Richmond Journal of Law and Technology

Volume 17 | Issue 4 Article 3

2011

Better Late than Never: How the Online Advertising Industry's Response to Proposed Privacy Legislation Eliminates the Need for Regulation

Catherine Schmierer

BETTER LATE THAN NEVER: HOW THE ONLINE ADVERTISING INDUSTRY'S RESPONSE TO PROPOSED PRIVACY LEGISLATION ELIMINATES THE NEED FOR REGULATION

By Catherine Schmierer*

Cite as: Catherine Schmierer, *Better Late Than Never: How the Online Advertising Industry's Response to Proposed Privacy Legislation Eliminates the Need for Regulation*, XVII Rich. J.L. & Tech. 13 (2011), http://jolt.richmond.edu/v17i4/article13.pdf.

I. INTRODUCTION

[1] Although Julie Matlin liked the shoes she saw on Zappos.com, she ultimately left the site without purchasing them.[1] However, it was not the last time she would see that pair of shoes.[2] For the next several days, the shoes followed Ms. Matlin to numerous other websites.[3] "It was as if Zappos had unleashed a persistent salesmen who wouldn't take no for an answer."[4] Understandably, Ms. Matlin found this "online stalking"

* J.D. Candidate, May 2012, George Mason University School of Law; Editor-in-Chief, *George Mason Law Review*, 2011-2012; B.A., Religious Studies, The College of William & Mary, 2005. The author would like to thank Cyrus Daftary, Kendal Smith, and Matthew McGuire for their invaluable assistance with this article, as well as Adam Fett for his unfailing patience and support.

[1] Miguel Helft & Tanzina Vega, *Retargeting Ads Follow Surfers to Other Sites*, N.Y. TIMES, Aug. 29, 2010, http://www.nytimes.com/2010/08/30/technology/30adstalk.html.

[2] *See id.*

[3] *Id.*

[4] *Id.*

disturbing, but she was more troubled when ads for her online dieting service started following her as well.[5] She stated, "They are still following me around, and it makes me feel fat."[6]

[2] The ads that followed Ms. Matlin around the Internet are a form of online behavioral advertising called retargeting.[7] Online behavioral advertising refers to the collection, use, and distribution of data about consumers' online activities in order to place advertisements that correspond to each consumer's interests.[8] Retargeting, however, merely connects advertisers with past website visitors to entice those visitors to complete their online transactions or purchases.[9] Though retargeting is not as invasive as traditional methods of behavioral advertising, it is often more disconcerting to consumers because it is more obvious.[10]

[5] *See id.*

[6] Helft & Vega, *supra* note 1 (internal quotation marks omitted).

[7] *See id.*; Isaac Scarborough, *Behavioral Retargeting 101*, IMEDIACONNECTION (July 7, 2006), http://www.imediaconnection.com/content/10276.asp.

[8] FED. TRADE COMM'N, FTC STAFF REPORT: SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING 2 (2009) [hereinafter FTC SELF-REGULATORY GUIDELINES], *available at* http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf; Richard Raysman & Peter Brown, *Developments in Online Behavioral Advertising*, LAW.COM, June 8, 2010, http://www.law.com/jsp/nylj/PubArticleNY.jsp?id=1202460986288&slreturn=1&hbxlogin=1.

[9] *See* Scarborough, *supra* note 7.

[10] *See* Helft & Vega, *supra* note 1 ("As [behavioral] tracking gets more and more crass and obvious, consumers will rightfully become more concerned about it." (quoting Michael Learmonth, *The Pants That Stalked Me on the Web*, ADVERTISING AGE, Aug. 2, 2010, http://adage.com/digitalnext/post?articleid=145204) (internal quotation marks omitted)). Retargeting relies on the placement of a cookie on a user's computer; thus, "if a user refuses or deletes cookies, they simply won't be exposed to retargeted ads." Hollis Thomases, *Retargeting Gains Traction, Part 2*, CLICKZ (May 9, 2006), http://www.clickz.com/clickz/column/1696600/retargeting-gains-traction-part.

[3] For more than a decade, consumers and privacy advocates have sought to increase consumer privacy protections online through lawsuits[11] and calls for regulation.[12] Many argue it is still too early for legislation.[13] However, the recent introduction of multiple privacy bills in the legislature displays a congressional belief that the online advertising industry is now ripe for formal regulation.[14]

---

[11] Most litigation involving online behavioral advertising has been brought under Title I of the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510-2522 (2006) ("Wiretap Act"), Title II of the Electronic Communications Privacy Act, 18 U.S.C. §§ 2701-2711 (2006) ("Stored Communications Act"), and the Computer Fraud & Abuse Act, 18 U.S.C. § 1030 ("CFAA"). To date, most of these actions have been unsuccessful. *See, e.g.*, *In re* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 500, 510-11 (S.D.N.Y. 2001) (dismissing a lawsuit because website operators authorized DoubleClick to collect data about consumers who viewed their websites).

[12] For example, many consumer groups support the creation of a Do-Not-Track list similar to the Do-Not-Call registry, which would allow consumers to choose whether to let advertisers collect information about their online activities. *See* FED. TRADE COMM'N, FTC STAFF REPORT: SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING—CONCURRING STATEMENT OF COMMISSIONER PAMELA JONES HARBOUR 5 n.11 (2009) [hereinafter HARBOUR CONCURRENCE], *available at* http://www.ftc.gov/os/2009/02/P085400behavadharbour.pdf. However, a Do-Not-Track list would differ from the Do-Not-Call registry in one key respect: "consumers who sign up for the [Do Not Call] registry are able to avoid . . . all telemarketing calls at home." Wendy Davis, *Without Legislation, FTC's Do-Not-Track System Lacks Mandate*, THE DAILY ONLINE EXAMINER (Nov. 10, 2010, 6:00 PM), http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=139324 [hereinafter Davis, *Do-Not-Track Lacks Mandate*]. By contrast, a Do-Not-Track list would not prevent advertisers from sending ads to individual consumers online; instead, it would only stop behavioral advertisers from "trailing people online and delivering ads based on users' [w]eb history[ies]." Davis, *Do-Not-Track Lacks Mandate*, *supra*.

[13] *See, e.g.*, HARBOUR CONCURRENCE, *supra* note 12, at 2 (stating that regulation of behavioral advertising is "not prudent at this time."); *see also* Robert Todd Graham Collins, Note, *The Privacy Implications of Deep Packet Inspection Technology: Why the Next Wave in Online Advertising Shouldn't Rock the Self-Regulatory Boat*, 44 GA. L. REV. 545, 551 (2010) ("[A] knee-jerk reaction instituting new . . . online information privacy legislation would be misguided given the essential features of the Internet and the likely future of online advertising.").

[14] *See The BEST PRACTICES Act, and the Boucher-Stearns Privacy Discussion Draft: Hearing on H.R. 5777 Before the Subcomm. on Commerce, Trade & Consumer Prot. of the H. Comm. on Energy & Commerce*, 111th Cong. 1-2 (2010) [hereinafter *Hearing on H.R. 5777*] (statement of Rep. Henry A. Waxman, Chairman, H. Comm. on Energy &

[4] In 2010, Representatives Rick Boucher and Cliff Stearns released a discussion draft of privacy legislation ("Boucher-Stearns Privacy Discussion Draft" or "the Draft").[15] The Draft proposed to regulate the collection and use of consumer information, both on and offline.[16] Shortly thereafter, Representative Bobby Rush introduced a bill, entitled the "Building Effective Strategies To Promote Responsibility Accountability Choice Transparency Innovation Consumer Expectations and Safeguards Act" or "BEST PRACTICES Act," which had a similar purpose.[17] Though these bills were certainly not the first efforts to provide additional legal protection to consumers regarding the collection and use of their personal data online, they are a recent display of the series of efforts by Congress to ensure that privacy legislation is enacted in the near future.[18]

[5] Considering this proposed legislation in light of the Self-Regulatory Guidelines for Online Behavioral Advertising issued by the

Commerce) (describing the need for privacy legislation that will "provide consumers with more control over their personal information and foster more responsible data collection practices by companies."); Press Release, Cong. Rep. Bobby L. Rush, Subcommittee Chairman Bobby L. Rush Fights for[ ]Consumer Privacy and Prot. of Pers. Info. Introduces the BEST PRACTICES ACT of 2010 (July 19, 2010), *available at* http://www.house.gov/list/press/il01_rush/pr_100719_best_practices_act.shtml; s*ee also* Learmonth, *supra* note 10 (stating that retargeting reflects the online advertising industry's lack of concern about privacy legislation).

