumers take three types of approaches to protecting their informational privacy online. Some consumers are unconcerned about protecting their personal information, and are

[8] FTC Staff, Self-Regulatory Principles for Online Behavioral Advertising: Behavioral Advertising; Tracking, Targeting & Technology, (Feb. 2009), http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf. (hereinafter "FTC SRP")
[9] http://www.ftc.gov/commissioners/leibowitz/index.shtml
[10] Commissioner Jon Leibowitz, Concurring Statement regarding FTC SRP, (Feb. 2009), http://www.ftc.gov/os/2009/02/P085400behavadleibowitz.pdf.
[11] Press Release, Interactive Advertising Bureau, Key Trade Groups Release Comprehensive Privacy Principles for Use and Collection of Behavioral Data in Online Advertising (July 2, 2009), http://www.iab.net/about_the_iab/recent_press_releases/press_release_archive/press_release/pr-070209. ("In January 2009, the [industry] task force announced that it had been working on the development of these Principles in direct response to calls on the Internet ecosystem by the FTC to develop more robust and effective self-regulation of online behavioral based advertising practices that would foster transparency, knowledge and choice for consumers").
[12] American Association of Advertising Agencies, et al., Self-Regulatory Principles for Online Behavioral Advertising 1 (July 2009), http://www.iab.net/media/file/ven-principles-07-01-09.pdf.

therefore unwilling or unmotivated to act to protect it. The current federal approach to protecting consumer's personal information online, which favors industry self-regulation over binding legislation, works fine for this first group of consumers. Even if their informational privacy rights were legally protected, such consumers would be unlikely to seek to enforce these privacy rights.

A second group of consumers may be concerned about protecting their personal information online, but are unable, unwilling, or unmotivated to act to protect it. Empirical studies indicate that most American consumers fall into this category. As early as the year 2000, "eighty-six percent of Internet users [said] they [were] concerned about businesses or people they don't know getting personal information about them or their families. Seven in ten Internet users [were] concerned about hackers getting their credit card number and six in ten [were] concerned about someone learning personal information about them because of things they've done online," yet 56% of Internet users could not identify cookies as the primary online tracking tool. [13] "Among internet users who worry about their personal information, just over half (54%) say they take steps to limit the amount of personal information that is available about them."[14] The self-regulatory approach promoted by the FTC is predicated upon industry entities providing sufficient information about their personal information collection and dissemination practices to provide consumers the opportunity to make informed and effective decisions regarding what information practices they are willing to concede to.[15] Assuming sufficient information is available; some might say that if consumers in category two do not make an effort to take this

[13] Susannah Fox, *Trust and Privacy Online: Why Americans want to rewrite the rules*. THE PEW INTERNET & AMERICAN LIFE PROJECT, Aug. 20, 2000.
[14] Pew Internet & American Life Project, Digital Footprints (Dec. 2007), http://www.pewinternet.org/Reports/2007/Digital-Footprints.aspx.
[15] The FTC SRP "Principles provide for transparency and consumer control and reasonable security for consumer data." FTC SRP, p. ii

opportunity, then they do not have a basis for complaining about how their information is used. However, as described below, practically speaking it is extremely difficult for consumers to protect their privacy interests in the OBA context. If it were easier to do so, more consumers in this second category might move into the third category.

Consumers who are both concerned about protecting their personal information, and are willing and motivated to act to protect it make up the third category. The ultimate success of the self-regulatory approach will depend upon whether or not those consumers in category three – consumers who are concerned about keeping their personal information private, and are willing to act to do so – can indeed act to effectively protect their informational privacy.

The remainder of this essay explores whether, under the guidelines promulgated by the FTC SRP and Industry SRP, consumers have the ability to effectively protect the privacy of their personal information. Part I deals with why consumers might be concerned about the online collection of their personal data, and its uses both online and offline. Part II addresses why, despite these concerns, consumers presently acquiesce in the online collection and use of their personal data.

Part III examines the specifics of the self-regulatory schema proposed by the FTC and Industry SRPs, and the extent to which these guidelines enable consumers to proactively protect the privacy of their personal information. In the absence of additional legislation, consumers are only able to do so under the SRPs if (A) the entities collecting and using the relevant data have a privacy policy; (B) the consumer is able to locate the privacy policy and its relevant terms; (C) the consumer is able to read and understand the privacy policy; (D) the consumer has the opportunity to consent to, or avoid consenting to, the terms of the privacy policy; (E) the content of the privacy policy favors protection of consumer information, such that the result of the

entity's compliance with its own policy will be the consumer's ability to act to protect his or her own informational privacy interests; and (F) the guidelines of the self-regulatory schema are enforceable.

Part IV discusses whether technological fixes within the grasp of concerned consumers might sufficiently fill the gaps of the self-regulatory schema such that, overall, consumers can regain effective control of their online informational privacy. Part V concludes that, as the FTC SRP and Industry SRP schema currently stand, they do not provide consumers with an effective means by which they can act to protect their own informational privacy with regard to online behavioral advertising. And, since there are no reliable technological fixes available to effectively supplement the self-regulatory schema, consumers' privacy interests are left unprotected.

I. Why should consumers be concerned about the online collection and dissemination of personal data?

A. *Data Collection and Dissemination Is Widespread*

The harvesting of data online for use online and offline is widespread. Approximately 33.8% of all websites currently use behavioral advertising in some form.[16] Data is harvested from consumers both online and offline, and both voluntarily (actively) and surreptitiously (passively).[17] 'Active' and 'passive' refer to the level of participation the consumer, the data subject, has in the data harvesting interactions.

Active online collection of consumer data involves the voluntary provision of consumer

[16] Lynn Russo Whylly, *Behind the Numbers: Can Behavioral Hit the Target?*, OMMA: THE MAGAZINE OF ONLINE MEDIA, MARKETING & ADVERTISING (Aug. 2, 2007), http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=65079.

[17] Offline collection of consumer data is outside the scope of this paper. However, just as in online collection of consumer data, consumer data is collected both actively and passively. For example, consumers actively provide their data in face to face interactions at retail points of sale in traditional "brick and mortar" stores when they provide checking account and routing numbers while buying a pair of pants by check. Consumer data is also harvested passively from commercial data brokerages, and from public and semi-public records: for example, from land ownership records held by county recorders offices and by Title Insurance companies; records of unlawful eviction adjudications kept at the clerk's offices in county courthouses; and the like.

info by consumers to data collectors (first parties). Active methods of collection of consumer data are those in which the consumer proactively offers up his or her personal information to the data collector, for example by typing information into a web form. In active data harvesting interactions, consumers are, by definition, aware of the data collection, and consent to the data collection. Indeed, it is physically impossible to collect data this way without the consent of the consumer/data subject. In active data harvesting interactions consumers control the collection of data and what data is collected. Consumers also control whether data is collected at all, since they can avoid actively providing data altogether, for example by simply refraining from filling in the web form or clicking 'submit.' Consumers only provide data when they want to, and therefore control when and how often data is collected. Consumers also control how much data is actively collected, and only provide the amount of data they want to provide. Consumers can control the content of the data that others harvest from them: for example, perhaps they feel comfortable providing an email address, but not a telephone number. In sum, active online collection of consumer data provides a consumer with control over the information that is available about him or her online.

Passive online collection of consumer data involves involuntary collection of consumer information by data collectors. Data collectors may be synonymous with the website being viewed (first party data collection) or may be a third party in relation to both the consumer (data subject) and the website being viewed (first party) who is authorized and enabled by the website being viewed to collect data about the visitors (consumers/data subjects) to that website. Passive methods of collection of consumer data include spyware, cookies, flash cookies, web bugs (also known as beacons and clear gifs), deep packet inspection, content extraction, and more.

Cookies are small files of code automatically deposited on the hard drive of a consumer

as the consumer views a website set up to do so. These software files track what the consumer does online, and can compile a profile of the consumer's online behaviors and communicate them to a recipient software program controlled by the entity that profits from the data harvesting – for example, by using the information gleaned from cookies on a consumer's hard drive to choose to show that consumer advertisements based on the tracking data held by the cookie. Some web browsers provide mechanisms by which consumers can block the functioning of some cookies, although these same mechanisms can also block cookies required to use desired web-based functionalities.[18]

Flash cookies, also known as "local shared objects," work in a manner similar to regular cookies, but pose more privacy concerns. Flash cookies are a capability of Adobe's Flash plug-in program, and work "exactly like a browser cookie, except that [they] can also store data more complex than simple text."[19] Whereas regular cookies store a maximum of 4KB of data,[20] "by default, Flash Player allows each site to store only 100KB of data in a local shared object on your computer."[21] However, 100KB is not the technological maximum, but merely the default setting for the amount of personal information about a consumer that a website's flash cookie can store without the explicit consent of the user of the computer upon which it is stored. According to Adobe, "[i]f a site needs more [storage space] than that, you will see a dialog box requesting that you allow more space."[22] According to a recent study, flash cookies are used on 54 of the top 100 most popular websites, and "[t]hese 54 sites set a total of 157 Flash shared

[18] *See, e.g.*, Cookies, Firefox Support, Mozilla, http://support.mozilla.com/en-US/kb/Cookies; Block or allow Cookies, Windows Internet Explorer 8 help page, Microsoft, http://windows.microsoft.com/en-us/windows-vista/Block-or-allow-cookies.
[19] Adobe, What are local shared objects?, http://www.adobe.com/products/flashplayer/articles/lso/.
[20] David Bender, Practicing Law Institute, *Privacy/Data Protection Developments – 2008*, 947 PLI/Pat 39, 52 fn29 (2008).
[21] Adobe, What are local shared objects?, http://www.adobe.com/products/flashplayer/articles/lso/.
[22] *Id.*

objects files yielding a total of 281 individual Flash cookies."[23] Whereas most web browsers provide mechanisms that enable consumers to manage or delete regular "HTTP" cookies, such consumer controls are not available in relation to flash cookies.

> Flash cookies are stored in a different location than HTTP cookies, thus users may not know what files to delete in order to eliminate them. Additionally, they are stored so that different browsers and stand-alone Flash widgets installed on a given computer access the same persistent Flash cookies. Flash cookies are not controlled by the browser. Thus erasing HTTP cookies, clearing history, erasing the cache, or choosing a delete private data option within the browser does not affect Flash cookies. Even the 'Private Browsing' mode recently added to most browsers such as Internet Explorer 8 and Firefox 3 still allows Flash cookies to operate fully and track the user.[24]

Instead, in order to delete or manage the existence of flash cookies on his or her computer, a consumer must learn how to do so by following instructions on Adobe's website.[25] As one commentator notes, the flash cookie control mechanism provided by Adobe is "not easily understood….In fact, the controls are so odd, the page has to tell you that it is the control, not just a tutorial on how to use the control."[26] Of even more concern is the fact that flash cookies can effectively circumvent the consumer's attempts to delete or manage regular "HTTP" cookies: some are currently doing so. Some websites are using Flash cookies to 'respawn,' deleted HTTP cookies, meaning a regular HTTP cookie is recreated after the consumer has used the browser-based mechanism to proactively remove it. "This means that privacy-sensitive consumers who 'toss' their HTTP cookies to prevent tracking or remain anonymous are still being uniquely identified online by advertising companies."[27] Respawning thereby circumvents existing consumer technical controls meant to empower consumers to protect their own privacy

---

[23] Ashkan Soltani, Shannon Canty, Quentin Mayo, Lauren Thomas, and Chris Jay Hoofnagle, Flash Cookies and Privacy (August 10, 2009), *available at* http://ssrn.com/abstract=1446862.
[24] *Id.*, at 1.
[25] Adobe, How to manage and disable Local Shared Objects, http://kb2.adobe.com/cps/526/52697ee8.html#change.
[26] Ryan Singel, *You Deleted Your Cookies? Think Again*, WIRED (Aug. 10, 2009), *available at* http://www.wired.com/epicenter/2009/08/you-deleted-your-cookies-think-again/. The author concurs.
[27] Soltani, *supra* note 22.

interests online.

Web bugs, also known as beacons, tracking pixels, clear GIFs, or GIF tags, generally track consumer's clickstream data. As described by the U.S. District Court for the Southern District of New York, in order to harvest clickstream data an OBA entity such as "DoubleClick places GIF tags on its affiliated Web sites. GIF tags are the size of a single pixel and are invisible to users. Unseen, they record the users' movements throughout the affiliated Web site, enabling DoubleClick to learn what information the user sought and viewed."[28] This information is then used to select advertisements for OBA. Some HTML-enabled emails also use GIF tags to track whether and when a consumer opens his or her email.[29] There is no known mechanism of consumer control for blocking or managing data harvesting by this method.[30]

Spyware programs are similar to the passive data collection methods described above, and sometimes incorporate these methods for data collection, but generally do more than simply collect or track consumer data. Spyware programs are usually more invasive than run-of-the-mill data collection mechanisms, and sometimes change settings on consumer's computers (for example, changing a user's default homepage), forcibly redirect consumers' web browsers to a particular website, or invisibly install software that slows or hijacks consumers' computers for alternate uses.[31] Anti-spyware programs are widely available to consumers for purchase and download.

---

[28] *In Re Doubleclick*, 154 F.Supp.2d at 504.
[29] Stephanie Olsen, *Privacy advocates shine light on "Web bugs*," CNET News (Dec. 21, 2000), http://news.cnet.com/2100-1023-250230.html.
[30] There have been some attempts at developing technology to block or manage tracking GIFs. *See*, *e.g.*, *Id.* Tracking GIFS are technically very similar to the spacing GIFs that properly manage the alignment of graphics within browser viewers. Because the two types of graphics coding are virtually indistinguishable, blocking one (the tracking GIF) without blocking the other (the spacing GIF – which would cause most web graphics to be presented improperly) would be very difficult. See, Richard M. Smith, Web Bugs: Frequently Asked Questions (FAQ), FTC Online Profiling Public Workshop Nov. 8 1999, Public Comments (Nov. 11, 1999), http://www.ftc.gov/bcp/workshops/profiling/comments/wbfaq.pdf.
[31] *See*, Heather Osborn Ng, *Targeting Bad Behavior: Why Federal Regulators Must Treat Online Behavioral Marketing as Spyware*, 31 HASTINGS COMM. & ENT. L.J. 369, 374-75 (2009).

Data harvesting via deep packet inspection (DPI) involves the monitoring of data by a consumer's internet service provider (ISP) or another network administrator. Since the passage of the Communications Assistance for Law Enforcement Act (CALEA) in 1994, ISPs and other telecommunications providers have been required to build technological capabilities into their systems to efficiently respond to law enforcement warrants for information available on their networks. [32] DPI technology enables ISPs to comply with CALEA, and also enables network administrators to 'see' into the content of the internet traffic that travels over their networks. By analyzing the 'packets' of data that cross their networks, network administrators using DPI technology can "peek inside all of these packets and assemble them into a legible record of your e-mails, web browsing, VoIP calls, and passwords….In fact, that's exactly what companies like Narus use the technology to do."[33] As of 2008, "at least 100,000 U.S. customers [were] tracked [by DPI], and service providers have been testing it with as many as 10 percent of U.S. customers, according to tech companies involved in the data collection."[34] Despite the possible impact of DPI technology for OBA, internet "service providers exploring and testing such services have largely kept quiet – 'for fear of customer revolt,'"[35] and a major company intending to use DPI in relation to OBA in the U.S., NebuAd, has disintegrated under public and legal pressure.[36]

Consumer data is also harvested from the content of communications that consumers otherwise might consider 'private.' For example, in one type of content extraction, Google's free

[32] Pub. L. No. 103-414, 108 Stat. 4279, codified at 47 USC 1001-1010.
[33] Nate Anderson, *Deep packet inspection meets 'Net neutrality, CALEA*, ARS TECHNICA, (July 26, 2007), http://arstechnica.com/hardware/news/2007/07/Deep-packet-inspection-meets-net-neutrality.ars.
[34] Peter Whoriskey, *Every Click You Make: Internet Providers Quietly Test Expanded Tracking of Web Use to Target Advertising*, WASHINGTON POST, April 4, 2008, available at http://www.washingtonpost.com/wp-dyn/content/article/2008/04/03/AR2008040304052.html.
[35] *Id.*
[36] Ryan Singel, *NebuAd Nearly Shut Down, Court Papers Say*, WIRED (May 19, 2009), http://www.wired.com/epicenter/2009/05/nebuad-venture-capital-dispatch-wsj/.

Gmail web-based email program uses software to harvest data from the content of consumer's emails. "When a user opens an email message, computers scan the text and then instantaneously display relevant information that is matched to the text of the message."[37] More specifically, according to Google's related patents, "Gmail examines the entire content of the e-mail message including the header and addressing information in order to derive the 'concepts' contained in the e-mail. Relevant ads are then placed to the subscriber when the e-mail is displayed. Different ads may be served at different times depending on when the e-mail message is viewed, or re-viewed."[38] According to Google, "Gmail users can't opt out of receiving ads because these sponsored links help Google support the cost of providing Gmail for free to our users."[39]

Similar concerns arise regarding cloud computing. Cloud computing "generally involves a subscription-based service that satisfies computing and storage needs from an immense hardware and communication *infra*structure, which is managed by a third-party provider,"[40] enabling consumers to access their stored data and software applications remotely. "Because users merely are using the Internet to obtain their data and computing power, they are less tethered to their office, home, or even their physical computer systems."[41] Approximately 69% of U.S. internet users use some web-based software that utilizes cloud computing.[42] End users benefit from the increased flexibility offered by cloud computing services, however in exchange for this flexibility they relinquish possession of and control over access to the data that resides on

[37] Google Privacy Center, Privacy FAQ, http://www.google.com/privacy_faq.html#toc-mail-ads.
[38] Electronic Privacy Information Center, Gmail Privacy Page, http://epic.org/privacy/gmail/faq.html#21.
[39] Gmail by Google, Ads in Gmail, http://mail.google.com/support/bin/answer.py?hl=en&answer=6603.
[40] Daniel J. Buller and Mark H. Wittow, *Cloud Computing: Emerging Legal Issues, Data Flows, and the Mobile User*, LANDSLIDE 54 (Nov./Dec. 2009).
[41] *Id.*
[42] John B. Horrigan, Associate Director, Pew Internet and American Life Project, *Cloud Computing Gains in Currency* (Sept. 12, 2008), *available at* http://pewresearch.org/pubs/948/cloud-computing-gains-in-currency.

cloud computing systems. A recent complaint filed with the FTC[43] alleges that the terms of service governing various cloud computing services run by Google, including Gmail, Google Docs, Google Desktop, Picasa, and Google Calendar, misrepresent the privacy and security of its users' data. In particular, Google "assures users of Google Docs that their data are secure and private unless the user specifically publishes them to the Web or invites collaborators. However, Google's Terms of Service explicitly disavow any warranty or any liability for harm that might result from Google's negligence to protect the privacy and security of user data," despite known security flaws.[44] Although the complaint focuses on problems with the security of user data held by a cloud computing service provider, it highlights the volume of consumer data that is available for content-extraction type data harvesting. Indeed, some content extraction is already occurring in software applications based on the cloud computing model, for example, content extraction and use for OBA within Gmail, as described above. Consumers who use cloud computing systems are "very concerned"[45] about this type of data use. Of cloud computing users, ninety percent would be "very concerned if the company at which their data were stored sold it to another party.…80%…would be very concerned if companies used their photos or other data in marketing campaigns," and "68% …would be very concerned if companies who provided these services analyzed their information and then displayed ads to them based on their actions."[46] Presently, there does not appear to be a way for consumers using cloud computing services to prevent their personal information from being harvested and used for OBA.

These methods of data collection also occur on mobile platforms such as mobile phones, personal digital assistants (PDAs), e-books and digital readers, portable entertainment players

[43] EPIC Complaint Before the Federal Trade Commission, *In re* Google, Inc. and Cloud Computing Services (Mar. 19, 2009), *available at* http://epic.org/privacy/cloudcomputing/google/ftc031709.pdf.
[44] Buller, *supra* note 40 at 55.
[45] Horrigan, *supra* note 42.
[46] *Id.*

such as the iTouch, and vehicle-based GPS navigation systems.[47] For example, niche OBA company Lat49 uses proprietary technology to enable marketers to "target their messages to a mobile device user's physical location, as well as any expressed location of interest, based on map views, weather lookups, local business searches, or local news requests. These location data points can then be combined…to provide the most accurate location-driven audience targeting available to advertisers today."[48] Depending upon the manner in which location data is harvested and used, this method of OBA and others like it appear to contravene the FTC SRP's requirement that affirmative consent be obtained before 'sensitive' information such as "precise geographic location information" is used for OBA.[49] If there are any mechanisms available for consumers to prevent the harvesting and use of data on mobile platforms for OBA purposes, this author is unaware of them.

Generally speaking, "the technology involved with the Internet allow[s] online surveillance to occur essentially invisibly to the user. It is virtually impossible for a user to keep track of all of the ways that they can be monitored while surfing the web."[50] In short, in the context of passive data collection methods, consumers do not get to control the amount, frequency, or content of the data collected. Because consumers/data subjects cannot control data harvesting, they are reliant on those who do control the collection of their personal information (OBA industry entities), or who could control such collection (the FTC) to protect their related privacy interests.

The FTC SRP attempts to resolve these concerns by suggesting that entities engaged in

---

[47] Rita Change, Mobile Marketing Beyond the Mobile Phone, Advertising Age (Nov. 30, 2009), *available at* http://adage.com/article?article_id=140746.
[48] Press Release, Lat49, Lat49 brings location-driven advertising and 'Location Logic' to mobile phones, http://lat49.com/aboutus/newstemplate.php?id=22.
[49] FTC SRP, 44.
[50] David Goldman, *I Always Feel Like Someone Is Watching Me: A Technological Solution For Online Privacy*, 28 Hastings Comm. & Ent L.J. 353, 355 (2006).

OBA provide "a clear, concise, consumer-friendly, and prominent statement that… data about consumers' activities online is being collected at the site for use in providing advertising… tailored to consumers' interests."[51] In other words, the FTC SRP recommends that OBA entities adopt clear and prominent privacy policies that disclose that OBA is occurring on the first party's website. Whether this recommendation is sufficient to enable consumers to protect their privacy interests is discussed more fully in Section III below.

B. *How collected data is used.*

Once personal information is collected, it is used in a variety of ways. Data collected from and on websites is used for site administration, for example to enable customers to log-in to their web-based email accounts, view their bank account information, and so on. Harvested data is also used to fulfill more traditional customer service needs, such as shipping goods to recipients at previously recorded addresses, confirming credit card purchases via previously recorded email addresses, communicating with repeat customers via email newsletters, and the like.

The collected data is also used to make money. The practice of data harvesting is widespread because it is profitable. In 2008, online advertising yielded a total of $23.4 billion in revenue nationwide.[52] Information about consumers has become commoditized: there is a large market for the sale, correlation, and resale of consumer data. Single data points are valuable, and the correlation and aggregation of those data points into marketing lists and databases is even more valuable.[53]

---

[51] FTC SRP, 46. See Section III.B, *infra*.

[52] PricewaterhouseCoopers, IAB Internet Advertising Revenue Report: 2008 Full-Year Results (March 2009), http://www.iab.net/media/file/IAB_PwC_2008_full_year.pdf.

[53] Corey Ciocchetti, *Just Click Submit: The Collection, Dissemination, and Tagging of Personally Identifying Information*, 10 VAND. J. ENT. & TECH. L. 553, 556 (2008). For example, a consumer can buy another consumer's cell phone records for approximately $100, and $180 can purchase an individual psychological/behavioral profile. "[D]ata collection firms aggregate these scattered pieces of personal information located all over the Web to create

In recent years, there has been a consolidation of multi-million dollar data collection and adserving companies with internet search companies. In 2007 Yahoo! acquired BlueLithium, at the time the fifth largest online ad network in the U.S. and the second largest in the U.K.[54] According to Yahoo!, the merger "will give advertisers access to powerful data analytics, advanced targeting, and innovative direct-response buying strategies across a broad range of high quality inventory. BlueLithium's product capabilities include: audience targeting based on consumer interests; remarketing ads to consumers across the Web who have interacted with an ad or web page; custom segmentation; spot buying capabilities to extend reach and frequency against a marketer's target audience."[55] Also in 2007, AOL/Time Warner acquired TACODA, which "track[ed] visits to key pages on some of the Web's most popular properties, including The New York Times….It then use[d] the information gleaned from those visits to send related, targeted ads to specific computers whose users are clicking on high-traffic sites throughout the Web."[56] In March 2008 Google completed its acquisition of DoubleClick,[57] which, among other services, allows advertisers to target ads based upon "audience segmentation; geographic selection by… zip and area codes; time of day and specific days; browser type and operating system; and keyword."[58] Mergers such as these allow the increased consolidation of consumer data harvested from multiple internet inflows (search queries, clickstream data, etc.), and the increased consolidation of platforms for web publishers who 'serve' ads to consumers based on

---

detailed profiles of a person's life. These 'digital dossiers' are worth much more on the open market than bits and pieces of personal information are worth individually." *Id.*, 557.

[54] Press Release, Yahoo! Inc., Yahoo! Announces Agreement to Acquire BlueLithium: Important Next Step in Yahoo!'s Mission to Lead the Transformation of How Advertisers Connect To and Engage With Their Customers (Sept. 4, 2007), http://yhoo.client.shareholder.com/PRESS/releasedetail.cfm?ReleaseID=262635.

[55] *Id.*

[56] Catherine Holahan, *AOL Joins the Ad Acquisition Party: With its plan to purchase Tacoda, AOL will take on Google, Yahoo and Microsoft in the swelling online advertising market*, BUSINESS WEEK (July 24, 2007), http://www.businessweek.com/technology/content/jul2007/tc20070724_535622.htm.

[57] Google Press Center, Google Closes Acquisition of DoubleClick (March 11, 2008), http://www.google.com/intl/en/press/pressrel/20080311_doubleclick.html.

[58] DoubleClick, Solutions for Marketers: Reach the Right Audience, http://www.doubleclick.com/solutions/marketers/reach_the_right_audience.aspx.

their previously collected data points. From the commercial perspective, this consolidation enables broader data point collection and more precise correlation and analysis, which in turn increases the market value of the harvested data. "Buyers are incentivized to purchase PII [personally identifiable information] because such information arrives prepackaged – collected, mined, and correlated into categorized lists – and ready to use. Purchasers find it much easier and more efficient to buy prepackaged PII than to gather and aggregate the same information independently."[59]

Commercial entities who harvest data can profit from it by packaging this data in usable formats and selling it to other commercial entities, government bodies, and non-profit organizations. Just as electronic record keeping is becoming more efficient than paper record keeping generally, it is much easier and faster to harvest consumer data online than it ever was through other means. Data harvested online can be automatically saved, retrieved, and manipulated in digital formats that can be transferred among entities almost spontaneously through email or other digital means. Once created, the overhead costs of maintaining these data harvesting programs are rather low in relation to their potential profitability. In short, "[c]ompanies are incentivized to sell the information they collect because, with a few mouse clicks and a plethora of available buyers, they generate additional revenue streams."[60]

Commercial entities who buy data profit from it by using it to tailor advertising campaigns to effectively target products and services to particular individuals based on the data points derived from their past behaviors. This is called behavioral advertising (BA), or targeted advertising. When such advertising campaigns are conducted online, this practice is called

[59] Ciocchetti, *supra note 50 at* 576.
[60] *Id.* See also, discussion of secondary uses, *infra*.

online behavioral advertising (OBA), or "online preference marketing."[61] Data buyers profit from these practices because the targeted use of the data increases the return on their marketing investments, yielding higher revenues in proportion to the cost of the advertising.[62] Data buyers increase their marketing return on investment by increasing the relevancy of advertisements to the particular web viewer to whom they appear, and by reducing the likelihood of showing irrelevant advertising to uninterested web viewers.[63]

In some instances, the commercial entity that collects the data and the entity that uses the data to conduct OBA may be one in the same. The FTC SRP guidelines refer to this phenomenon as 'first party' or 'intra-site' OBA.[64] The FTC defines first party OBA as "the tracking of the consumer's online activities in order to deliver a recommendation or advertisement tailored to the consumer's inferred interests involv[ing] a single website where the consumer has previously purchased or looked at items."[65] 'First party' OBA may be used to advertise a commercial entity's (the first party's) own products and services to repeat customers through the interface of its own website (the first party's website). Alternatively, first party OBA may be used to sell the products or services of another commercial entity (third party A) through the interface of the first party's website (*see Figure 1*), so long as it does not use a separate ad-publishing or ad-serving company (third party B) to do so (*see Figure 2*).