[15] Press Release, Cong. Rep. Cliff Stearns, Stearns, Boucher Release Discussion Draft of Privacy Legislation (May 4, 2010), *available at* http://stearns.house.gov/News/DocumentSingle.aspx?DocumentID=183894.

[16] *See* Boucher-Stearns Privacy, H.R. ___ § 2(4), 111th Cong. (as published by H. Subcomm. on Commc'ns, Tech., & the Internet, May 4, 2010) (Staff Discussion Draft), *available at* http://stearns.house.gov/UploadedFiles/privacy_staff__discussion__draft.pdf (stating the bill's goal is "[t]o require notice to and consent of an individual prior to the collection and disclosure of certain personal information relating to that individual").

[17] *See* The BEST PRACTICES Act, H.R. 5777, 111th Cong. (as reported by H. Comm. on Energy & Commerce, July 19, 2010).

[18] *See, e.g.*, Personal Data Privacy and Security Act of 2009, S. 1490, 111th Cong. (as reported by S. Comm. on the Judiciary, July 22, 2009).

Federal Trade Commission ("FTC")[19] and recent FTC enforcement actions,[20] this Article argues that the advertising industry's reaction to the proposed legislation has already expanded the FTC's ability to use its enforcement authority. In fact, the threat of legislation is already changing the way online advertisers do business.[21] More specifically, the online advertising industry has established new compliance and education programs, which will provide more transparency and control to consumers about online behavioral advertising.[22]

[6] Consequently, despite promises that recently-introduced privacy bills will provide additional protection to consumers, these bills will likely do nothing more than maintain the status quo. This Article demonstrates that the self-regulatory actions (or reactions) of the online advertising industry bring online behavioral advertising within the FTC's authority to attack "deceptive practices" under § 5 of the FTC Act.[23] Thus, the FTC's ability to protect consumer privacy online through enforcement actions against online advertisers makes the proposed legislation unnecessary, and ultimately too premature to result in the meaningful privacy protections they seek to provide.

[7] Part II of this Article describes consumers' attitudes toward online privacy, and provides background on online behavioral advertising, including what it is, how it works, and how companies obtain consent to collect consumers' data. Part III evaluates the FTC's enforcement authority and its current framework of self-regulation. In addition, this Part analyzes two reports released by the FTC and Department of Commerce ("Commerce"), which offer new frameworks for increasing

[19] *See infra* Part III.B (describing the FTC's Self-Regulatory Principles for Online Behavioral Advertising).

[20] *See infra* Parts III.A.1, II.A.2 (outlining two recent FTC enforcement actions against online service providers).

[21] *See infra* Part IV.B (discussing the changes in the advertising industry's standard practices in light of recent legislative action by Congress).

[22] *See infra* Part IV.B (discussing the advertising industry's reaction to proposed privacy legislation).

[23] 15 U.S.C. § 45 (2006).

consumer privacy. Finally, Part IV examines the proposed privacy legislation and the online advertising industry's response, ultimately concluding that the industry's response to the potential legislation expands the FTC's ability to bring enforcement actions against online behavioral advertisers and renders the proposed legislation virtually meaningless.

II. BACKGROUND

[8] Louis Brandeis and Samuel Warren were the first to articulate a common law right to privacy.[24] They argued that "the right to be let alone" was necessary to protect individuals from invasions of privacy that resulted from new technologies.[25] More than a century later, their concern is still valid. The proliferation of the Internet has brought with it many new legal challenges, and one need only look to the popular press to find that behavioral advertising and online consumer privacy are chief among them.[26]

A. Consumer Attitudes About Online Privacy

[9] Despite the media attention devoted to the issue of online privacy, some argue that society no longer recognizes an individual's right to privacy.[27] Notably, Mark Zuckerberg, CEO of Facebook, believes that privacy, particularly among young adults, is "no longer a social norm"

[24] *See* Louis D. Brandeis & Samuel D. Warren, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890).

[25] *See id.* at 193-96 ("Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society."). In fact, Brandeis and Warren wrote their article based on a concern that the rise of newspapers and the invention of "instantaneous photographs" (e.g., Polaroids) would compromise individuals' rights to keep aspects of their lives private. *See id.* at 195-96.

[26] *See, e.g.*, *What They Know Series*, WALL ST. J., http://online.wsj.com/public/page/what-they-know-digital-privacy.html (last visited Apr. 18, 2011).

[27] *See* Bobbie Johnson, *Privacy No Longer a Social Norm, Says Facebook Founder*, GUARDIAN.CO.UK (Jan. 11, 2010, 9:58 PM), http://www.guardian.co.uk/technology/2010/jan/11/facebook-privacy.

because "[p]eople have really gotten comfortable not only sharing more information [of] different kinds, but more openly and with more people."[28] However, recent empirical studies suggest that this characterization of consumer attitudes about online privacy is inaccurate.[29]

[10] For example, in April 2010, the University of California Berkeley and University of Pennsylvania jointly released the results of an empirical study, in which they found that young adults in the United States are as concerned about online privacy as older adults.[30] The real disparity between young adults and their older counterparts was that younger consumers believed, incorrectly, that the law provides a strong degree of protection for their privacy both on and offline.[31] Similarly, a Zogby poll showed that most teens understand that search engines and social networks track their online activity, and demonstrated that they, like most adults, wanted more control over the collection of their personal information.[32]

[11] Despite the public's desire for more control over their personal data, it is often argued that people should not be concerned about privacy unless they have something to hide.[33] Scholars describe this "nothing to

[28] *Id.* (internal quotations omitted). Although social media raises different privacy concerns than behavioral targeting, when companies use social media to collect information about consumers' online activity, they should abide by the same self-regulatory principles as traditional online advertisers. *See* Melissa Landau Steinman & Mikhia Hawkins, *When Marketing Through Social Media, Legal Risks Can Go Viral*, 22 INTELL. PROP. & TECH. L.J. no. 8, 2010 at 1, 7; *infra* Part III.B.

[29] Chris Jay Hoofnagle et al., *How Different Are Young Adults from Older Adults When It Comes to Information Privacy Attitudes and Policies?* 20 (Apr. 14, 2010) (unpublished research study), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1589864; Austin Carr, *Teens Want More Privacy Online Too*, FASTCOMPANY.COM, Oct. 7, 2010, http://www.fastcompany.com/1693718/teens-want-more-privacy-controls-poll.

[30] Hoofnagle et al., *supra* note 29, at 3.

[31] *Id.* at 4, 17-19.

[32] *See* Carr, *supra* note 29.

[33] Daniel J. Solove, *"I've Got Nothing to Hide" and Other Misunderstandings of Privacy*, 44 SAN DIEGO L. REV. 745, 746-47 (2007).

hide argument" as an "all-too-common refrain" and the "most common retort against privacy advocates."[34] Moreover, this view fails to recognize that "real" problems result from a widespread perception that individuals have no right to be free from intrusion by business and government entities.[35] As Professor Daniel J. Solove argues, harms that result from a lack of privacy "need not be physical or emotional" and "can occur by chilling socially beneficial behavior (for example, free speech and association) . . . ."[36] Similarly, Professor Julie Cohen argues that the First Amendment includes an implicit "right to read anonymously" on the Internet.[37] However, although these concerns about privacy are valid and publicly supported,[38] they must be balanced against the broad First Amendment protections for commercial speech (i.e., advertising),[39] particularly when applied in the context of the Internet and other new technologies.

B. What is Behavioral Advertising and How Does It Work?

[12] Behavioral advertising is the collection of data regarding consumer activity online, which allows a marketer to focus advertisements on each

[34] *Id.* at 747 (quoting Bruce Schneier, Commentary, *The Eternal Value of Privacy*, WIRED (May 18, 2006), http://www.wired.com/politics/security/commentary/securitymatters/2006/05/70886; Geoffrey R. Stone, Editorial, *Freedom and Public Responsibility*, CHI. TRIB., May 21, 2006, http://articles.chicagotribune.com/2006-05-21/news/0605210386_1_phone-records-nsa-freedoms).

[35] *See* Solove, *supra* note 33, at 764.

[36] *Id.* at 758.

[37] Julie E. Cohen, *A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace*, 28 CONN. L. REV. 981, 982, 1003-15 (1996) ("[R]eading is so intimately connected with speech and freedom of thought that the First Amendment should be understood to guarantee such a right.").

[38] *See supra* notes 28-31 and accompanying text.