---

[61] This term is used by the Network Advertising Initiative (NAI) in its comments to the FTC. See Letter from J. Trevor Hughes, Executive Director, NAI, to Office of the Secretary, FTC 15 (April 10, 2008), http://www.ftc.gov/os/comments/behavioraladprinciples/080410nai.pdf. Readers may also be familiar with the term "direct marketing," which is often used to denote behavioral advertising that occurs through the medium of mailing direct advertising pieces through the U.S. postal service.

[62] Andrew Hotaling, *Protecting Personally Identifiable Information on the Internet: Notice and Consent in the Age of Behavioral Targeting*, 16 COMMLAW CONSPECTUS 529, 536 (2008) (behavioral targeting "offers companies the highest return on investment for dollars spent on e-advertising").

[63] K. C. Jones, *Online Behavioral Ads Beat Contextual Ads, Survey Says*, INFORMATION WEEK, Sept. 13, 2007, http://www.informationweek.com/story/showArticle.jhtml?articleID=201806110 (citing research showing that behavioral targeting outperforms contextual advertising in gaining consumer attention by at least 10%).

[64] FTC SRP, 26. Industry SRP p. 23.

[65] FTC SRP, 27.

Figure 1

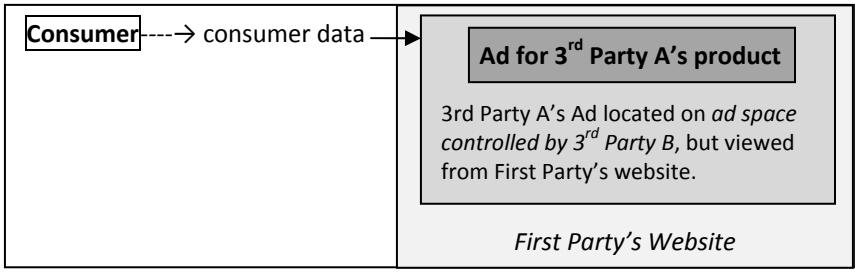

Figure 2

The key point is that, in first party OBA, the interaction of consumer data and commercial entity is singular, two-way (between the website administrator and consumer), and linear. The FTC has declined to address first-party OBA within the scope of their self-regulatory guidelines, because it is persuaded that "'first-party' behavioral advertising practices are more likely to be consistent with consumer expectations, and less likely to lead to consumer harm, than practices involving the sharing of data with third parties or across multiple websites."[66]

Although the data harvested online is used for a great many purposes, and the data used in OBA may be derived from many sources (including offline sources), it is only the practice of collecting data online for use in OBA *by another entity* (i.e., a third-party entity) that the FTC SRP and Industry SRP seek to 'regulate.' According to the FTC SRP:

> [W]hen behavioral advertising involves the sharing of data with ad networks or other third parties, the consumer may not understand why he has received ads from unknown marketers based on his activities at an assortment of previously viewed websites. Moreover, he may not know whom to contact to register his concerns or how to avoid the practice…. If a website collects and then sells or shares data with third parties for the purpose of behavioral advertising or participates in a network that collects data at the site for purposes of behavioral advertising,… such practices would remain within the scope of the Principles.[67]

The Industry SRP defines third-party OBA in a much more complex way.

[66] FTC SRP p. 26
[67] FTC SRP, 28.

According to the Industry SRP, a third-party is an entity that "engages in OBA on a non-Affiliate's Web site."[68] Under the Industry SRP, two entities are non-affiliates if 1) the two entities are subject to OBA policies that are materially inconsistent, or 2) the two entities are subject to OBA policies that are *not* materially inconsistent, and the two entities are not under significant common ownership, and neither entity has the power to exercise a controlling influence over the management or policies of the other.[69] Given this complex definition, it is virtually impossible for a reasonable consumer to know or to find out whether the particular website he is visiting is conducting only contextual or first-party OBA – in which case the practice is not covered by either SRP guidelines – or whether the website is engaged in third-party OBA practices – in which case the consumer's privacy interests would presumably be sheltered by whatever protections are provided by the SRPs.

In particular, how is an average consumer to know if a particular website is acting as a third party operating under the Principles, or as a first party or group of affiliated first parties? Is it reasonable to ask consumers to review and compare two or more sets of OBA policies for possibly-affiliated entities in order to determine whether the entities have materially consistent OBA policies, and therefore practice first or third party OBA? How much effort should a reasonable consumer be expected to expend attempting to discover whether two entities who may be engaged in OBA practices on a particular website are under common ownership? Is it reasonable to ask a consumer to research the corporate structures or shareholder portfolios of multiple, possibly-affiliated companies before deciding whether to use a particular website and thereby expose his

[68] Industry SRP, 27.
[69] Industry SRP,21-22 (defining "Affiliate" and "Control").

personal information to these corporate entities? How is a consumer to know whether one entity has sufficient power to influence the management or policies of the other?

The Industry SRP provides little useful guidance for the average consumer in this regard. Consumers cannot rely on brand or company names to determine whether such entities are acting as third parties covered by the Principles, or as first parties not subject to the Prinicples. "The tests for [affiliate] Control are unrelated to brand names….[D]ifferent brands, if they otherwise meet one of the tests…, would be treated as Affiliates rather than Third Parties."[70] The Industry SRP further notes that:

> the use of the term Affiliate is intended to allow affiliated companies that are in the same corporate family to share information within that family as if they are the same company, thereby benefitting from their collective assets…. In many cases companies can readily be transparent either in branding on the Web sites or through clarity in the privacy notices of their particular Affiliates….However, such branding on a Web site or inclusion in a privacy notice is not required under the Principles as in some instances the complexity of corporate affiliates driven by corporate legal principles post practical operational challenges.[71]

Accordingly, although OBA entities may, of their own accord, provide transparency to consumers regarding their affiliate or non-affiliate status, and thereby provide consumers with information regarding whether the OBA practices they engage in are or are not covered by the Principles, they are not required to do so to be in compliance with even the voluntary self-regulatory principles.

In sum, both the FTC SRP and Industry SRP exclude from their policy suggestions the practice of first-party OBA, as defined by the FTC: "where no data is shared with third parties."[72] However, the Industry SRP appears to exclude from its self-regulatory scheme the very practice which the FTC considers most threatening to consumer privacy: the sharing of

[70] Industry SRP, 22.
[71] *Id.*
[72] FTC SRP, 46.

consumer data with ad networks or other third parties.[73]

Both the FTC SRP and Industry SRP also exclude the use of data harvested online for purposes other than OBA – what they call "secondary uses" – from the scope of their suggestions. The FTC SRP covers only "the tracking of a consumer's online activities over time… in order to deliver advertising targeted to the individual consumer's interests,"[74] and not secondary uses such as "selling personally identifiable behavioral data, linking clickstream data to PII [personally identifiable information] from other sources, or using behavioral data to make credit or insurance decisions."[75] The Industry SRP uses similar language to limit the scope of the personal consumer information covered by its Principles: "All references to data collection and use in the Principles are for data collected online and used for Online Behavioral Advertising purposes. Data collected and used for other purposes falls outside of the definition of Online Behavioral Advertising and these Principles."[76] In keeping with this limitation, the Industry SRP is careful to always include the descriptive terms "for online behavioral advertising purposes,"[77] or similar phrases[78] when discussing OBA data collection practices, thereby narrowing the range of the data collection practices that fall under its scope.

During the 2007-2008 public comment period, the FTC received comments on secondary uses of "tracking data."[79] "Most of the industry comments that [addressed] this… focused on such internal [secondary] uses as website design and optimization, content customization, research and development, fraud detection, and security."[80] On the other hand, consumer group comments cited "potential harmful secondary uses, including selling personally identifiable

[73] *Id.* at 28.
[74] *Id.* at 46 (formatting emphasis eliminated).
[75] *Id.* at 45.
[76] Industry SRP, 24.
[77] *Id.* at 4.
[78] *See, e.g.*, Industry SRP, 20 ("the collection and use of the data used to deliver relevant advertising").
[79] FTC SRP, 44.
[80] *Id.*

behavioral data, linking click stream data to PII [personally identifiable information] from other sources, or using behavioral data to make credit or insurance decisions."[81] In the FTC SRP, FTC staff conclude that, because there was a "dearth of responses to staff's request for specific information" from industry regarding these potentially harmful secondary uses, "it is unclear whether companies currently use tracking data for non-behavioral advertising purposes other than the internal operations identified above."[82] Because FTC staff found it to be "unclear" whether data collected for OBA is being sold, correlated with data from other sources, and the like, the staff "does not propose to address this issue"[83] in the FTC SRP. Unfortunately for consumer privacy protection, FTC staff seem to be the only ones who are "unclear" whether consumer data collected for OBA purposes is being used for these secondary purposes. There is no doubt that it is being so used. Online advertisers themselves proclaim that this is so. For example, a writer for ThoughtStream, a blog run by ChoiceStream, Inc.,[84] notes that:

> [t]o capitalize on performance technology, you need to really understand each shopper's tastes and preferences by analyzing all of the behavioral and shopping data you have available. That includes purchase data (both online and in-store), loyalty card transactions, online click and browsing behavior, etc. You're missing a huge opportunity if you're not learning from every engagement a customer has on your site, in your store and with your brand.[85]

Rich Karpinski of *Advertising Age* describes the process of OBA this way:

> Behavioral data are collected on publisher or e-commerce websites (or via offline methods, such as the collection of straight demographic data), then sold to a data exchange, which then resells the data at market value to advertisers, which use the data to buy impressions directly from another publisher via an ad network or ad

---

[81] *Id.* at 44-45.
[82] *Id.* at 45.
[83] *Id.* ("Given the dearth of responses to staff's request for specific information, it is unclear whether companies currently use tracking data for non-behavioral advertising purposes other than the internal operations [website design, content customization, research and development, fraud detection, and security] identified above").
[84] ChoiceStream, Inc. is an OBA company that "delivers dynamic, personalized display ads, email and ecommerce product recommendations that increase purchases and customer engagement for today's biggest brands." About ChoiceStream, http://www.choicestream.com/company/.
[85] Posting of Cheryl Kellond to ThoughtStream, "Shining a Light on Performance Display Advertising," http://www.choicestream.com/blog/archives/2009/09/shining_a_light.asp (Sept. 2, 2009, 10:23 AM EST).

> exchange. The result is that data exchanges can, for instance, collect information from travel site Kayak about users who are booking flights to Orlando, then sell that cookie-based data to a buyer in the exchange. That buyer then uses that data to go to another party to buy and serve ads (say, for a hotel stay) to those users when they are surfing another site. Just as likely, a publisher or network could buy the data in order to improve the ad targeting on the sites they're selling.[86]

The FTC and Industry SRPs' failure to address the issue of secondary use of data harvested from consumers online therefore fails to address one of the largest risks to consumers' privacy interests.

By their terms, both the FTC SRP and Industry SRP also do not apply to what is termed 'contextual advertising.' Because the advertisements presented to web viewers via contextual advertising are not dictated by data sets tied to the particular viewer, but instead are tied to the topics of the website on which they are presented, contextual advertising may be targeted advertising, but is not necessarily OBA per se. For example, if a golf course's website were using contextual advertising rather than OBA, a web visitor to the site might see advertisements for golf shoes or golf clubs not because the purchased aggregated behavioral data linked to the web viewer indicated that he was interested in golf (as would be the case if OBA were being used); but rather because the contextual advertising programmer has inferred that topics related to the topic of the website (golf) are also likely to be of interest to all those who visit the golf course's website, and presents ads for these related topics (golf shoes, golf clubs) accordingly. "[C]ontextual advertising provides greater transparency than other forms of behavioral advertising, is more likely to be consistent with consumer expectations, and presents minimal privacy intrusion when weighed against the potential benefits to consumers….[FTC] Staff consequently does not believe that it is necessary for the Principles to cover this form of online

[86] Will Using Behavioral Data Lead to Smarter Ad Buys?, Advertising Age, http://adage.com/adnetworkexchangeguide09/article?article_id=136003.

advertising."[87]

C. *Data Security Breaches and Identity Theft Are Also Widespread*

The practices of data harvesting, analysis, and dissemination pose several threats to consumer interests. In many instances, the initial data collection process itself poses an inherent threat to consumer's privacy interests. Some data collection practices prompt fewer privacy concerns than others. For example, as discussed above, active data collection practices are likely to prompt fewer privacy concerns than passive data collection practices, since they are conducted with the active participation and consent of the data subject and therefore do not substitute the data collector's decision regarding what to share for the data subject's own decisional agency.

A more tangible threat to consumer's financial interests and physical safety is the involvement of harvested data in incidences of data security breach, and related incidences of identity theft. Data security breaches are prevalent and becoming more common. For the past nine years, identity theft has been the topic of the most frequent consumer complaints to the FTC, constituting 26% of the total complaints to the FTC in 2008.[88] The number of reported data breaches has increased by 47% from 446 in 2007 to 656 in 2008,[89] and since 2005, approximately 341,742,628 database records containing personal information have been exposed to identity theft risk through known data breaches.[90] Public knowledge of these data security breaches has increased over time, as the vast majority of U.S. states and territories now statutorily require companies who hold various types of consumer data and who experience an unintentional breach in the security of that data to provide notification of the breach either to the

[87] FTC SRP, 30.
[88] Press Release, FTC, FTC Releases List of Top Consumer Complaints in 2008, http://www.ftc.gov/opa/2009/02/2008cmpts.shtm.
[89] ITRC, 2008 Data Breach Totals Soar (June 15, 2009), http://www.idtheftcenter.org/artman2/publish/m_press/2008_Data_Breach_Totals_Soar.shtml.
[90] Privacy Rights Clearinghouse, Chronology of Data Breaches (accessed Nov. 30, 2009), http://www.privacyrights.org/ar/ChronDataBreaches.htm.

affected consumers themselves, or to consumer protection authorities.[91]

The harvesting and sale of consumer data involves intentional exposure of consumer data to entities other than the entity to which the consumer first exposed their personal information. However, data breach notification laws only require notice upon the unintentional exposure of consumer data to outside entities. The exposure of consumer data occurs in a variety of ways, including attacks from external hackers who exploit companies' own lax data security systems. In a 2009 survey, 92% of information technology security professionals indicated that the organization they worked for had experienced a criminal cyber attack.[92] Unintentional loss of consumer data also is caused by company employees, for example from lost or stolen laptops containing consumer data,[93] and by intentional exposure of consumer data by company employees. According to research by the non-profit Identity Theft Resource Center, insider theft of data by employees now accounts for 15.7% of total known data breaches, and has more than doubled between 2007 and 2008.[94] In addition, phishing schemes play on human psychology to

[91] Forty-five states, the District of Columbia, Puerto Rico, and the Virgin Islands now have some form of legislation that requires notice to consumers whose personal information has been involved in a data breach. States lacking such a law include Alabama, Kentucky, Mississippi, New Mexico, and South Dakota. National Council of State Legislatures, State Security Breach Notification Laws as of July 27, 2009, http://www.ncsl.org/Default.aspx?TabId=13489.

[92] Ponemon Institute LLC, 2009 Security Mega Trends Survey 3-4 (Nov. 2008), http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/2009%20Security%20Mega%20Trends%20Final%20V_3.pdf (In comparison, of those surveyed, 40% were concerned that an external cyber attack would cause a business interruption, but only 29% were concerned that such an attack would cause the loss of information about employees or customers, thus requiring data breach notification).

[93] Ponemon Institute LLC, The Cost of a Lost Laptop 2 (APRIL 2009), http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/Cost%20of%20a%20Lost%20Laptop%20White%20Paper%20Final%203.pdf (Though the cost of a lost laptop varies by industry, the average value to the corporate owner of a lost laptop is $49,246, based on the costs of replacement, detection, forensics, lost intellectual property, lost productivity, legal, consulting and regulatory expenses, and the costs of dealing with data breach , which alone accounts for 80% of the cost of a lost laptop).

[94] ITRC, *supra* note 89. In a well publicized incident, in August 2008 Rene L. Rebollo Jr., a senior financial analyst at Countrywide's subprime lending arm was accused of selling the personal information of company clients over the course of two years, in batches of 20,000 about every week for $500 per batch, or 2.5 cents per person. Renae Merle, *Countrywide Says Customer Data Were Sold*, WASHINGTON POST, Sept. 14, 2008, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2008/09/13/AR2008091300337_pf.html.

prompt fraudulent transfers of information.[95]

Such data security breaches can have severe financial and legal ramifications for the businesses involved. "The direct monetary ramifications of being called to account for alleged violations include counsel fees and a major diversion of…employee time....[M]onetary sanction[s] may run as high as one million dollars or more, and injunctive relief may require"[96] an even greater immediate cost outlay, "with an ongoing reporting cost stretching out for as long as 20 years."[97] Additionally, "a data breach will require the company to spend money notifying data subjects when notification is required by law or is deemed advisable by the company...[and] any credit monitoring or other services funded by the company for the benefit of affected data subjects will cost money."[98] As data breach notification laws increasingly require the fact that data breaches have occurred to be made public, consumer perceptions of the desirability of doing business with companies who have experienced data breaches change for the worse. This loss of consumer/customer goodwill in turn creates new financial burdens on the breaching entity, including lost opportunity costs of as much as $128 per breached record, which include customer turnover and the costs of acquiring new customers.[99]

Business litigation risks arise from both private and governmental quarters. "A company's failure to comply with privacy requirements that adversely affects (or colorably affects) a competitor, may trigger litigation….While injury as a result of a competitor's privacy violation may not be particularly common, it can occur, and compliance with privacy law will

---

[95] FTC Consumer Alert: How Not to Get Hooked by a 'Phishing' Scam (October 2006), http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt127.shtm.
[96] David Bender, *Privacy and Data Protection Developments – 2009*, 984 PLI/PAT 131, 155 (2009).
[97] *Id.*
[98] *Id.* at 158.
[99] Thomas Claburn, *The Cost Of Data Loss Rises*, INFORMATION WEEK, Nov. 28, 2007, http://www.informationweek.com/story/showArticle.jhtml?articleID=204204152.

avert it."[100]

In the past few years the FTC has increasingly pursued systemic data security failures under Section 5's unfair and deceptive trade practices provision. As of March 2008, the FTC had pursued twenty such actions.[101] For example, *In The Matter of The TJX Companies, Inc.*,[102] the FTC alleged that TJX, the parent company of TJ Maxx and other retail stores, "failed to use reasonable and appropriate security measures to prevent unauthorized access to personal information on its computer networks. An intruder exploited these failures and obtained tens of millions of credit and debit payment cards…[and] the personal information of approximately 455,000 consumers who returned merchandise to the stores," resulting in fraudulent charges amounting to tens of millions of dollars.[103]

In 2006, following a 2005 data breach that involved the sale of the personal financial records of at least 163,000 consumers to unauthorized purchasers who turned out to be identity thieves,[104] the FTC and data broker ChoicePoint reached a stipulated settlement[105] requiring ChoicePoint to pay $10 million in civil penalties, and undergo security audits for the next twenty years. The "FTC allege[d] that ChoicePoint did not have reasonable procedures to screen prospective subscribers, and turned over consumers' sensitive personal information to subscribers whose applications raised obvious 'red flags,'" despite "receiving subpoenas from

[100] Bender, *supra* note 96 at 159. *See, e.g.*, *CollegeNet, Inc. v. XAP Corp*, Nos. 2009-1109, 2009-1458, 2009 WL 3169290, (Fed. Cir. Sept. 29, 2009).
[101] Press Release, FTC, Agency Announces Settlement of Separate Actions Against Retailer TJX, and Data Brokers Reed Elsevier and Seisint for Failing to Provide Adequate Security for Consumers' Data (March 27, 2008), http://www.ftc.gov/opa/2008/03/datasec.shtm.
[102] . FTC File No. 072-3055
[103] Press Release, FTC, *supra* note 101.
[104] Press Release, FTC, ChoicePoint Settles Data Security Breach Charges; to Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress: At Least 800 Cases of Identity Theft Arose From Company's Data Breach (Jan. 26, 2006), http://www.ftc.gov/opa/2006/01/choicepoint.shtm (at the time, the civil penalty was the largest in FTC history).
[105] *United States of America (for the Federal Trade Commission) v. ChoicePoint Inc.*, FTC File No. 052-3069.

law enforcement authorities alerting it to fraudulent activity going back to 2001."[106] In October 2009, ChoicePoint settled additional FTC charges that "the company failed to implement a comprehensive information security program protecting consumers' sensitive information," as was required by the 2006 settlement.[107] The new charges stemmed from an incident in which "a key electronic security tool used to monitor access to one of its databases" was turned off for the four months beginning April 2008, during which time "an unknown person conducted unauthorized searches of a ChoicePoint database containing sensitive consumer information, including [the] Social Security numbers" of approximately 13,750 consumers.[108]

Consumers caught up in data breaches and identity theft face risks to their financial and credit interests, medical insurance, physical safety, and even their very liberty that are difficult and time consuming to resolve.[109] In 2008, consumers who suffered identity theft spent an average of $739 dollars in out-of-pocket expenses to resolve damage done to an existing account, and an average of $951 to resolve problems stemming from new accounts being fraudulently opened under their names.[110] These amounts do not include financial losses due to fraudulent charges perpetrated using the compromised accounts.[111]

Sixty-nine percent of identity theft victims in 2008 reported that new lines of credit had been opened using their identities, and 39% reported that fraudulent charges had been posted to

---

[106] *Id.*
[107] Press Release, FTC, Consumer Data Broker ChoicePoint Failed to Protect Consumers' Personal Data, Left Key Electronic Monitoring Tool Turned Off for Four Months (Oct. 19, 2009), http://www.ftc.gov/opa/2009/10/choicepoint.shtm.
[108] *Id.*
[109] In 2008, victims of identity "reported spending an average of 58 hours repairing the damage done by identity theft to an existing account used or taken over by the thief," and an average of 156 hours to resolve problems caused by identity thieves opening new accounts using their personal information. *Id.* Thirty percent of victims of identity theft reported in 2008 indicated that it took them between 7 and 23 months to resolve all the problems caused by the theft of their personal information, and 20% reported needing more than 2 years to clear their names. *Id.*
[110] Identity Theft Resource Center, Identity Theft: The Aftermath 2008 (2009), *available at* http://www.idtheftcenter.org/artman2/uploads/1/Aftermath_2008_20090520.pdf.
[111] *Id.*

their credit card accounts.[112] One third of 2008's identity theft victims reported that fraudulent mortgages had been taken out using their personal information, 22% reported car loans, and 32% reported personal loans taken out this way.[113] Seventy percent reported that they were denied credit or had their credit cards cancelled as a result of identity theft.[114]

More than two thirds of victims of identity theft said in 2008 that they had been billed for medical services received by the identity thief. [115]

According to the facts in *Remsburg v. Docusearch, Inc.*, a stalker was able to purchase his victim's social security number and information on her place of work from Docusearch, Inc., a data broker, then later murdered her at her place of business and killed himself. [116] The New Hampshire Supreme Court subsequently held that data brokers can be liable for the harms caused by selling personal information.[117]

Fifty-six percent of victims of identity theft reported in 2008 that financial crime or fraud instigated by the identity thief resulted in a warrant in victim's name, and the same percentage indicated that the identity thief had been arrested, booked or arraigned under the identity of the victim.[118] One third reported that identity thieves had committed a non-financial crime and given the arresting officer the victim's name, and the same proportion indicated that the identity thief was prosecuted under the victim's identity, resulting in a criminal record in the victim's name.[119]

---

[112] *Id.*
[113] *Id.*
[114] *Id.*
[115] Identity Theft Resource Center, *supra* note 110.
[116] 816 A.2d 1001 (N.H. 2003).
[117] *Id.*
[118] Identity Theft Resource Center, *supra* note 110.
[119] *Id.*

Some federal laws cover data security for some sectors,[120] and the FTC is promulgating 'Red Flag Rules' to expand vigilance against identity theft to a wider net of commercial actors.[121] Even so, most online data harvesters and ad servers do not fall under these existing regulations, and therefore are not legally required to protect consumer's online data privacy, even if they might want to do so independently in order to avoid possible economic ramifications.

II. Despite these ramifications…Why do consumers acquiesce?

Despite the serious ramifications of data collection and use in online advertising, consumers who take all three approaches to protecting their online informational privacy appear to acquiesce in the online harvesting and use of their personal information. Why might this be so?

A. *Benefits To Consumers of Online Data Collection & Use*

Consumers who are tracked online do receive some benefits from the practice. The FTC notes that consumers "may benefit…from the free content that online advertising generally supports, as well as the personalization of advertising that many consumers appear to value."[122] According to the Industry SRP, "[o]nline behavioral advertising increasingly supports the convenient access to content, services, and applications over the Internet that consumers have

[120] For example, "Title V of the Gramm-Leach-Bliley Act of 1999 (GLBA) requires financial institutions to provide customers with notice of their privacy policies, and requires financial institutions to safeguard the security and confidentiality of customer information, to protect against any anticipated threats or hazards to the security or integrity of such records; and to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer." Gina Stevens, Legislative Attorney, Congressional Research Service, *Federal Information Security and Data Breach Notification Laws*, CRS 7-5700, 13, *available at* http://assets.opencrs.com/rpts/RL34120_20090129.pdf (citing 15 U.S.C. § 6801 – 6809).
[121] FTC, FTC Business Alert: New 'Red Flag' Requirements for Financial Institutions and Creditors Will Help Fight Identity Theft (June 2008), http://www.ftc.gov/bcp/edu/pubs/business/alerts/alt050.shtm. (The FTC's enforcement of the Fair and Accurate Credit Transactions (FACT) Act of 2003 requires financial institutions and 'creditors,' defined as any entity that regularly extends, renews, or continues credit, to implement programs to provide for the identification, detection, and response to patterns, practices, or specific activities that could indicate identity theft).
[122] FTC SRP, 1.

come to expect at no cost for them."[123] Harvesting of consumer data may result in making web navigation more convenient, since cookies and other technologies may enable a consumer's computer, browser, or web application to skip navigation steps by automatically filling in web forms, remembering bookmarked websites, and the like. Similarly, the data collected may be used to complete commercial transactions more efficiently. For example, consumers are able to complete online payment transactions at any time of day or night, simply by entering a (tracked) user name and password to access his or her bank account, PayPal account, etc.

Of most relevance to OBA, consumers may benefit from the receipt of more relevant online advertisements than they would otherwise receive. This "improved" marketing experience is the major consumer benefit promoted by OBA proponents.[124] In reality, whether the experience of the consumer is "improved" is dependent upon the consumer's subjective opinion of the invasiveness of the data harvesting required to provide targeted advertisements; the actual relevance of the targeted advertisements (i.e., the accuracy of the digital stereotyping conducted by adserving algorithms);[125] and the desire to be marketed to in the first place.

While proponents of OBA insist that consumers demand and desire more relevant

---

[123] Industry SRP, 1.