[39] *See generally* 44 Liquormart, Inc. v. Rhode Island, 517 U.S. 484, 495 (1996) ("Advertising has been a part of our culture throughout our history. Even in colonial days, the public relied on 'commercial speech' for vital information about the market.").

customer's personal interests.[40] This practice uses technology to increase the value of each marketing impression by "plac[ing] the right ad before the right person at the right time."[41] Moreover, the tailored advertisements that consumers receive because of behavioral advertising are the "quid pro quo" of free services they have access to online.[42]

[13] There are two common forms of behavioral advertising.[43] The first type, contextual or first-party marketing, occurs when an advertiser itself uses information about the particular website a consumer is viewing to determine what type of ad to display.[44] Contextual advertising typically does not require the collection or retention of customer data.[45] For example, if a consumer views an article about Fashion Week on a news website, an advertisement for a high-end clothing store might appear next to the story she is reading. While the FTC does not actively support this form of advertising, it is generally regarded as less invasive than the alternative.[46]

---

[40] *See* FTC SELF-REGULATORY GUIDELINES, *supra* note 8, at 2; Raysman & Brown, *supra* note 8.

[41] Peter Brown, *Behavioral Marketing*, PRACTISING L. INST., Apr.-May 2010, *available at* 1001 PLI/Pat 227, 229 (Westlaw).

[42] *See* JOHN BATTELLE, THE SEARCH: HOW GOOGLE AND ITS RIVALS REWROTE THE RULES OF BUSINESS AND TRANSFORMED OUR CULTURE 194 (2005). John Battelle describes data collection about consumers' online activity as a "Database of Intentions," which includes "the aggregate results of every search ever entered, every result list ever tendered, and every path taken as a result." *Id.* at 6.

[43] Susan E. Gindin, *Perfect Storm for Behavioral Advertising: How the Confluence of Four Events in 2009 May Hasten Legislation (and What this Means for Companies Which Use Behavioral Advertising)*, ISAACSON ROSENBAUM P.C., 1 (Nov. 2009), [hereinafter Gindin, *Perfect Storm*], *available at* http://ir-law.com/files/3166_Gindin_BehavAdvertising_.pdf.

[44] FTC SELF-REGULATORY GUIDELINES, *supra* note 8, at iii.

[45] *Id.*

[46] *Id.*; Gindin, *Perfect Storm, supra* note 43, at 1.

[14] The second form of behavioral advertising involves placement of a "cookie" on the consumer's computer.[47] A cookie is a program that, when placed on a consumer's hard drive, collects information about the user, including usernames, search terms, and passwords.[48] "Cookies are, by design . . . largely invisible to consumers and encrypted to be unintelligible to any user wanting to know what the cookies are saying about him or her."[49] As a result, consumers often are unaware that advertisers are tracking their online activities.[50] Moreover, cookies are more invasive than contextual advertising, which tracks only consumers' action on a particular website, because cookies monitor consumers' movements across multiple websites within an ad network and record information they type into search boxes and online registration forms.[51]

[15] There are two classes of cookies: browser-based and Flash cookies.[52] Consumers can easily remove browser-based cookies from their computer's hard drive by clearing their online browsing history or deleting cookies through a browser tool.[53] Unlike browser-based cookies, Flash cookies are a more "persistent" form of behavioral tracking;

[47] FTC SELF-REGULATORY GUIDELINES, *supra* note 8, at 2.

[48] *See In re* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 502-03 (S.D.N.Y. 2001); *see also In re* Pharmatrak, Inc. Privacy Litig., 329 F.3d 9, 14 (1st Cir. 2003) ("Cookies are widely used on the internet by reputable websites to promote convenience and customization.").

[49] Richard M. Marsh, Jr., Note, *Legislation for Effective Self-Regulation: A New Approach to Protecting Personal Privacy on the Internet*, 15 MICH. TELECOMM. & TECH. L. REV. 543, 546 (2009).

[50] *See id*.

[51] *See* Brown, *supra* note 41, at 232.

[52] *See* Robert D. Forbes, *Recent Lawsuits Challenge Use of Flash Cookies to Track Online Behavior*, PROSKAUER PRIVACY L.BLOG (Sept. 14, 2010, 10:36 AM), http://privacylaw.proskauer.com/2010/09/articles/behavioral-marketing/recent-lawsuits-challenge-use-of-flash-cookies-to-track-online-behavior/.

[53] *See* Ashkan Soltani et al., *Flash Cookies and Privacy* 1-2 (Aug. 10, 2009) (Working Paper), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1446862.

uncontrolled by a browser, Flash cookies are more difficult for consumers to delete if they wish to prevent companies from using them to collect behavioral data.[54] In fact, a recent study found:

> [The] top 100 websites are using Flash cookies to 'respawn,' or recreate deleted HTTP cookies. 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. [In addition, f]ew websites disclose their use of Flash in privacy policies, and many companies using Flash are privacy certified by TRUSTe.[55]

For these reasons, Flash cookies ignite greater concern among consumers and privacy advocates, and have been at the heart of several class-action lawsuits.[56]

[16] In addition, scholars also distinguish between "passive" and "active" collection of consumer data.[57] In the case of active data collection, the consumer chooses to share his or her personal information with the advertiser – typically in response to some kind of incentive.[58] By contrast, passive collection typically occurs when the advertiser places a cookie on the consumer's computer.[59] Spyware and adware represent two methods of passive data collection related to behavioral advertising.[60]

---

[54] *Id.* at 1.

[55] *Id.* at 2. TRUSTe is a for-profit entity that monitors privacy policies on various websites to determine if they are adequate. *See infra* Part IV.B (discussing TRUSTe's business model and its compliance program for online behavioral advertisers).

[56] *See, e.g.*, Complaint at 2, Godoy v. Quantcast Corp., No. CV10-7662-RGK (JCG), 2010 WL 4236367 (C.D. Cal. Oct. 13, 2010) ("'Flash cookies' … are often used in place of or as a back-up for browser cookies . . . [and] have been used to recreate the browser cookie if it is deleted by the internet user."); Complaint, La Court v. Specific Media, Inc., No. SACV10-01256, 2010 WL 3581775 (C.D. Cal. Aug.18, 2010).

[57] Raysman & Brown, *supra* note 8.

[58] *Id.*

[59] *Id.*

[17] Spyware is a form of software that, when installed on a consumer's computer, "collects and reports in-depth information about [an] end-user."[61] On the other hand, adware does not involve the installation of software on a consumer's hard drive.[62] Instead, adware is software that tracks a consumer's online activity and causes pop-up advertisements to appear on the consumer's screen only after the consumer views a specific website.[63]

[18] The foregoing methods of behavioral targeting are designed to help advertisers provide the consumer with tailored advertisements.[64] This collection of data about Internet users is important to advertisers because it increases the value of each ad impression and improves the "click-through rate"[65] – ultimately, increasing the advertisers' overall revenue.[66]

---

[60] *See* Daniel B. Garrie et al., *Regulating Spyware: Challenges and Solutions*, 13 J. INTERNET L. 3, 3-4 (2010); Heather Osborn Ng, *Targeting Bad Behavior: Why Federal Regulators Must Treat Online Behavioral Marketing as Spyware*, 31 HASTINGS COMM. & ENT. L.J. 369, 373-75 (2009).

[61] Garrie et al., *supra* note 60, at 3.

[62] *C.f.* Denise A. Golumbaski, Comment, *Spyware Phones Home: Should the FTC Answer the Call for Regulation?*, 57 ADMIN. L. REV. 1171, 1178 (2005) (stating that adware has several legitimate uses and poses less of a threat to consumers).

[63] *See id.*

[64] *See* Adam Thierer & Berin Szoka, *Chairman Leibowitz's Disconnect on Privacy Regulation & the Future of News*, THE PROGRESS & FREEDOM FOUND. (Jan. 2010), http://www.pff.org/issues-pubs/ps/2010/ps6.1-Leibowitz-disconnect-on-privacy-and-advertising.html.

[65] The "click-through rate" is a metric used to determine how many times a web user is diverted from the site on which an advertisement is displayed to the advertiser's website. *See* Stacey L. Dogan, *Trademark Remedies and Online Intermediaries*, 14 LEWIS & CLARK L. REV. 467, 478 (2010). It is measured by dividing the total number of clicks an ad receives by the number of times the ad is shown. *See* Peter T. Tschanz, *A Constitutional Right to Deceive?: The First Amendment Implications of Regulating Pay per Click*, 2010 B.C. INTELL. PROP. & TECH. F. 92201, *7 n.56 (2010) (quoting Animesh Animesh et al., *Competing "Creatively" in Online Markets: Evidence from Sponsored Search* 6 (Univ. of Md. Robert H. Smith Sch. of Bus., Working Paper No. RHS-06-064, 2007), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1032199.