[124] Press Release, Yahoo!, Yahoo! Announces New Privacy Choice for Consumers (Aug. 8, 2008), http://yhoo.client.shareholder.com/press/releasedetail.cfm?ReleaseID=327212 ("Yahoo! strongly believes that consumers want choice when customizing their online experience and they have also demonstrated a strong preference for advertising that is more personally relevant to them") (quoting Ann Toth, Yahoo!'s head of privacy and vice president for policy). TRUSTe interprets the fact that "72 percent of those surveyed said they found online advertising intrusive and annoying when the products and services being advertised were not relevant to their wants and needs" to mean that consumers "prefer[] to be served targeted advertisements from brands they know and trust over irrelevant, intrusive advertisements," rather than to mean that consumers find online advertisements intrusive and annoying in general. Press Release, TRUSTe, Behavioral Targeting: Not that Bad?! TRUSTe Survey Shows Decline in Concern for Behavioral Targeting (Mar. 4, 2009), http://www.truste.com/about_TRUSTe/press-room/news_truste_behavioral_targeting_survey.html. The same TRUSTe survey showed that "[h]alf of all consumers still say they are uncomfortable with advertisers using their browsing history to serve them relevant ads, and many make concerted efforts to achieve anonymity when surfing the web." *Id.*

[125] *In re DoubleClick Inc. Privacy Litigation*, 154 F.Supp.2d 497, 503 (S.D.N.Y. 2001) (the advertising "server identifies the user's profile by the cookie identification number and runs a complex set of algorithms based, in part, on the user's profile, to determine which advertisements it will present to the user. It then sends a communication to the user with banner advertisements saying 'Here are the targeted banner advertisements….' Meanwhile, it also updates the user's profile with the information from the request.") (citations omitted).

advertising, empirical studies show that most consumers feel the potential benefits of behavioral advertising are outweighed by privacy concerns. A recent study found that "[c]ontrary to what many marketers claim, most adult Americans (66%) do not want marketers to tailor advertisements to their interests."[126] That proportion rose to 84% when the respondents heard that the advertisements would be targeted based on tracking them on other websites they visited.[127] A study by the Pew Research Center found that an "overwhelming majority of Internet users (84%) are concerned about businesses or people they don't know getting personal information about themselves or their families. Some 54% say they are 'very concerned.'"[128] Another "54% of Internet users believe that Web sites' tracking of users is harmful because it invades their privacy. Just 27% say tracking is helpful because it allows the sites to provide information tailored to specific consumers."[129] A 2009 TRUSTe survey reports that "50.5% of respondents say they're uncomfortable with advertisers using their browsing history to serve relevant ads, even when that information cannot be tied to their names or any other personal information. Only 30.6% said they would be comfortable having their browsing behavior captured by websites on which they've registered in order to improve user experience."[130] Empirical studies also indicate that, despite the vast consumer data underlying the targeting of OBA, most OBA advertisements are still not very relevant to their target consumer audiences. Despite OBA targeting efforts, eighty-three percent of respondents to the 2009 TRUSTe poll said "that less than 25% of the ads they see while browsing online are relevant to their wants and

[126] Joseph Turow, et al., *Americans Reject Tailored Advertising and Three Activities that Enable It* 3 (September 29, 2009), *available at* http://ssrn.com/abstract=1478214.
[127] *Id.* at 14-15.
[128] Fox, *supra* note 12.
[129] *Id.*
[130] TRUSTe, TRUSTe-TNS Study: Consumer Attitudes about Behavioral Targeting 3 (2009), available at http://www.truste.com/resources/index.html.

needs."[131]

Consumers' privacy concerns could certainly be allayed by outlawing online data collection for advertising purposes altogether, however doing so surely would not "balance the potential benefits of behavioral advertising against the privacy concerns"[132] of consumers, as the FTC seeks to do.

B. *Consumers Acquiesce Because They Are Unaware of the Practices*

Most consumer web users are unaware of the online collection and use of their personal information.[133] Indeed, although approximately 33% of all websites conduct data harvesting and OBA,[134] nearly 59% of Americans[135] and 55% of Californians[136] incorrectly believe that websites with a privacy policy cannot sell personal information without the data subject's consent. Although consumers arguably must be aware of the active collection of their personal information, it is more difficult for them to become apprised of passive methods of data collection. By definition, passive data collection is invisible to the naked eye. Even for tech-savvy consumers who may be aware that passive data collection is occurring, blocking or preventing such collection is logistically quite difficult.[137] Whether data is collected via active or passive methods, unless websites or adservers proactively give some notice of their practices, consumers may not be aware of the uses to which this data is put after it is collected. Some online commercial entities provide information regarding their consumer data collection and use

[131] *Id.*
[132] FTC SRP p. ii
[133] See, e.g., Andy Greenberg, *Not As Private As You Think: Users' confusion about their online privacy raises questions about whether the private sector will adequately protect personal data*, FORBES.COM (Sept. 25, 2008), http://www.forbes.com/2008/09/25/online-privacy-protection-tech-security-cx_ag_0925privacy.html.
[134] Whylly, *supra* note 16.
[135] Joseph Turow, Lauren Feldman, & Kimberly Meltzer, *Open to Exploitation: American Shoppers Online and Offline*, ANNENBERG PUBLIC POLICY CENTER OF THE UNIVERSITY OF PENNSYLVANIA (2005) *available at* http://www.annenbergpublicpolicycenter.org/NewsDetails.aspx?myId=31.
[136] Joseph Turow, Deirdre K. Mulligan & Chris Jay Hoofnagle, Research Report: Consumers Fundamentally Misunderstand the Online Advertising Marketplace (Oct. 2007), *available at* http://www.law.berkeley.edu/clinics/samuelson/annenberg_samuelson_advertising-11.pdf.
[137] See Section IV., *infra*.

in privacy policies; however it is questionable whether these policies provide sufficient notice to make consumers aware of the relevant practices. The FTC SRP and Industry SRP purport to address this problem of consumer awareness and notification by their "Transparency" and "Choice" provisions. See Part III below.

C. *Consumers Acquiesce Because They Have No Alternatives*

Even if consumers are made aware of the data collection and use practices of a particular online commercial entity, consumers are still generally faced with a 'take it or leave it' decision regarding the use of the online resources offered by these commercial entities. These resources are promoted as 'free,'[138] when in fact they are offered on a quid pro quo basis. While no money changes hands at the point of data collection or use for OBA, this 'free' content is provided in exchange for the surreptitious harvesting of consumer data: you(consumer) give us(data harvester) whatever personal data we can collect, and in exchange we give you X web-based content without monetary charge at the point of content delivery. Whether this quid pro quo is truly of net benefit to consumers is an open question.

The FTC SRP is an attempt to prompt industry actors to give consumers transparent notice of this quid pro quo exchange, and choice regarding whether consumers want to enter into this exchange. Presumably, the purpose of this notice and choice is to enable consumers to protect their own privacy, if they are motivated to do so. Part III examines whether the proposed self-regulatory schema actually provide consumers notice and choice, and whether the notice and choice that is provided is sufficient to enable consumers to protect their own privacy

[138] Online Publishers Association, Legislative Positions, http://www.online-publishers.org/legislative.php (noting that "overbroad restrictions on behavioral advertising could jeopardize publishers' ability to create and deliver high quality and free content on the Web"). The Official Google Blog, http://googleblog.blogspot.com/2009/03/making-ads-more-interesting.html (Mar. 3, 2009, 02:01:00 AM PST) ("At Google, we believe that ads are a valuable source of information….Users get more useful ads, and these more relevant ads generate higher returns for advertisers and publishers. Advertising is the lifeblood of the digital economy: it helps support the content and services we all enjoy for free online today, including much of our news, search, email, video and social networks").

interests.

III. FTC & Industry SRP guidelines do not enable consumers to protect their own personal information.

Currently, the only legally enforceable standards placed on OBA are those prohibiting the "unfair" and "deceptive" trade practices regulated by the FTC under Section 5 of the F.T.C. Act, as described above.[139] Thus, if consumers are to be empowered to protect their own privacy interests, their privacy interests must be enforceable under Section 5, or they must have a source of leverage over commercial online behavioral advertisers that is based on something other than the effect of legal process.

Even assuming consumers are aware of OBA practices and motivated to act to protect their privacy interests, consumers have no such other source of power. Consumers are not in a position to assert financial power to encourage online behavioral advertisers to change practices which they do not appreciate, either individually (through a personal boycott of an entity's website) or as a group (through a wide-spread boycott of an entity's website), since the value of one consumer's data points(or even several thousand consumers' data points) to a particular commercial entity is miniscule (as little as 2.5 cents)[140] in comparison to the overall value of OBA as a whole (approximately $23.4 billion dollars).[141] Even a widespread boycott of several thousand people would still leave the commercial web operator with a pool of 248.2 million

---

[139] 15 U.S.C. § 45.

[140] In a well publicized incident, in August 2008 Rene L. Rebollo Jr., a senior financial analyst at Countrywide's subprime lending arm was accused of selling the personal information of company clients over the course of two years, in batches of 20,000 about every week for $500 per batch, or 2.5 cents per personal record. Renae Merle, *Countrywide Says Customer Data Were Sold*, WASHINGTON POST, Sept. 14, 2008, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2008/09/13/AR2008091300337_pf.html.

[141] Press Release, Interactive Advertising Bureau, Internet Advertising Revenues Surpass $23 Billion in '08, Reaching Record High, http://www.iab.net/about_the_iab/recent_press_releases/press_release_archive/press_release/pr-033009 ("Full-year 2008 revenues [for internet advertising] totaled a record $23.4 billion, exceeding 2007's performance, itself the former record of $21.2 billion, by $2.2 billion or 10.6%).

potential data subjects nationwide.[142] Given that consumer's attempts to assert their political power to prompt regulation of OBA through binding legislation have so far failed,[143] and OBA practitioners' have successfully avoided binding federal regulation of their industry, it is apparent that consumers' political power is not sufficient to protect their own privacy interests through the federal political system.

Consumers are not able to physically or technologically prevent their privacy interests from being threatened through OBA.[144]

Since consumers' have no inherent financial, physical/technical, or political power over OBA practitioners, their privacy interests will only be legally protected if these interests have the protection of the FTC through its Section 5 authority. The FTC's ability to act to protect consumer's privacy interests derives from its ability, under their Section 5 authorization, to prevent unfair trade and deceptive trade practices. In practice, the FTC is only able to protect consumer's privacy interests by forcing commercial entities to comply with their own privacy policies. The FTC explicitly notes in their February 2009 staff report that they will seek

---

[142] Chart, Internet Users in North America: United States, http://www.internetworldstats.com/stats14.htm.

[143] There is a possibility that the legislative approach of Congress may change soon, following additional congressional hearings in recent months. *See, e.g.*, *Communications Networks and Consumer Privacy: Recent Developments: Hearing Before the Subcomm. on Communications, Technology, and the Internet of the H. Comm. on Energy and Commerce*, 111th Cong. (April 23, 2009) (focusing on "technologies that network operators utilize to monitor consumer usage and how those technologies intersect with consumer privacy. The hearing explored three ways to monitor consumer usage on broadband and wireless networks: deep packet inspection (DPI); new uses for digital set-top boxes; and wireless Global Positioning System (GPS) tracking"); *Aggressive Sales Tactics on the Internet and Their Impact on American Consumers: Hearing Before the S. Comm. on Commerce, Science & Transportation*, 111th Cong. (Nov. 17, 2009) (statement of John D. Rockefeller, IV, Member, S. Comm. on Commerce, Science & Transportation) (regarding online scams involving transferring consumer data from "online businesses that have each made more than a million dollars through sharing their customers' credit card information with internet scammers….[s]tarting with this hearing today, I think this Committee needs to start thinking about the legislative steps we can take to end these practices"); Emily Steel, *Evaluating Offline Privacy --- Policy Makers' Concerns Spread Beyond the Internet*, WALL STREET JOURNAL, Nov. 19, 2009, *available at* http://online.wsj.com/article/SB10001424052748704533904574543400320693232.html ("Rep. Rick Boucher [D., Va.], chairman of the Subcommittee on Communications, Technology and the Internet. Rep. Boucher says he is preparing legislation that would force Web sites to disclose the information they are collect about their visitors and clearly state how it is used. It also would give consumers an easy way to say no to its collection. 'A number of parties have suggested it would be appropriate to extend these privacy rights as a consumer protection to the offline side as well,' Rep. Boucher says").

[144] See Section IV.

enforcement of company's own privacy policies: "[r]egardless of the scope of the Principles,… companies must adhere to the promises they make regarding how they collect, use, store, and disclose data."[145]

Thus, if consumers are to be able to protect their own privacy interests within the current self-regulatory regime, (A) the entities collecting and using the relevant data must have a privacy policy; (B) the consumer must be able to locate the privacy policy and its relevant terms; (C) the consumer must be able to read and understand the privacy policy; (D) the consumer must have the opportunity to consent to, or avoid consenting to, the terms of the privacy policy; (E) the content of the privacy policy must favor protection of consumer information, such that the result of the entity's compliance with its own policy will be the consumer's ability to act to protect his or her own informational privacy interests; and (F) the guidelines of the self-regulatory schema must be enforceable.

A. *Do online commercial entities engaged in OBA have privacy policies?*

If consumers are to receive notice and choice regarding an OBA company's data collection and use practices, these practices must be described somewhere. FTC SRP and Industry SRP recommend that these practices be described in a privacy policy. Although the FTC is technically unable to force OBA entities to have privacy policies,[146] the vast majority of online commercial entities do have some form of written privacy policy.[147] The content and efficacy of such privacy policies is especially important, since most Americans erroneously believe that the mere presence of a privacy policy indicates that their privacy interests are legally

[145] FTC SRP p. iii
[146] Michael D. Scott, *The FTC, The Unfairness Doctrine, and Data Security Breach Litigation: Has the Commission Gone too Far?*, ADMIN. L. REV. 3 (2008) (although the FTC has "the power under § 5 of the FTC Act to pursue deceptive practices, such as a website's failure to abide by a stated privacy police…it could not require companies to adopt privacy policies in the first place").
[147] Allyson W. Haynes, *Online Privacy Policies: Contracting Away Control Over Personal Information?*, 111 PENN. ST. L. REV. 587, 593-594 (2007).

protected.[148]

B. *Insufficient notice? Can consumers find the privacy policies?*

If consumers are to protect their own privacy interests, they must at least be able to find a company's privacy policy. That is, to be aware of a company's data collection and use practices, notice of such practices must be "clear, concise, consumer-friendly, and prominent."[149] In the past, the FTC's previous guidance regarding what constitutes effective notice of disclosures required that such disclosures be "clear and conspicuous."[150] Whether a disclosure is clear and conspicuous has generally been determined based on a variety of factors, including the presentation of the information in understandable language, the placement of the disclosure in a format that consumers will read, whether the disclosure is located in proximity to the claim that it is meant to explain, and whether the disclosure is "prominent enough for consumers to notice it and read…it."[151] It is unknown whether the FTC will interpret "clear and prominent" disclosures to require the same level of notice to consumers as "clear and conspicuous" disclosures have required in the past, or whether this change in vocabulary signals a change in the substantive standard to be applied to online disclosures in the context of FTC enforcement.