[19] Frequently, however, consumers do not expressly consent to the collection of their personal information.[67] For example, in the context of traditional behavioral advertising, including the placement of cookies on consumers' computers, website operators include provisions about these practices in their privacy policies and terms of use.[68] Operators typically link to these documents from the initial landing page.[69] However, it is also widely believed that consumers do not read these policies, because either they are uninterested or feel the documents are written in legalese and, thus, are incomprehensible.[70]

[20] Nonetheless, even if consumers do not read online license agreements, privacy policies, or terms of use, they could be bound by their terms.[71] For example, in the case of spyware, a consumer downloads software onto his or her computer, but often can do so only after expressly consenting to the software provider's license agreement (typically referred

---

[66] *See* Pamela Jones Harbor, Comm'r, Fed. Trade Comm'n, Remarks before FTC Exploring Privacy Roundtable 2 (Dec. 7, 2009), *available at* http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf.

[67] *See id.*

[68] *See, e.g.*, Collins, *supra* note 13, at 564-66 (describing Google's privacy policy and its presumption of consent regarding "cookie-based data collection").

[69] *See generally* Ian Rambarran & Robert Hunt, *Are Browse-Wrap Agreements All They Are Wrapped Up to Be?*, 9 TUL. J. TECH. & INTELL. PROP. 173, 202 (2007).

[70] *See* Thierer & Szoka, *supra* note 64, at 1 (stating the "'literature is clear' that few people read [online] privacy policies"); *see also* Carr, *supra* note 29 ("Meanwhile, 45% of teens said they do read [websites'] terms and conditions-- but does anyone actually believe nearly half of all 15- to18-year-olds are scanning pages of online legalese?").

[71] *See* M. Angela Buenaventura, *Teaching a Man to Fish: Why National Legislation Anchored in Notice and Consent Provisions Is the Most Effective Solution to the Spyware Problem*, 13 RICH. J.L. & TECH. 1, 14-15 (2006) (noting that courts often construe clickwrap agreements as binding "whether or not meaningful consent was actually present, and whether or not the user even saw the terms [of the contract] to begin with."). *But cf.* Mark A. Lemley, *Place and Cyberspace*, 91 CAL. L. REV. 521, 528 n.29 (2003) (stating that unlike clickwrap agreements, browsewrap agreements involve no actual consent; therefore, "no court to actually consider the enforceability of browsewrap licenses under contract law has found them enforceable.").

to as a "clickwrap agreement").[72] One federal judge jokingly described consumers' assent to clickwrap agreements in the following way:

> Has this happened to you? You plunk down a pretty penny for the latest and greatest software, speed back to your computer . . . click on "install" and, after scrolling past a license agreement which would take at least fifteen minutes to read, find yourself staring at the following dialog box: "I agree." Do you click the box? You probably do not agree in your heart of hearts, but you click anyway, not about to let some pesky legalese delay the moment for which you've been waiting. Is that "clickwrap" license agreement enforceable? Yes . . . .[73]

Accordingly, although a consumer may never actually read the terms of a clickwrap agreement before clicking "I Agree," courts generally uphold these agreements as enforceable contracts.[74] However, companies have had less success arguing that when they include a link to their privacy policies and terms of use on their home page, those legal documents (i.e., browsewrap agreements) constitute enforceable contracts with consumers who use their website.[75] "Unlike a clickwrap agreement, a browsewrap

[72] *See infra* Part III.A.2 (describing a clickwrap agreement Sears required consumers to consent to before allowing them to download its software program).

[73] I.Lan Sys., Inc. v. NetScout Serv. Level Corp., 183 F. Supp. 2d 328, 329 (D. Mass. 2002).

[74] *See id.* at 338 (holding a clickwrap agreement to be an enforceable contract); Forrest v. Verizon Commc'ns, Inc., 805 A.2d 1007, 1010-11 (D.C. 2002) (upholding a forum selection clause contained in a clickwrap agreement).

[75] *See, e.g.*, Specht v. Netscape Commc'ns Corp., 306 F.3d 17, 20 (2d Cir. 2002) (holding a browsewrap agreement unenforceable because there was insufficient notice of its terms); Cvent, Inc. v. Eventbrite, Inc., 739 F. Supp. 2d 927, 937 (E.D. Va. 2010) (stating that for a browsewrap agreement to be enforceable, "the website user must have had actual or constructive knowledge of the site's terms and conditions, and have manifested assent to them."). *But see* Kimberley Rose Goldberg, Note, *Platform for Privacy Preferences ("P3P"): Finding Consumer Assent to Electronic Privacy Policies*, 14 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 255, 270-71 & n.89 (2003) (stating that courts might enforce browsewrap agreements if consumers continue browsing a website after they view that website's home page).

agreement 'does not require the user to manifest assent to the terms and conditions expressly . . . [a] party instead gives his assent simply by using the website.'"[76]

[21] Nonetheless, as Part III describes, the enforceability of an online agreement may not necessarily prevent the FTC from bringing an enforcement action against an online advertiser.[77] In the past, to avoid facing an FTC enforcement action, an online advertiser only needed to disclose the extent to which it collected and used data about consumers' online activities – provided that the company abided by the representations in its online agreements.[78] But, recently, the FTC brought an enforcement action against Sears for data collection practices it did disclose in its online privacy policy because the agency believed the privacy policy was misleading and led consumers to believe that they would know the extent to which Sears was tracking them online when, in fact, they did not.[79]

III. THE FTC'S ROLE: SELF-REGULATION & ENFORCEMENT

A. The FTC's Authority to Attack Unfair and Deceptive Trade Practices

[76] Hines v. Overstock.com, Inc., 668 F. Supp. 2d 362, 366-67 (E.D.N.Y. 2009) (quoting Sw. Airlines Co. v. BoardFirst, L.L.C., No. 06-CV-0891-B, 2007 WL 4823761, at *4 (N.D. Tex. Sept. 12, 2007)), *aff'd*, 380 F. App'x. 22 (2d Cir. 2010).

[77] *See infra* Part III.A.

[78] J. Thomas Rosch, Comm'r, Fed. Trade Comm'n, Some Reflections on the Future of the Internet: Net Neutrality, Online Behavioral Advertising, and Health Information Technology at the U.S. Chamber of Commerce Telecommunications & E-Commerce Committee Fall Meeting 8 (Oct. 26, 2009), *available at* http://www.ftc.gov/speeches/rosch/091026chamber.pdf ("I'm personally not sure I would conclude that behavioral tracking that collects nonsensitive information is necessarily deceptive or unfair within the meaning of Section 5 [of the FTC Act], even if a particular consumer might find such practices disturbing or invasive.").

[79] *See In re* Sears Holdings Mgmt. Corp., No. 082-3099, 2009 WL 2979770 (F.T.C.), at *1 (Aug. 31, 2009); *infra* Part III.A.2.

[22] The FTC and more specifically, its Bureau of Consumer Protection ("BCP"), acts as the primary enforcer for matters involving online consumer privacy.[80] In fact, the FTC recently established a new office, the Division of Privacy and Identity Protection, which aims to protect online consumer privacy, ensure information security, and combat identity theft.[81] The FTC's authority to attack improper conduct related to online consumer privacy exists under Section 5 of the FTC Act.[82] This statute authorizes the FTC to protect consumers by prohibiting any "unfair or deceptive acts or practices in or affecting commerce" as well as "[u]nfair methods of competition."[83] For the first thirty years after the enactment of the FTC Act, the FTC failed to distinguish between "unfair" and "deceptive" practices when bringing enforcement actions.[84] However, in 1964, the FTC articulated a test for unfairness in its Cigarette Rule Statement of Basis and Purpose and, thereby, created two distinct categories of enforcement authority: unfairness authority and the authority to attack deceptive practices.[85]

[23] Unlike its authority to attack deceptive practices, the FTC's unfairness authority is no longer widely utilized.[86] In a 2003 speech, former Director of the FTC's BCP Howard Beales suggested that the FTC's resistance to using its unfairness authority stemmed from a period

---

[80] *See* DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 72-73 (2004); Collins, *supra* note 13, at 571-73.

[81] *Division of Privacy & Identity Protection*, FTC BUREAU OF CONSUMER PROTECTION, http://www.ftc.gov/bcp/bcppip.shtm (last updated Oct. 23, 2007).

[82] *See* 15 U.S.C. § 45(a) (2006).

[83] 15 U.S.C. § 45(a)(1); Howard J. Beales, *The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection* (May 30, 2003), *available at* 2003 WL 21501809 (F.T.C.), at *1.

[84] Beales, *supra* note 83.

[85] *See id*. (citing Unfair or Deceptive Advertising and Labeling of Cigarettes in Relation to the Health Hazards of Smoking, Statement of Basis and Purpose, 28 Fed. Reg. 8355 (1964)).

[86] *See id*. at *1, *4-5.

in the 1970s during which the FTC executed a broad and overreaching plan to ban all advertising aimed at children on grounds that it was "immoral, unscrupulous, and unethical."[87] In response to this and similar actions, members of the popular press began referring to the FTC as, "[The] [N]ational [N]anny."[88] The FTC's actions also garnered disapproval from members of Congress.[89] As a result, Congress enacted legislation that prohibited the FTC from utilizing "unfairness" to restrict advertising and did not reauthorize the FTC to use its unfairness authority for enforcement actions until approximately fifteen years later.[90] In addition, when Congress eventually reauthorized the FTC's unfairness authority in 1994, it set forth a three-part test for unfairness that focused on consumer injury.[91]

[24] Therefore, today, for the FTC to use its enforcement authority to attack a trade practice based on unfairness, the injury to consumers must be: "(1) substantial, (2) without offsetting benefits, and (3) one that consumers cannot reasonably avoid."[92] To fulfill the first element, the injury must be real and considerable, even when weighed against offsetting benefits.[93] Generally, substantial injury constitutes economic harm or threats to public health and safety, but emotional distress typically

---

[87] *Id*. at *2 (internal quotation marks omitted) (discussing how Former Chairman Michael Pertschuk also stated in his remarks that the FTC's unfairness authority was so broad that the agency could utilize it to punish polluters and regulate the employment of illegal aliens, among other things).

[88] *See, e.g.*, Editorial, *The FTC as National Nanny*, WASH. POST, Mar. 1, 1978, at A22.

[89] *See* Beales, *supra* note 83, at *2.

[90] *Id*.; *see* Federal Trade Commission Improvements Act of 1980, Pub. L. No. 96-252, 94 Stat. 374.

[91] *See* Federal Trade Commission Act Amendments of 1994, Pub. L. No. 103-312, 108 Stat. 1691; Beales, *supra* note 83, at *5. Today, the unfairness test is codified at 15 U.S.C. § 45(n) (2006).

[92] Beales, *supra* note 83, at *5; *see* 15 U.S.C. § 45(n).

[93] Beales, *supra* note 83, at *6.

does not satisfy the standard.[94] The second part of the unfairness test requires that any harm or injury to consumers be weighed against any benefit consumers receive because of the allegedly unfair practice.[95] For example, in the context of online behavioral advertising, the collection of consumer data is arguably not an "unfair trade practice" because consumers receive access to free online content in exchange for data about their online activity.[96] Finally, "the reasonable avoidance prong limits unfairness actions to those where the Commission seeks 'to halt some form of seller behavior that unreasonably creates or takes advantage of an obstacle to the free exercise of consumer decision-making.'"[97] Although the FTC does not currently utilize its unfairness authority often, it can be a powerful tool to attack unfair business practices online, like Internet scams.[98]

[94] *Id*.

[95] *Id*. This element is important in the context of online behavioral advertising because consumers receive "free" content in exchange for the collection of their personal data. *See* HARBOUR CONCURRENCE, *supra* note 12, at 1.

[96] *See* J. Thomas Rosch, *supra* note 78, at 13. In the *Sears* action, *infra* Part III.A.2, Sears paid consumers $10.00 in exchange for permission to collect data about the consumer's online activity. Lesley Fair, *Someone to Watch Over Me?*, BCP BUS. CTR., http://business.ftc.gov/documents/someone-watch-over-me (last visited Jan. 6, 2011). Thus, the FTC brought its enforcement action against Sears under its authority to attack deceptive practices, rather than its unfairness authority. *See* 15 U.S.C. § 45; *In re* Sears Holdings Mgmt. Corp., No. 082-3099, 2009 WL 2979770, at *4 (F.T.C. Aug. 31, 2009). *But see* Susan E. Gindin, *Nobody Reads Your Privacy Policy or Online Contract? Lessons Learned and Questions Raised by the FTC's Action Against Sears*, 8 NW. J. TECH. & INTELL. PROP. 1, 2 (2009).

[97] Beales, *supra* note 83, at *6 (quoting Letter from the FTC to Hon. Wendell Ford & Hon. John Danforth, Comm. on Commerce, Sci. & Transp., U.S. Senate, Comm'n Statement of Policy on the Scope of Consumer Unfairness Jurisdiction (Dec. 17, 1980), *reprinted in In re* Int'l Harvester Co., 104 F.T.C. 949, 1984 WL 565290, at *95 (F.T.C. Dec. 21, 1984)).

[98] *See* Beales, *supra* note 83, at *7-13; FTC v. Zuccarini, No. CIV.A. 01-CV-4854, 2002 WL 1378421, at *4 (E.D. Pa. Apr. 9, 2002) (attacking online "mousetrapping," i.e., programming websites to take control of consumer computers and forcing consumers to view numerous pop-up advertisements).

[25] The FTC's authority to prohibit deceptive acts is much more straightforward. In its 1983 Statement of Deception, the agency articulated three elements that must be present for the FTC to bring an enforcement action under its authority to attack deceptive practices.[99] A deceptive trade practice exists when: (1) there is a representation or omission; (2) that is likely to mislead reasonable consumers; and (3) the representation or omission is material.[100]

[26] Either express or implied claims may fulfill the first element, but for implied claims the FTC examines extrinsic evidence and other facts like the nature of the transaction and the location of the language within the document.[101] The FTC evaluates such statements from the perspective of a "reasonable consumer," and when a product targets a specific audience, the FTC also investigates the effect on members of that consumer group.[102] Finally, "[a] 'material' misrepresentation or practice is one which is likely to affect a consumer's choice of or conduct regarding a product. In other words, it is information that is important to consumers."[103] The FTC presumes that express claims are material because an advertiser would not logically include information in its marketing if it did not want the claim to affect consumer perception about

[99] *See* Letter from James C. Miller III to Hon. John D. Dingell, Chairman, Comm. on Energy and Commerce, FTC Policy Statement on Deception (Oct. 14, 1983), *reprinted in In re* Cliffdale Assocs., Inc., 103 F.T.C. 110, 1984 WL 565319, at *45 (F.T.C. Mar. 23 1984) [hereinafter FTC Statement on Deception].

[100] *Id*.

[101] *See id*. at *46; *see also In re* Am. Home Prods. Corp., 98 F.T.C. 136, 1981 WL 389401, at *192 (F.T.C. Sept. 9, 1981) (evaluating the advertisements at issue "in their entirety" to determine the existence of an implied claim), *aff'd*, 695 F.2d 681 (3d Cir. 1982); *In re* Warner-Lambert Co., 86 F.T.C. 1398, 1489-90 (1975) (examining an implied claim through the location of language within a document), *aff'd*, 562 F.2d 749 (D.C. Cir. 1977).

[102] *See* FTC Statement on Deception, *supra* note 99, at *46 n.20 ("An interpretation may be reasonable even though it is not shared by a majority of consumers . . . or by particularly sophisticated consumers.").

[103] *Id*. at *49.

the relevant product or service.[104] Moreover, most representations will fulfill this element because the FTC also classifies information as material if "it concerns the purpose, safety, efficacy, or cost of [a] product or service" or "if it concerns durability, performance, warranties or quality."[105]

[27] Enforcement actions against providers of Internet products or services have typically been brought under the FTC's authority to attack deceptive practices.[106] To date, the FTC has brought only one enforcement action specifically related to online behavioral advertising.[107] Because of this, two recent actions involving deceptive practices online, *In re Gateway Learning Corp.*[108] and *In re Sears Holdings Management Corp.*,[109] are particularly relevant to the analysis of how the FTC might attack the collection of data regarding consumers' online activities going forward.

[104] *See* Cent. Hudson Gas & Elec. Co. v. Pub. Serv. Commission of N.Y., 447 U.S. 557, 567-68 (1980) ("In the absence of factors that would distort the decision to advertise, we may assume that the willingness of a business to promote its products reflects a belief that consumers are interested in the advertising.").

[105] FTC Statement on Deception, *supra* note 99, at *49 (footnotes omitted).