The Industry SRP suggests that those third-party OBA entities covered by the Industry SRP provide consumers with a "clear, meaningful, and prominent notice" that describes "the types of data collected and their uses, [and provides] an easy to use mechanism for exercising choice not to permit the collection and use of data for [OBA] purposes, or the transfer of the data

[148] Whylly, *supra* note 16 (59% of Americans surveyed falsely believed that websites with a privacy policy cannot sell personal information without the data subject's consent).
[149] FTC SRP, 46.
[150] *See, e.g.*, *FTC v. Cyberspace.com*, 453 F.3d 1196 (9th Cir. 2006) (fine print statement on faux rebate check was not sufficient to indicate clearly and conspicuously that cashing the check would initiate monthly internet access charges).
[151] Pamela Jones Harbor, Commissioner, FTC, *Advertising and Unfair Competition: Federal and State Enforcement*, SP050 ALI-ABA 449, 455.

to a non-Affiliate for such purposes."[152] The Industry SRP suggests that third party OBA entities should apprise consumers of the notice either by linking "to it from a location in or around the advertisement on the Web page where the data is collected…or from a location on the Web page where data is collected."[153] Alternatively, third parties could comply with the Industry SRP's notice requirements by having "its name(s) listed either on the industry-developed Web site(s) linked from [the consumer's ISP's disclosure page], or, if agreed to by the First Party, individually listed in the disclosure on the Web site where the Third Party collects data for use for [OBA] purposes."[154] While such notices would likely be a dramatic improvement over the current scenario – in which third party entities that most consumers have never heard of only provide privacy policy disclosure from their own homepages, if at all – this approach still requires consumers to look for the relevant privacy disclosures in a minimum of four places on different websites throughout the internet. Additionally, it is unclear from the text of the Industry SRP whether the link "in or around the advertisement" would also cause the clicking consumer to have their clickstream data tracked via a web bug implanted in the advertisement. If so, such a practice would, of course, raise the privacy concerns described above in relation to such passive data collection.

Presently, although most websites have privacy policies, not all of these policies are located in clear and prominent places. Of the top twenty-five websites with the most U.S. traffic, only 68% of the privacy policies were "conspicuous," defined as "any link to a company's privacy policy…containing the word 'privacy,'…appearing somewhere on a company's homepage,…published in a font at least as large as any other links in the vicinity, and ...likely to

[152] Industry SRP, 30.
[153] Industry SRP, 31.
[154] *Id.*

appear to a Web site visitor upon first glance."[155] Thus, despite its faults in other areas, the Industry SRP's suggestions regarding the placement and presentation of disclosure notices in and around advertisements would be an improvement over the current state of affairs.

C. *Can consumers read and understand the terms of the privacy policies?*

The self-regulatory approach is predicated on the idea that consumers should be able to operate in the free market to protect their privacy interests by "survey[ing] the available alternatives, choos[ing] those that are most desirable, and avoid[ing] those that are inadequate or unsatisfactory."[156] In order to educate themselves on what types of privacy protections website operators provide, they must first read the website's privacy policies. Unfortunately, it is almost physically impossible for consumers to read the privacy policies of each website they visit. If consumers wanted to read the privacy policy of each website they visited one time each year, each web user would have to spend 244 hours per year (40 minutes per day) doing so.[157] By comparison, the average web user spends a total of 72 minutes online each day.[158] The self-regulatory approach therefore requires that consumers use about 55% of their internet time reading privacy policies. Economically speaking, the opportunity cost of reading the privacy policy of each website that consumers visited once per year would be $781 billion nationally.[159] By comparison, the estimated value of U.S.-based OBA in 2009 is $23.4 billion dollars.[160] The success of the self-regulatory approach is consequently predicated on the idea that, in the

[155] Ciocchetti, *supra* note 53 at 587, 599.
[156] Pertschuk, *supra* note 5 at 1070.
[157] Aleecia M. McDonald and Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J.L. & POL'Y FOR INFO. SOC'Y 543, 563, 565 (Winter 2008-2009) ("These estimates presume that people visit sites, read the policies once a year, and then carry on their business as before….The true cost of adherence to the self-regulation vision is perhaps on the order of double the costs we estimate, depending on…how many sites people are expected to compare").
[158] *Id.* at 563.
[159] *Id.* at 565.
[160] Press Release, Interactive Advertising Bureau, *supra* note 141 ("Full-year 2008 revenues [for internet advertising] totaled a record $23.4 billion, exceeding 2007's performance, itself the former record of $21.2 billion, by $2.2 billion or 10.6%).

national aggregate, American consumers should expend $757.6 billion more on reading privacy policies than the entire OBA industry is worth. This seems a shaky economic proposition to build consumer privacy protections upon.

Even if they were physically able to read the privacy policies of each website they visited, many consumers would not be able to understand the terms of the privacy policies they found there. Privacy policies use legalese, euphemisms, and vague terms that are difficult for most consumers to understand. For example, even the U.C. Berkeley law students conducting research into compliance with California's required disclosure law found them mystifying: "Privacy policies are so confusing that in some cases, our students did not fully understand the responses."[161] One survey found that 32% of the privacy policies of the top twenty-five websites used terminology that was unclear.[162] An easy solution to this problem would be to require OBA entities to use "plain English" to draft their privacy policy disclosures. "Plain English" is a standard in use by the Securities and Exchange Commission and is required to be used in some of mandatory regulatory disclosures in that field.[163] "Plain English" is meant to "eliminate writing styles and phrasing that the average citizen struggles to understand."[164] Writing in "plain English" involves avoiding "long sentences, passive voice,…legal and financial jargon, numerous defined terms, abstract words,…and unreadable design and layout."[165] Since this standard is already in use in commercial and financial disclosures, the standard is not unfamiliar to corporate attorneys, and there seems no valid reason why internet companies' privacy policy disclosures should not be held to the same standard of clarity.

---

[161] Chris Jay Hoofnagle and Jennifer King, Consumer Information Sharing: Where the Sun Still Don't Shine, U.C. Berkeley School of Law, http://www.law.berkeley.edu/samuelsonclinic/files/sb27report.pdf.
[162] Ciocchetti, *supra note 50 at* 588, 598.
[163] *Id.* at 588.
[164] Corey A. Ciocchetti, *The Future of Privacy Policies: A Privacy Nutrition Label Filled with Fair Information Practices*, 26 J. MARSHALL J. COMPUTER & INFO. L. 1, 16 (2008).
[165] *Id.* at 16-17.

D. *Can (and do) consumers effectively consent to the terms of the privacy policies?*

Many privacy policies incorporate, or are incorporated by reference into, the OBA entity's terms of service.[166] These terms of service generally state that the consumer's use (or continued use) of the OBA entity's website or service indicates that the consumer assents to the data harvesting and use methods included in the entity's privacy policy. However, depending upon the method of passive data collection, data harvesting can begin the moment a consumer's web browser accesses a website (or, in the case of DPI, the moment the consumer's computer accesses the network). Since most posted privacy policies are accessed by a hyperlink from the first party's homepage,[167] data harvesting inevitably begins before the consumer could possibly have read the privacy policy: i.e., before knowing consent could possibly have been gained.

Case law differs on whether the presence of such privacy policies constitutes contractually binding assent via "browse-wrap." Browse-wrap scenarios involve purported unilateral contracts "where terms and conditions are posted on a website but no specific act of acceptance…is required" for the terms to bind visitors to the website.[168] Some courts have found that consumers did not or could not express the requisite intent to be bound when a company attempted to unilaterally change the terms of an agreement by posting the changed terms online with no additional notice to its customer;[169] when the consumer could have finished an application process without having to view the user agreement;[170] when the consumer was not

[166] *See, e.g.*, Google Terms of Service, http://www.google.com/accounts/TOS (For information about Google's data protection practices, please read Google's privacy policy at http://www.google.com/privacy.html. This policy explains how Google treats your personal information, and protects your privacy, when you use the Services….You agree to the use of your data in accordance with Google's privacy policies).
[167] Ciocchetti, *supra* note 164 at 14-15.
[168] Andre R. Jaglom, *Internet Distribution, E-Commerce and other Computer Related Issues: Current Developments in Liability On-line, Business Methods Patents and Software Distribution, Licensing and Copyright Protection Questions*, SP050 ALI-ABA 541, 619 (2009).
[169] *Douglas v. U.S. Dist Ct. C.D.Cal. and TalkAmerica, Inc*., 495 F.3d 1062 (9th Cir. 2007).
[170] *Comb v. Paypal, Inc.*, 218 F.Supp.2d 1165 (N.D. Cal. 2002).

required to read each page of the terms of service in order to use the service;[171] and when a consumer was able to download software without having to affirmatively indicate acceptance of the disputed terms, and notice of the purported contract's existence was only visible if the consumer scrolled to the bottom of the web page.[172] On the other hand, browse-wrap terms were enforced where the website's homepage included prominent notice that use of the interior pages was only permitted upon acceptance of the terms and conditions, and there was evidence that the defendants had knowledge of said terms.[173]

Thus, it is unclear whether a consumer's mere use of a website that contains a link to a privacy policy is sufficient to find that the consumer assented to the privacy policy's terms, particularly terms allowing OBA entities to harvest and use his or her personal data. Conversely, it is unclear whether an OBA entity's failure to comply with its own posted privacy policy would constitute sufficient grounds for a breach of contract action.

The FTC SRP requires that "before a company can use previously collected data in a manner materially different from promises the company made when it collected the data, it should obtain affirmative express consent from affected consumers."[174] Similarly, the Industry SRP suggests that if an OBA entity wants to amend its privacy policy to use, "for materially different Online Behavioral Advertising purposes, data collected from individuals prior to the material change, the Principle requires the entity to obtain Consent from the affected individuals…before the entity uses the previously collected data for the materially different [OBA] purposes."[175]

Unfortunately, the SRPs' notice, amendment, and choice requirements appear to be

[171] *Strujan v. AOL*, No. 055175/05, 2006 WL 1452778 (N.Y. Civ. Ct. May 19, 2006).
[172] *Specht v. Netscape Communications Corp.*, 306 F.3d 17 (2d Cir. 2002).
[173] *Ticketmaster Corp. v. Tickets.com, Inc.*, 2003 U.S. Dist. LEXIS 6483 (C.D. Cal. Mar. 7, 2003).
[174] FTC SRP, 47.
[175] Industry SRP, 38-39.

internally inconsistent. Does the fact that the FTC and Industry SRP places the burden to opt-out on consumers imply that consumer's mere ability to view privacy policies constitutes assent to the OBA company's privacy policy terms? In other words, does failure to opt-out after being presented with a hyperlink titled "privacy policy" constitute a consumer giving consent to an OBA entity to use that consumer's personal information in any manner the OBA entity chooses, so long as the OBA entity provides notice of its intent to use the consumer's personal information for targeted marketing online in the body of the hyperlinked privacy policy, whether or not the consumer has actually followed the link to read the privacy policy?

If so, it appears that the FTC and Industry SRPs endorse the idea that browsewrap terms of service are enforceable, even absent actual knowing consent. This would constitute a significant departure from the long standing common law and constitutional doctrine of freedom of contract, which includes the freedom from contract,[176] and might therefore have severe consequences in other areas of consumer and commercial law. In addition, if this form of 'notice' is sufficient to notify the reasonable consumer of their supposed assent to the use of their harvested personal information in the first place, why does the FTC SRP require additional opt-in consent for post-amendment use of previously harvested data? If browse-wrap is sufficient for initial notice, why not for subsequent notice?

On the other hand, if this form of 'notice' is not sufficient to notify the reasonable consumer of their supposed assent to the use of their harvested personal information, then this inconsistency seems to be an implicit admission that posting a privacy policy covering OBA practices (or even providing a hyperlink to it in served ads), is insufficient notice of the content of said privacy policy in the first place. By this standard, such browse wrap privacy policies

[176] *Blue Cross & Blue Shield Mut. of Ohio v. Blue Cross and Blue Shield Ass'n*, 110 F.3d 318 (C.A.6.Ohio 1997) (Freedom of contract entails freedom not to contract).

cannot bind consumers whose personal information is harvested and used according to the privacy policy's terms. The FTC SRP's requirement that OBA entities seek affirmative consent for the use of harvested information post-amendment would therefore be incongruous, since presumably consumers being asked to subsequently opt-in did not give their assent to the precedent data collection in the first instance. In other words, upon the amendment of an OBA entity's privacy policy, the FTC SRP seems to require OBA entities to ask consumers/data subjects: May we please have your express consent to use for additional online marketing purposes information that we previously collected from you without your consent and are already using for some online marketing purposes? This type of request for affirmative consent lacks meaningful substance from the consumer perspective.

Alternatively, under the FTC SRP guidelines, after amending its privacy policy (or just before doing so), an OBA entity could merely discard (or sell off) all data collected under the earlier privacy policy's terms, and start afresh with a new round of data harvesting and use. This would mean that none of the data collected under the less invasive terms would be used for the more invasive purposes, and for that reason would require no affirmative consent from the data subject/consumer whose personal information is affected.[177] If OBA entities choose to use this approach, consumers will only be 'protected' by the general opt-out option: that is, consumers will face the Catch 22 of browse wrap service 'contracts' whose terms may or may not be enforceable, and may or may not provide consumers with any privacy protections.