[106] *See* Rosch, *supra* note 78, at 9.

[107] *In re* Chitika, Inc., No. 102-3087, 2011 WL 914035, at *1-3 (F.T.C. March 14, 2011); *see also* Ng, *supra* note 60, at 391; Rosch, *supra* note 78, at 12-13 (explaining that presumably, it is difficult for the FTC to bring enforcement actions against online behavioral advertisers because (1) the agency cannot bring an enforcement action for a deceptive practice if advertisers fully disclose their data collection practices in online privacy policies or a website's terms of use; and (2) the FTC is unable to fulfill second prong of the unfairness test because although the collection of data may "harm" consumers, they receive an off-setting benefit because they receive free access to online content, like newspapers and magazines).

[108] *In re* Gateway Learning Corp., 138 F.T.C. 443, 443-44, 467 (2004).

[109] *In re* Sears Holdings Mgmt. Corp., No. 082-3099, 2009 WL 2979770, at *1, *5 (F.T.C. Aug. 31, 2009).

1. FTC Enforcement Action Against Gateway Learning Corporation

[28] Beginning in 2000, Gateway Learning Corporation, the provider of "Hooked on Phonics" products, marketed its products online at the following website: http://www.hop.com.[110] The privacy policy on Gateway's website declared: "We do not sell, rent or loan any personally identifiable information regarding our consumers with any third party unless we receive customer's explicit consent."[111] Moreover, the policy stated that Gateway would notify consumers of any changes to their privacy policy and, at that time, would offer consumers the opportunity to "opt-out" of Gateway's data collection practices.[112] Nonetheless, in 2003, Gateway began renting consumers' personal information to third-party advertisers for direct mailing and telemarketing purposes.[113] Subsequently, the company altered its privacy policy "to say that 'from time to time' Gateway Learning would provide consumers' personal information to 'reputable companies' whose products or services consumers might find of interest . . . ."[114]

[29] Shortly thereafter, the FTC filed an enforcement action in which it alleged that by failing to notify consumers about the retroactive application of its altered privacy policy, Gateway engaged in both unfair *and* deceptive trade practices.[115] Because Gateway failed to notify its existing customers about the change to their privacy policy, it prevented consumers from deciding whether to allow Gateway to provide third-party marketers with their personal information and, thus, engaged in an unfair

[110] Press Release, Fed. Trade Comm'n, Gateway Learning Settles FTC Privacy Charges (Jul. 7, 2004), *available at* http://www.ftc.gov/opa/2004/07/gateway.shtm.

[111] *Id.* (internal quotations marks omitted).

[112] *Id.*

[113] *See id.*

[114] *Id.*

[115] *See In re Gateway Learning Corp.*, 138 F.T.C. at 449-50.

practice in violation of § 5 of the FTC Act.[116] Similarly, the FTC alleged that Gateway also engaged in deceptive practices because Gateway represented to consumers in its privacy policy that it would not sell or rent customer data and, subsequently, rented the information to third-party advertisers without obtaining the express consent of consumers.[117]

[30] The FTC entered a Consent Order (i.e., a settlement agreement between the agency and the offending party) in *Gateway* on September 10, 2004.[118] The agreement prohibited Gateway from making misrepresentations about how it would use data collected about consumers' online activities.[119] In addition, the Consent Order required Gateway to obtain "express affirmative ('opt-in') consent from consumers" when it made "material changes to its [online] privacy polic[ies]" and prohibited Gateway from making retroactive changes to its data collection practices.[120]

2. FTC Enforcement Action Against Sears Holdings Management Corporation

[31] More recently, in 2009, the FTC filed an action against Sears under § 5 of the FTC Act for deceptive practices related to its "My SHC Community" program.[121] The FTC alleged that Sears failed to notify customers that when they installed Sears' software tracking application, the software collected information about all of the consumers' online and even offline activities (including web browsing histories, purchases, e-mail messages, and even secure data like online checking account information), and transmitted the customers' data to Sears.[122] According

[116] *See id.* at 449.

[117] *See id.* at 449-50.

[118] *Id.* at 443.

[119] *See* Press Release, Fed. Trade Comm'n, *supra* note 110.

[120] *Id.*

[121] *See In re Sears*, 2009 WL 2979770, at *1; Gindin, *supra* note 96, at 1.

[122] *See* Gindin, *supra* note 96, at 1.

to the FTC, Sears invited customers to their websites – http://www.sears.com and http://www.kmart.com – and asked them to participate in the "My SHC Community" program.[123] Sears offered to pay customers $10.00 and, in exchange, customers would download the "My SHC Community" software to their computers, which would track their "online browsing."[124] In its marketing e-mails, Sears stated:

> My SHC Community is a dynamic and highly interactive online community. It's a place where your voice is heard and your opinion matters, and what you want and need counts! As a member of My SHC Community, you'll partner directly with the retail industry. You'll participate in exciting, engaging and on-going interactions – *always on your terms and always by your choice*.[125]

Sears's marketing e-mails reiterated that although participants downloaded software that would "confidentially track [customers'] online browsing," the collection would always be "on [their own] terms and always by [their] choice."[126] Once consumers elected to participate in the program, Sears directed them to a landing page that displayed the same content included in its marketing e-mails.[127] Finally, consumers completed a registration form that presented a Privacy Statement and User License Agreement ("PSULA").[128] Consumers were required to click on a box, stating that they had read and agreed to the terms of the PSULA, to complete their registration.[129] Sears included additional details in the PSULA about the

---

[123] Fair, *supra* note 95.

[124] *Id.*

[125] *In re Sears*, 2009 WL 2979770, at *2 (emphasis added).

[126] *Id.*

[127] *See id.* at *3.

[128] *Id.* at *3-4.

[129] *Id.* at *4.

extent to which they would track consumers' activities.[130] Even though Sears required consumers to agree to the terms of the PSULA before downloading the "My SHC Community" software, the FTC argued that the marketing e-mails (and information on various landing pages) made material misrepresentations to consumers and, thus, constituted a deceptive practice.[131] In essence, the FTC alleged that Sears could not reasonably expect consumers to read the PSULA and, therefore, should have provided "clear and prominent" notice to consumers about the information they planned to collect on the landing pages consumers viewed prior to downloading the software.[132]

[32] Eventually, Sears settled with the FTC, agreeing to destroy the data collected and clearly identifying any future attempts to track consumers' online activities.[133] The current Director of the FTC's BCP, David Vladeck, described *Sears* as "'an absolutely classic deception case'" that "hinged on full disclosure and notice."[134] In his view, "Sears enticed people into participating in this program by offering a few dollars but not really telling them what they were doing with the data."[135] In so doing,

[130] *See In re Sears*, 2009 WL 2979770, at *3-4; *see also* Exhibit D, *In re* Sears Holding Mgmt. Corp., 2009 WL 2979770 (F.T.C. Aug. 31, 2009) (No. C-4264).

[131] *See In re Sears*, 2009 WL 2979770, at *4.

[132] *See id.* at *6-7. The FTC's action did not challenge the enforceability of the PSULA – instead it argued that Sears placed deceptive language in its marketing e-mails and websites (i.e., Sears implied that consumers would retain control over the collection of their information when, in fact, the "My SHC Community" software ran in the background of their computers, and consumers who installed the application often had no knowledge that their personal information was collected). *See id.* at *4; Gindin, *supra* note 96, at 2.

[133] *See In re Sears*, 2009 WL 2979770, at *6-7; Edmund Lee, *FTC's Top Consumer Cop Likes Personalization of Web*, ADVERTISING AGE, Sept. 27, 2010, http://adage.com/article?article_id=146064.

[134] Lee, *supra* note 133.

[135] *Id.* (internal quotation marks omitted).

Sears belittled consumers and demonstrated a genuine lack of concern for online consumer privacy.[136]

B. FTC Guidelines for Self-Regulation in Online Behavioral Advertising

[33] After almost a decade of exploring the impact of Internet advertising on online consumer privacy through discussions with privacy advocates, members of the online advertising industry, and legislators, the FTC released its Guidelines for Self-Regulation in Online Behavioral Advertising ("FTC Guidelines") in February 2009.[137] Although the FTC recognized that individuals had legitimate concerns about the collection and storage of data related to their online activities, the agency also stated that consumers received a real benefit from this practice, in the form of free access to online content.[138] In addition, the agency noted that many consumers valued the tailored advertising they received because of behavioral tracking.[139] For example, Director Vladeck admitted that he "sort of like[s] the personalization" of advertisements he receives on the Internet.[140] Therefore, by implementing a voluntary program of self-regulation, the FTC sought to "address practices that raise genuine privacy concerns without interfering with practices – or stifling innovation – where privacy concerns are minimal."[141] In addition, the FTC Guidelines "appl[ied] broadly to companies engaged in online behavioral advertising, defined as tracking consumers' online activities in order to deliver advertising that is targeted to the individual consumers' interests."[142]

[136] *See id.*

[137] *See generally* FTC SELF-REGULATORY GUIDELINES, *supra* note 8.