The FTC SRP also requires opt-in consent before OBA entities may collect and use particular types of 'sensitive' information that consumers are likely to want to protect most vociferously. However, the FTC's definition of "sensitive information" is itself too vague to be useful. According to the FTC, "[w]hat constitutes sensitive data… may often depend on the

[177] FTC SRP, 47.

context," but at minimum includes "financial data, data about children, health information, precise geographic location information, and Social Security numbers."[178] These categories appear to parallel some of the types of information already protected under COPPA, HIPPAA, and so on, but do not exactly match their scope. For example, under this rubric, do search queries for vitamins count as health information? What constitutes "precise" for the purposes of harvesting location data? Does "data about children" include whether or not an adult is a parent? The FTC has provided no further guidance on this topic. Given the FTC's vague definition, there appears to be no way for a consumer to know or to find out whether a particular data point is "sensitive" and therefore automatically kept private, requiring opt-in to allow its collection and use; or whether it is non-sensitive and therefore automatically fair game for harvesting, requiring opt-out to prevent its collection.

The Industry SRP narrows the definition of what constitutes "sensitive data" to cover personal information harvested from children that is already subject to COPPA protections, "financial account numbers, Social Security numbers, pharmaceutical prescriptions, or medical records about a specific individual."[179] Although this definition is more precise, it does not cover the range of personal information that the FTC suggests should be granted special protection. For example, by the plain terms of this definition, while the harvesting of a consumer's checking account number would require opt-in permission, harvesting the retail location and amounts of debit card purchases conducted using that account apparently would not require such permission. This type of loophole is the sort that would lead a reasonable consumer to erroneously think a wider range of his or her personal information is protected by the opt-in provision, whereas in reality in order to protect such information he or she would have to

[178] FTC SRP, 44.
[179] Industry SRP, p. 16-17

proactively opt-out. It is unclear whether semantic evasions such as these would constitute a type of systematic deception actionable under Section 5 of the FTC Act.

Assuming OBA entities comply with the SRPs and proactively seek consumers' affirmative assent to harvest and use their sensitive information for OBA, and to use the data for additional OBA subsequent to an amendment in their privacy policies, how will this affirmative assent be gained? The FTC SRP merely suggests that OBA websites "provide consumers with a clear, easy-to-use, and accessible method for exercising this option." [180] The Industry SRP is similarly vague, only defining the "Consent" required before using sensitive information. According to the Industry SRP, consent means "an individual's action in response to a clear, meaningful, and prominent notice regarding the collection and use of data for Online Behavioral Advertising purposes."[181] Since there are presently no functional mechanisms to seek assent from consumers for the use of their 'sensitive' personal information for OBA, it is impossible to assess how such mechanisms might work. However, if consumers are voluntarily entering into hard copy, click-wrap or other enforceable electronic contracts consumers with OBA entities, and the terms of these contracts allow for the use of 'sensitive' information for OBA purposes, then consumers may already be opting-in in this way.

E. *Consent to what? The content of privacy policies*

The FTC can only enforce compliance with the content of OBA entities' own privacy policies. [182] Therefore, if consumers' privacy interests are to be protected, the terms of the commercial entities' privacy policies themselves must provide such protection. The FTC SRP suggests only that a privacy policy should exist, that it be clearly and prominently placed, and

[180] FTC SRP, 46.
[181] Industry SRP, 23.
[182] Scott, *supra* note 146 at 3 (although the FTC has "the power under § 5 of the FTC Act to pursue deceptive practices, such as a website's failure to abide by a stated privacy policy…it could not require companies to adopt privacy policies in the first place").

that it alert consumers that "data about consumers' activities online is being collected at the site for use in providing advertising…tailored to consumers' interests, and…[that] consumers can chose whether or not to have their information collected for such purpose."[183] However, beyond this, the FTC SRP recommends no particular content for OBA entities' privacy policies. The Industry SRP requires no particular wording, but suggests that OBA disclosures "should be clear, meaningful, and prominent, and describe the types of data collected and their uses, as well as an easy to use mechanism for exercising choice [regarding] the collection and use of the data for [OBA] purposes, or the transfer of the data to a non-Affiliate for such purposes.[184] Most privacy policies today are filled with legal loopholes, such as warranty disclaimers, limitations of liability, forum selection clauses, arbitration clauses,[185] and catch-all clauses indicating that information may be collected "from or about you in ways not specifically described here."[186] Thus, if OBA entities comply with the Industry SRP OBA policy content requirements, this will go some way toward enabling consumers to understand the content of the privacy policies which purport to determine consumers' ability to protect their own privacy interests online.

However, because, under the self-regulatory approach there are no legally binding restrictions on or affirmative requirements for the content of privacy policies, an industry-friendly, broadly permissive, but non-deceptive privacy policy might simply state:

> We reserve the right to collect any data about you, our web visitors, that we can – through voluntary submission of web forms, cookie placement and tracking, web beacons, and any other means that are technologically possible now or may become possible in the future. We reserve the right to use the data we collect about you for whatever purposes we deem convenient, including, but not limited to, completing transactions that you initiate, providing you with targeted advertisements, and disseminating such data to third parties without further notice

[183] FTC SRP, 46. See Section III.B., *supra*.
[184] Industry SRP, 30.
[185] Haynes, *supra* note 147 at 595-597, 613.
[186] PayPal, Privacy Policy: Last Update: Oct 14, 2009, https://cms.paypal.com/cgi-bin/marketingweb?cmd=_render-content&content_ID=ua/Privacy_full&locale.x=en_US.

> to you or consent from you. If you would like to opt out of our use of collected data to provide you with targeted advertisements, you may do so ***here***. Even if you opt out of our use of collected data to provide you with targeted advertisements, we reserve the right to collect data as described above and use it for other purposes. Though we may attempt to notify you of any changes to this privacy policy by posting it on this website, we reserve the right to alter this privacy policy without notice.

Such a privacy policy would be in complete compliance with both the FTC and Industry SRPs, yet would provide no consumer privacy protection at all.

F. *Can consumers enforce privacy policies under the self-regulatory regime?*

Assuming that privacy policies make any promises to protect consumer information, it is unlikely that consumers will be able to force OBA entities to keep these promises. The FTC SRP calls on industry to "redouble its efforts in developing self-regulatory programs, and also to ensure than any such programs include meaningful enforcement mechanisms."[187] The Industry SRP also urges "entities participating in the development of these Principles to develop and implement policies and programs to further advance the Prinicples," and "calls for [these] programs to have mechanisms by which they can police entities engaged in [OBA] and help bring these entities into compliance."[188] The Industry SRP suggests that enforcement programs at least allow consumers to complain of instances of non-compliance, "publicly report instances of non-compliance and refer entities that do not correct violations to the appropriate government agencies."[189] However, instances of non-compliance that are corrected may be publicly reported "without identifying the entity whose practices were in violation of the Principles."[190] The Industry SRP aims to have such programs in place "at the beginning of 2010," however as of today's date (December 1, 2009), there has been no word that such programs have been initiated.

[187] FTC SRP, 47.
[188] Industry SRP, 41-42.
[189] *Id.* at 41.
[190] *Id.*

It is therefore unclear what enforcement of the Industry SRP would mean in practice, although the Council of Better Business Bureaus (BBB) has an existing structure for dealing with customer service concerns outside of government enforcement structures,[191] and has indicated that it will be involved in the complaint resolution process.[192]

It is unclear from the FTC's existing commentary how the FTC intends to treat the forthcoming Industry complaint mechanisms. Will the Industry SRP complaint mechanism be treated as a substitute for FTC complaint procedures? As a supplement to existing FTC complaint procedures? Will the consumer be expected to pursue an Industry SRP complaint first, before the FTC will act? In other words, are the proposed Industry SRP complaint and enforcement mechanisms yet another barrier to effective protection of consumers' privacy interests?

As the FTC notes, "[s]elf-regulation can work only if concerned industry members actively monitor compliance and ensure that violations have consequences."[193] That is, under the present self-regulatory schema, consumers' privacy interests are only protected if the very entities that stand to profit from the exposure of their personal information do a good job of preventing its exposure, and punish themselves if they do a bad job. Asking the industries whose

---

[191] BBB, Before you begin filing your complaint with BBB please note, https://odr.bbb.org/odrweb/public/getstarted.aspx ("BBB's goal is to successfully resolve complaints involving buyers and sellers in a fair and timely fashion. This includes complaints involving consumer-to-business… transactions that involve the advertisement and/or sale of a product or service…. BBB generally does not handle complaints which are more effectively handled by other government or private agencies or the legal system, such as complaints involving employment practices, discrimination, or matters in litigation….Your complaint will be forwarded to the company within two business days. The company will be asked to respond within 14 days, and if a response is not received, a second request will be made. You will be notified of the company's response when we receive it [or notified that we received no response]. Complaints are usually closed within 30 calendar days").

[192] Press Release, Better Business Bureau, Principles on Collection and Use of Behavioral Advertising Data Released, (July 2, 2009), http://www.bbb.org/us/article/principles-on-collection-and-use-of-behavioral-advertising-data-released-11287 ("The Council of Better Business Bureaus is delighted to join this effort…. We think that what is most important about this effort is the real commitment by a broad coalition of businesses joining in to deliver a transparent and credible monitoring and enforcement program…. We look forward to working closely with the DMA and our other National Advertising Review Council partners to deliver a quality program").

[193] FTC SRP, 47.

business models depend on the use of consumer data for OBA to be self-accountable and enforce their own privacy policies is tantamount to trusting the fox to guard the henhouse. More specifically, the major incentives surrounding OBA practices all tend away from protecting consumers' privacy interests. "Today's thriving market rewards companies who collect data while remaining invisible. This skewed incentive structure inspires firms to be less transparent and avoid consumer complaints by hiding their behavior, instead of actually taking measures to ensure adequate protection."[194] Alternatively, since OBA entities may only face legal accountability when their consumer data practices differ from the terms of their privacy policies, OBA companies may simply avoid liability by including catch-all phrases in their privacy policies that cover every conceivable instance of data collection and use, as in the above sample. A recent assessment of how companies should approach compliance with varying data privacy laws among European Union countries is illustrative: "Prioritization is key: the company must figure out what to do first to most cost-effectively meet its objectives, based on a wide range of factors, including…countries that have particularly strict or specific legal requirements or have particularly active data protection authorities enforcing the law (with correspondingly serious consequences for violations)."[195] By this measure, compliance with U.S.-based self-regulatory regimes – with no specific legal requirements, no dedicated data protection authorities, and no laws to enforce (with correspondingly minimal consequences for violations) – should be very low on a corporate privacy officer's to-do list.

Beyond the illogical financial incentives underlying self-regulation, a consumer who wanted to go beyond reliance on OBA entities' self-enforcement to attempt to limit the OBA

[194] Richard M. Marsh, Jr., *Legislation for Effective Self-Regulation: A New Approach to Protecting Personal Privacy on the Internet*, 15 MICH. TELECOMM. & TECH. L. REV. 543, 554 (2009).
[195] Ruth Hill Bro, *Titanic Privacy Mistakes: Icebergs Looming for Multinational Companies*, THE SCITECH LAWYER 17 (Fall 2009).

entity's use of that consumer's personal information to those purposes noted in the OBA entity's privacy policy would face significant practical obstacles to doing so. Under both the FTC and Industry SRPs, there is still no requirement that first-parties disclose the name or contact information of third parties to whom consumers' info has been sold, transferred, or shared. Because of this there is no real way for consumers to opt out of data harvesting by *all* third parties who may be given access to a particular consumer's personal information.

California residents may gain some assistance in seeking disclosure of third party data transfer from SB 27, the "Shine the Light" law. [196] Passed in 2003, SB 27 was intended to address this very issue, and created a right to access and limit the use of personal information that "allows any Californian to make a request to almost any business for a disclosure of how individuals' information is used for secondary marketing purposes."[197] Within thirty days of a request for information from a consumer with whom they have a business relationship, businesses must either provide such disclosures or offer Californian consumers an opportunity to opt-out of the practice of sharing their personal information with third parties for marketing purposes. Unfortunately, the level of compliance with the law is low. Of eighty-six test requests made as part of a study by researchers at University of California Berkeley School of Law, only twenty-four companies who share data with third parties responded properly by providing the requesting consumer with either a list of entities with whom they shared consumer information for marketing purposes, or with an opportunity to opt out.[198] Almost the same number did not comply properly. Ten companies did not respond at all to requests sent to the address designated by the company for this purpose, and nine others "refused to comply with the law, [inaccurately] claiming either that no established business relationship existed, or that the requestor was under

[196] 2003 Cal. SB 27, codified at Cal. Civ. Code § 1798.83-84.
[197] Hoofnagle, *supra* note 161.
[198] *Id.* at 10.

an affirmative duty to prove that one existed."[199] An additional forty-three companies responded by indicating that they did not sell customer's personal information to third parties for marketing purposes without the customer's consent.[200] However, the content of the responses of those companies that did share consumer's personal information with third parties for marketing purposes "demonstrated policies that contravene consumers' expectations at best."[201] For example, Ann Taylor responded to the SB 27 request merely by providing a copy of the company's privacy policy. The policy first "promises not to sell data collected online, but later states that information can be shared with 'specially chosen marketing partners.'"[202] Regarding the SB 27 opt-out requirement, although Ann Taylor's privacy policy indicates that "the company does offer an ability to opt out of Ann Taylor emails[,]…a careful reader will notice that no mention is made whether this also restrains information sharing with third parties."[203] Thus, even when there is extant legislation requiring companies to provide consumers with informational tools that empower them to protect their own privacy interests, only 55% of companies who use the transfer of consumer's personal information as a revenue stream properly comply. Given the financial incentives discussed above, it is reasonable to expect a far lesser proportion will properly comply with the FTC and Industry SRPs' non-binding self-regulatory guidelines.

If the self-regulatory schema break down, are ineffective, or simply insufficient in scope, consumers have no private right of action to bring suit to force OBA entities to comply with their own privacy policies, absent a showing of actual damages.[204] Given the difficulty of discovering

[199] *Id.* at 11.
[200] *Id.* at 10.
[201] *Id.* at 15.
[202] *Id.* at 16.
[203] *Id.* at 14-15.
[204] Though there have been few suits brought to limit OBA entities' use of personal information, several such suits have failed at least in part because plaintiffs failed to allege or prove damages. See, e.g., *In re American Airlines,*

which entities collect, transfer, and use a particular consumer's personal information in the first place, showing that such entities caused actual harm to consumers physical, emotional or property rights would likewise be very difficult. Thus, in most instances, the FTC is the only party with standing to bring suit.[205] The FTC has finite resources and of course cannot address or resolve all consumer complaints. As a result, only OBA entities with a high volume of complaining customers or viewers, and/or OBA entities whose egregious practices are widely publicized are really at risk of facing action by the FTC. Most smaller-volume consumer complaints regarding privacy violations will likely go un-addressed for some time, if they are taken up by the FTC at all. In effect, to legally enforce their rights, consumers must submit their complaints to the FTC, cross their fingers that enough other consumers also have their privacy violated to catch the FTC's attention, and then wait for the FTC to get around to acting on the complaints. In the meantime, improper data harvesting and use can continue unchecked, even though these violations may have serious detrimental effects for consumers acting reasonably in the circumstances, who are misled by the representations or practices of OBA entities described above.

IV. Can consumers use technological fixes to fix the self-regulatory regime?

Both the FTC and Industry SRPs recommend that consumers be able to exercise choice regarding whether they would like to continue to have their harvested data used for OBA purposes through opt-out mechanisms provided by the OBA entities themselves.[206] However, both SRPs are silent regarding the technical means by which consumer opt-out will or should be

---

Inc., Privacy Litigation, 370 F.Supp.2d 552 (N.D. Tex. 2005) (dismissing breach of contract claims based on privacy policy because passengers failed to allege damages); *In re Northwest Airlines Privacy Litigation*, No. Civ.04-126 (PAM/SJM), 2004 WL 1278459 (D. Minn. June 6, 2004) (finding that plaintiffs failed to allege damages); *In re Jetblue Airways Corp. Privacy Litigation*, 379 F.Supp.2d 299 (E.D.N.Y. 2005) (dismissing breach of contract claims based on privacy policy because plaintiff failed to allege actual damages).

[205] *See* 15 U.S.C. §53 (authorizing the FTC to file suit in federal court to enjoin practices that violate provisions of law otherwise enforceable by the FTC).

[206] FTC SRP, 46; Industry SRP, 34.

achieved.

One larger scale opt-out system controlled by OBA entities already exists: the National Advertising Initiative's Opt-out Tool.[207] The Tool works by using additional cookies to essentially counter-act the OBA cookies used by NAI members, without interfering with the other services provided by NAI members. "Some NAI members offer services such as email…in addition to providing ad serving for other Websites….The opt-out cookie replaces the ad network cookie used to help tailor ads that appear on other Websites, but leaves the cookies used for these other kinds of services untouched."[208]

On the surface, opt-ing out using a cookie-based mechanism appears to enable consumers to control the use of their harvested data for online marketing purposes. Thirty-eight OBA entities currently participate in the NAI opt-out program,[209] however many other OBA entities do not. Therefore, while consumers who take advantage of the NAI opt-out page may limit their privacy risks with regard to NAI members, in order to minimize the exposure of their personal information to non-NAI OBA entities consumers will still need to delete many OBA cookies from non-NAI members. When a consumer deletes her cookies, she deletes her opt-out. As described by the NAI, "If you ever delete the 'opt-out cookie' from your browser, buy a new computer, or change Web browsers, you'll need to perform the opt-out task again."[210] Thus, cookie-based opt-out mechanisms are significantly flawed, in that they are inherently temporary. In order for a consumer to ensure that her privacy interests were maximally protected, she would need to clear non-NAI OBA cookies from her system after every web browser session, and then revisit the NAI website to reinstall NAI opt-out cookies at the beginning of every web browser

[207] Network Advertising Initiative, Opt Out of Behavioral Advertising, http://www.networkadvertising.org/managing/opt_out.asp.
[208] Network Advertising Initiative, FAQs, http://www.networkadvertising.org/managing/faqs.asp#question_17.
[209] Network Advertising Initiative, Opt Out of Behavioral Advertising, *supra* note 207.
[210] Network Advertising Initiative, FAQs, *supra* note 208.

session. Most consumers would likely find this process to be unreasonably cumbersome. The FTC SRP recognizes this problem, and "encourages interested parties to examine this issue and explore potential standards and other tools to assist consumers."[211]

A related problem is that the extant opt-out cookies can be, and are being, circumvented by flash cookies.[212] U.C. Berkeley researchers testing this hypothesis found that "persistent Flash cookies were still used when the NAI opt-out cookie for QuantCast[213] was set. Upon deletion of [regular HTTP] cookies, the Flash cookie still allowed a respawn of the QuantCast HTML cookie. It did not respawn the opt-out cookie. Thus, user tracking is still present after individuals opt out"[214] via the NAI-provided mechanism.

Some individual OBA entities, such as Google, provide an option to 'permanently' opt-out of the use of harvested data for OBA purposes on their sites. From its website, Google provides web viewers with a plug-in browser extension that "permanently saves the DoubleClick opt-out cookie in your browser, allowing you to save your opt-out status even when you clear all cookies….When you clear all cookies in your browser, the plugin automatically sets the DoubleClick opt-out cookie again, so that cookie is effectively not deleted and your opt-out setting stays enabled."[215] The Google perma-cookie is available for consumers using Firefox and Internet Explorer web browsers, and Google also provides consumers using Chrome and

---

[211] FTC SRP, 36.
[212] See discussion of flash cookies generally, above.
[213] QuantCast, an OBA entity and NAI member, claims "to measure and organize the world's audiences in real-time so advertisers can buy, sell and connect with those that matter most….¶QuantCast is currently used by 9 of the top 10 media agencies, more than half of the top publishers (by ad revenue), and marketers from every major vertical to define, buy, or sell the audiences that matters to them most. When QuantCast is connected to planning, buying, and media fulfillment, we deliver the marketplace's purest audiences across a broad range of quality destinations." About QuantCast, QuantCast, http://www.quantcast.com/docs/display/info/About+Quantcast.
[214] Soltani, *supra* note 22.
[215] Google, Advertising Cookie Opt-out Plugin: Frequently Asked Questions, http://www.google.com/ads/preferences/plugin/pluginfaq.html.

Safari web browsers other instructions on how to 'permanently' opt-out.[216] Technically, the opt-out is not permanent, but rather is durable: Google also provides instructions on how to un-install the perma-cookie.[217] Such perma-cookies get around the problem of non-durable opt-out cookies not surviving cookie deletion, and the need to constantly revisit particular web pages' opt-out mechanisms. However, the control of the opt-out perma-cookie by the OBA entity that would stand to profit from the collection and use of the consumer data that OBA cookies might otherwise track poses a further problem: should consumers trust OBA entities themselves to install 'permanent' software files on their computers for the purpose of controlling OBA? Requiring consumers to install perma-cookies developed by the very entities seeking to profit from OBA in order to combat privacy invasions by these same OBA entities is tantamount to inviting the fox to live in the henhouse.

One solution to the fox in the henhouse is to get an independent guard dog. Christopher Soghoian, a Ph.D. Candidate in the School of Informatics and Computing at Indiana University, and Dan Witte of Mozilla have created a free add-on tool for the Firefox web browser called TACO (Targeted Advertising Cookie Opt-Out), which "sets a number of permanent, generic, non personally identifiable opt-out cookies in the browser, which will prevent [more than] 90 different online advertising networks from subjecting users to behavioral advertising (and in some cases, will stop the networks from being able to track users' web browsing habits too)."[218] These opt-out cookies are made permanent, such that "clearing your cookies will delete all regular cookies, but leave the non-identifiable opt-out cookies behind,"[219] so that the consumer will no longer be shown targeted advertisements from the entities correlated to the opt-out

[216] *Id.*
[217] *Id.*
[218] Download the latest stable version of Targeted Advertising Cookie Opt-Out (TACO) Firefox Add-on from Mozilla.org, http://taco.dubfire.net/.
[219] *Id.*

cookies. If the consumer chooses, she may remove the TACO program, and delete even these 'permanent' opt-out cookies. This opt-out mechanism solves the problem of the use of consumer's harvested data by the opted-out entities for OBA purposes, but, as the creators of TACO concede:

> [m]ost advertising networks will continue to collect detailed information about your web browsing habits, which in some cases is retained indefinitely. Even if you use TACO to opt-out of behavioral advertising, many companies [whose opt-out cookies are not currently supported by the TACO program] will still attempt to insert other unique, identifiable cookies into your browser in order to track your browsing across multiple sessions.[220]

Thus, although the TACO program will block the advertisement presenting part of OBA, currently there are no effective ways for consumers to block the data harvesting part of OBA. Hence, although consumers will no longer be subject to viewing advertisements specifically targeted to their supposed purchasing interests, consumers' root privacy interests are left unprotected.

Privacy Bird is a free browser plug-in that "automatically searches for privacy policies at every website you visit. You can tell the software about your privacy concerns, and it will tell you whether each site's policies match your personal privacy preferences. The software displays a green bird icon at Web sites that match, and a red bird icon at sites that do not."[221] The Privacy Bird shows a yellow bird at sites whose privacy policies have not been coded to be read by the underlying P3P software.[222] P3P is "an XML-based specification that enables policy authors to code privacy policies in a machine-readable format which fosters comparison between policies in a standardized way."[223] An associated tool, Privacy Finder, provides a search engine whose results "reference

[220] Does TACO protect my privacy?, http://taco.dubfire.net/#privacy.
[221] Privacy Finder, Find web sites that respect your privacy, http://www.privacybird.org/.
[222] Privacy Bird Frequently Asked Questions, http://www.privacybird.org/faq.html.
[223] McDonald, *supra* note 157 at 563, 567.

more than 15,000 sites using P3P."[224] While 15,000 websites is no small number, merely enabling P3P coding does not mean that the related privacy policies are protective of consumers' privacy interests. Additionally, Privacy Bird appears to be available for the Internet Explorer browser only.[225] At bottom, the ultimate success of this approach requires proactive action on the part of industry players to standardize privacy policies, standardize coding, etc. To do so would be expensive and time consuming for commercial entities and, as discussed, absent a legal requirement to do so, industry players do not have the proper financial incentives to expend resources to empower consumers to protect their own privacy interests.

Theoretically, ISP deep packet inspection might be used as a force for good. A consumer's ISP or network administrator could monitor the consumer's data stream for packets sent back and forth, to and from known OBA adservers and data harvesters, and proactively block them. This could perhaps be done for a premium fee paid to the ISP or network administrator. This technological fix poses some practical and conceptual problems. Practically speaking, ISPs would need to have an accurate black list of known data harvesters and adservers, in order to be able to block them. Such a comprehensive list would be both politically and technically difficult to create, and it might be easy to get around: for example, data harvesters and OBA entities could simply shift from IP address to IP address. Also, more philosophically, consumers would have to trust their ISPs more than they trust other OBA practitioners. Given the direct contractual relationship between consumers and their ISP providers, this trust might be reasonable, since consumer's privacy interests might be enforced through regular contractual litigation, with remedies determined by an effective liquidated damages clause.

[224] Web Sites using the P3P 1.0 Recommendation, http://www.w3.org/P3P/compliant_sites. Privacy Finder can be accessed at http://www.privacyfinder.org/.
[225] Privacy Bird Frequently Asked Questions, *supra* note 222.

In addition, this type of approach might not be legal in some jurisdictions, including the state of California. California's wiretapping law requires that *all* parties to a monitored electronic communication consent to the monitoring, which would include both the consumer on one end of the network connection, and any OBA or other entity transmitting data across the ISP's network to the consumer.[226] Without affirmative consent form the OBA entity to allow monitoring of the data it sends, such an approach would be illegal in California. Hence, the twelve percent of the population of the United States who live in California[227] would not be able to use this type of solution.

V. **Conclusion**

As discussed above, in their current iterations, the FTC and Industry SRPs' attempts to provide consumers with effective tools to protect their privacy interests within a self-regulatory regime are ineffective. Even if the proposed self-regulatory schemes work exactly as planned, at bottom OBA entities still face no penalties of any consequence if they do not comply with the self-regulatory guidelines, and the economic value to be gained from harvesting data and using it in OBA gives commercial entities no incentives to protect consumers' privacy interests of their own accord. Binding legislation therefore is not merely the best way to protect consumers' privacy interests; it appears to be the only way.[228]

---

[226] Cal. Pen. Code § 631(a) provides criminal punishment for "Any person who,…willfully and without the consent of all parties to the communication,… attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable,…at any place within this state."

[227] U.S. Census Bureau, State & County Quick Facts: California, http://quickfacts.census.gov/qfd/states/06000.html (as of 2008, the population of the U.S. was 304,059,724. The population of California was 36,756,666).

[228] For discussions of proposed federal legislation, see Ciocchetti, *supra* note 50 (recommending federal legislation requiring entities engaging in OBA to either provide a clear and conspicuous privacy policy written in plain English or electronically identify their corporate name with each piece of data they disseminate at the point of dissemination); Candice L. Kline, *Security Theater and Database-Driven Information Markets: A Case for an Omnibus U.S. Data Privacy Statute*, 39 U. TOL. L. REV. 443 (2008) (suggesting federal legislation modeled after the EU Data Privacy Directive); Scott, *supra* note 146 (proposing the Gramm-Leach-Bliley Act as a model for data security breach legislation); Marsh, *supra* note 194 (recommending Congress seek out the best privacy policy, and

legislate that privacy policy as minimum legal compliance); and Osborn Ng, *supra* note 31 (recommending federal legislation to create an opt-in program administered by industry trade groups and overseen by the FTC).