[138] *Id.* at 1.

[139] *Id.*

[140] Lee, *supra* note 133 (internal quotations marks omitted).

[141] FTC SELF-REGULATORY GUIDELINES, *supra* note 8, at 1.

[142] *Id.* at 20.

[34] Four major concepts govern the FTC Guidelines: (1) control and transparency; (2) security and limited data retention; (3) affirmative express consent for material changes to existing privacy promises; and (4) affirmative express consent to (or prohibition against) use sensitive data for behavioral advertising.[143] The first principle instructs companies that collect data regarding consumers' online activity to "provide meaningful disclosures to consumers" about the information collected and an ability to opt-out of the practice.[144] The second principle encourages companies that employ behavioral advertising to "provide reasonable data security measures" that will prevent inadvertent disclosure of sensitive data and to keep such data on file only as long as necessary to achieve their business objectives.[145] The third principle directs companies to obtain consumers' express consent when they make material changes to their privacy policies concerning the data collected.[146] Finally, the fourth principle requires companies to "obtain [consumers'] affirmative express consent before they use sensitive data – for example, data about children, health, or finances – for behavioral advertising."[147]

[35] Although the FTC Guidelines provided broad principles to move the industry toward an environment more protective of online consumer privacy, the agency recognized that this was just a "step in an ongoing process."[148] Moreover, the FTC urged the industry to take ownership of the self-regulatory model by requiring that all industry members comply

[143] *Id.* at 11-12.

[144] *Id.* at 11. The FTC described "meaningful disclosure" in the following way: "[W]ebsites where data is collected for behavioral advertising should provide [1] prominent notice to consumers about such practices and [2] should also offer consumers the ability to choose whether to allow such collection and use." *Id.* at 30.

[145] *Id.* at 11. The report does not specifically define "reasonable data security measures," however, it does note that these measures could include (1) ensuring anonymity of all the data collected; or (2) requiring companies to destroy data after a certain length of time, like six months. *See id.* at 37-38.

[146] FTC SELF-REGULATORY GUIDELINES, *supra* note 8, at 11-12.

[147] *Id.* at 12.

[148] *Id.* at 47.

with the FTC Guidelines and work to solve the privacy problems behavioral advertising presents.[149] As a result, in July 2009, several trade associations[150] representing various parts of the advertising industry developed a similar set of self-regulatory guidelines ("Industry Guidelines").[151]

[36] Like the FTC Guidelines, the Industry Guidelines set forth seven core principles: (1) transparency; (2) consumer control; (3) data security; (4) notification of material changes in privacy practices; (5) enhanced protection of sensitive data; (6) consumer education; and (7) accountability.[152] In fact, five of the seven principles, the Transparency and Consumer Control Principles, the Data Security Principle, the Material Changes Principle, and the Sensitive Data Principle, corresponded directly to the governing principles in the FTC Guidelines.[153] In addition, the Industry Guidelines' two other principles, the Education and Accountability Principles corresponded to important additional commentary in the FTC Guidelines.[154] For example, the Education Principle directed companies to educate consumers about the

[149] *See id.* at 47-48.

[150] The trade associations that developed the online advertising industry's self-regulatory guidelines were the American Association of Advertising Agencies, Association of National Advertisers, the Council of Better Business Bureaus, the Direct Marketing Association, and the Interactive Advertising Bureau. *See* Interactive Advertising Bureau et al., *Self-Regulatory Principles for Online Behavioral Advertising*, ABOUTADS.INFO (July 2009), http://aboutads.info/resource/download/seven-principles-07-01-09.pdf [hereinafter Industry Guidelines].

[151] *See id.* at 1.

[152] *Id.* at 2-4.

[153] *Id.* at 1.

[154] *See id.* at 1-4; *see also* Hunton & Williams LLP, *Live Coverage from Jerusalem: Vladeck Provides Overview of Upcoming FTC Report*, PRIVACY & INFORMATION SECURITY LAW BLOG (Oct. 28, 2010), http://www.huntonprivacyblog.com/2010/10/articles/events/live-coverage-from-jerusalem-vladeck-provides-overview-of-upcoming-ftc-report/#more [hereinafter Hunton & Williams LLP, *Live from Jerusalem*].

benefits and concerns associated with online behavioral advertising.[155] Similarly, the Accountability Principle encouraged members of the industry to "develop and implement policies and programs to further adherence to [the Industry Guidelines]," and stated that these programs should "have mechanisms by which they [could] police entities engaged in online behavioral advertising and help bring [non-compliant] entities into compliance."[156]

[37] Despite the FTC's efforts to adopt a regulatory model that would be flexible in response to innovation, some argued that the FTC did not go far enough.[157] For example, FTC Commissioner J. Thomas Rosch argued that the best way to protect online consumer privacy was for the United States to adopt a regulatory framework like the European Union's overarching approach to privacy instead of the existing sectoral approach to privacy legislation.[158]

[38] Nonetheless, FTC Commissioner (now Chairman) Jon Leibowitz issued a Concurring Statement to the FTC Guidelines, which stated that the agency's endorsement of self-regulation was not a "regulatory

[155] *See* Industry Guidelines, *supra* note 149, at 2.

[156] *Id.* at 4.

[157] *See, e.g.*, HARBOUR CONCURRENCE, *supra* note 12, at 1 (stating the FTC Guidelines "while commendable, focus[] too narrowly" and she would prefer a "more comprehensive approach to privacy.").

[158] *See* Rosch, *supra* note 78, at 8 (acknowledging that Europeans view the American approach to online behavioral advertising as "a cavalier attitude toward . . . 'spying'"). The European Union, unlike the United States, has data privacy rules that apply broadly across all industries. *See* DEP'T OF COMMERCE INTERNET POLICY TASK FORCE, COMMERCIAL DATA PRIVACY AND INNOVATION IN THE INTERNET ECONOMY: A DYNAMIC POLICY FRAMEWORK 11-12 (2010) [hereinafter COMMERCE DEP'T PRIVACY FRAMEWORK], *available at* http://www.ntia.doc.gov//reports/2010/IPTF_Privacy_GreenPaper_12162010.pdf. By contrast, the United States "protects personal data through a sectoral framework . . . . that uses voluntary enforceable codes of conduct . . . together with strong sectoral privacy laws covering certain information categories such as health, finance, education, and information about children." *Id.* at 11-12 (citations omitted).

retreat."[159] Instead, he stated that the industry should view the guidelines as its "last clear chance to show that self-regulation can – and will – effectively protect consumers' privacy in a dynamic online marketplace."[160] Therefore, the FTC hoped that the threat of regulation – should voluntary self-regulation not be successful in ensuring greater protection of online consumer privacy – would "scare" companies into taking self-regulation seriously.[161]

C. New Frameworks for Online Consumer Privacy: Recent FTC and Department of Commerce Reports

1. Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers (Preliminary FTC Staff Report)

[39] Approximately two years after the release of its guidelines for self-regulation in online behavioral advertising, the FTC published a preliminary staff report, *Protecting Consumer Privacy in an Era of Rapid Change* (the "Report"), which broadly addresses consumer privacy both on and offline.[162] Based on a series of roundtable discussions the agency held with members of the industry and Congress, the Report encourages companies to provide real-time notification of behavioral tracking and includes recommendations for providing "clear and meaningful ways for

[159] FED. TRADE COMM'N, FTC STAFF REPORT: SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING – CONCURRING STATEMENT OF COMMISSIONER JON LEIBOWITZ 1 (2009) [hereinafter LEIBOWITZ CONCURRENCE], *available at* http://www.ftc.gov/os/2009/02/P085400behavadleibowitz.pdf.

[160] *Id.*

[161] *See id.*

[162] *See* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS i (2010) [hereinafter FTC PROPOSED PRIVACY FRAMEWORK], *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

consumer to have more control and choice over information collected about them online."[163]

[40] At the 2010 International Conference of Data Protection and Privacy Commissioners, Director Vladeck spoke about the Report and emphasized that it highlights the need for consumer education so that consumers are fully aware of what behavioral advertising is, when it is happening, and how they can control their information.[164] In addition, the Report concludes that neither of the existing privacy models – the "notice-and-choice" and the "harm-based" models – have kept up with the rapidly evolving technologies that businesses use to collect and manipulate consumer data.[165]

[41] First, the notice-and-choice model sought to "encourage[] companies to develop privacy notices describing their [data] collection and use practices to consumers, so that consumers [could] make informed choices . . . ."[166] However, this approach became problematic because, over time, privacy notices grew more complex and difficult for consumers to understand.[167] In addition, very few companies gave consumers any opportunity to the control the collection and use of their personal information.[168] As a result, the notice-and-choice model "place[d] too

[163] Juliana Gruenwald, *FTC Privacy Report May be Released by Late October*, NATIONAL JOURNAL (Sept. 29, 2010, 12:08 PM), http://techdailydose.nationaljournal.com/2010/09/ftc-privacy-report-may-be-rele.php (internal quotation marks omitted); *see* FTC PROPOSED PRIVACY FRAMEWORK, *supra* note 162, at ii.

[164] *See* Hunton & Williams LLP, *Live from Jerusalem*, *supra* note 154.

[165] *See* FTC PROPOSED PRIVACY FRAMEWORK, *supra* note 162, at iii ("[T]he notice-and-choice model . . . has led to long, incomprehensible privacy policies that consumers typically do not read," while the harm-based model fails to compensate privacy-related injuries, like damage to one's reputation or "fear of being monitored.").

[166] *Id.*

[167] *See id.* at 19.

[168] *Id.*

much burden on consumers to read and understand privacy notices and make privacy choices."[169]

[42] Second, the harm-based model aimed to "protect[] consumers from specific harms" like "physical security, economic injury, and unwanted intrusions into their daily lives."[170] However, this model is often maligned for its failure to take into account reputational injury and other privacy-related harms.[171] Therefore, because "[c]onsumers may feel harmed when their personal information . . . is collected, used, or shared without their knowledge or consent or in a manner that is contrary to their expectations,"[172] the FTC recognized that "there is a pressing need to reexamine the conception of 'harm' in U.S. law . . . ."[173]

[43] Based on those conclusions, the Report proposes a new framework centered on three key principles.[174] The first principle, Privacy by Design, contends that online advertisers and all businesses that collect consumer data should do more to protect consumer privacy "on the front end," by incorporating additional privacy protections into their day-to-day business operations.[175] The second principle, Simplified Choice, states that companies should ensure that their data collection and retention practices align with consumers' expectations, while offering consumers a real, clear

[169] Hunton & Williams LLP, *Live from Jerusalem*, *supra* note 154.

[170] FTC PROPOSED PRIVACY FRAMEWORK, *supra* note 162, at iii.

[171] *Id.*

[172] *Id.* at 20 (citing Joel R. Reidenberg, *Privacy Wrongs in Search of Remedies*, 54 HASTINGS L.J. 877, 881 (2003)).

[173] Hunton & Williams LLP, *Live from Jerusalem*, *supra* note 154.

[174] *See generally* FTC PROPOSED PRIVACY FRAMEWORK, *supra* note 162.

[175] *Id.* at 41, 44-52; Hunton & Williams LLP, *Live from Jerusalem*, *supra* note 154. Privacy by Design is an approach adopted by the Information and Privacy Commissioner of Ontario, Ann Cavoukian, Ph.D., which promotes that organizations adopt a proactive role in developing privacy protections. *See* FTC PROPOSED PRIVACY FRAMEWORK, *supra* note 162, at v n.3 (citing PRIVACY BY DESIGN, http://www.privacybydesign.ca (last visited Jan. 6, 2011)).

choice to opt-out, at the exact time they plan to collect consumers' personal information.[176] However, the FTC stated that companies need not provide consumers an opportunity to opt-out of data collection for "commonly accepted practices."[177] Commonly accepted data collection practices include the fulfillment of product orders, "internal operations" (i.e., customer service surveys), "fraud prevention," compliance with law enforcement, and, most controversially, "first-party marketing."[178]

[44] The third principle, Greater Transparency, concludes that "[c]ompanies should increase the transparency of their data practices."[179] Specifically, businesses should strive to provide consumers with short, clear, and easily understandable privacy notices.[180] In addition, the Report also states that companies should give consumers the ability to access information collected about them, so they can correct or modify inaccurate data.[181] Although the Report encourages companies to simplify their privacy policies dramatically, it acknowledges the challenges companies might face in implementing this principle, particularly in the "mobile

[176] *See* FTC PROPOSED PRIVACY FRAMEWORK, *supra* note 162, at 41; Hunton & Williams LLP, *Live from Jerusalem*, *supra* note 154.

[177] FTC PROPOSED PRIVACY FRAMEWORK, *supra* note162, at 41, 52-69.

[178] *Id.* at 53-54; *see supra* Part II.B (describing the difference between first-party marketing and cookie-based behavioral advertising). First-party marketing can be controversial because companies might share consumer data with their affiliates, when consumers are unaware of the extent of a company's network of affiliates; however, the FTC explicitly stated that "[i]f a company shares data with a third party other than a service provider acting on the company's behalf – including a business affiliate unless the affiliate relationship is clear to consumers through common branding or similar means – the company's practices would not be considered first-party marketing." FTC PROPOSED PRIVACY FRAMEWORK, *supra* note 162, at 55.

[179] *Id.* at 41; Hunton & Williams LLP, *Live from Jerusalem*, *supra* note 154.

[180] FTC PROPOSED PRIVACY FRAMEWORK, *supra* note 162, at 41-42; Hunton & Williams LLP, *Live from Jerusalem*, *supra* note 154.

[181] *See* FTC PROPOSED PRIVACY FRAMEWORK, *supra* note 162, at 74-75.

context where, because of the small size of the device, a privacy notice can be spread out over 100 separate screens."[182]

[45] Finally, the Report also advocates for the creation of a Do-Not-Track list, akin to the Do-Not-Call registry, which established a limit on telemarketing calls made to residences.[183] Nonetheless, the FTC can only recommend, rather than mandate, a Do-Not-Track list unless Congress provides the agency with additional rule-making authority.[184] Privacy advocates and members of the advertising industry also debate whether it would even be technologically feasible to establish such a mechanism.[185] However, immediately following the FTC's release of the Report, Microsoft announced that Internet Explorer 9, which it plans to release shortly, incorporates "Tracking Protection," a feature allowing "consumers to determine the types of third-parties that can track their [w]eb behavior."[186]

---

[182] *Id.* at 70-71.

[183] *See id.* at 66; *see also* HARBOUR CONCURRENCE, *supra* note 12 at 5 n.11 (discussing the interest of privacy advocates in creating a Do-Not-Track List); Edward Wyatt & Tanzina Vega, *Stage Set for Showdown on Online Privacy*, N.Y. TIMES, Nov. 9, 2010, http://www.nytimes.com/2010/11/10/business/media/10privacy.html; Wendy Davis, *FTC Considers Do-Not-Track List*, ONLINE MEDIA DAILY (July 27, 2010, 6:21 PM), http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=132700.

[184] Davis, *Do-Not-Track System Lacks Mandate*, *supra* note 12 ("[T]hough the FTC is considering recommending such a system, *the agency lacks the authority to mandate do-not-track*. Yes, the FTC can certainly say it thinks Web companies should figure out a way to implement a universal do-not-track program, but can't do much more absent legislation." (emphasis added)); *see also* FTC PROPOSED PRIVACY FRAMEWORK, *supra* note 162, at 66 (acknowledging that a Do-Not-Track List could be instituted by self-regulation, but would likely require legislation).

[185] *See* Sara Jerome, *Public Interest Groups, Advertisers at Odds over Feasibility of 'Do Not Track' List*, HILLICON VALLEY: THE HILL'S TECHNOLOGY BLOG (Oct. 21, 2010, 2:07 PM), http://thehill.com/blogs/hillicon-valley/technology/125235-sides-disagree-on-technological-ease-of-do-not-track (stating that consumer advocates "say the obstacles to the [Do-Not-Track] system are policy-related and not technological," but digital advertisers claim the system would be difficult to implement because online tracking methods are constantly evolving).

[186] Juan Martinez, *Microsoft Says Internet Explorer 9 Will Include Behavioral Advertising Opt-Out*, DIRECT MARKETING NEWS (Dec. 8, 2010),

[46] Notably, in the Report, the FTC did not ask Congress for additional rule-making authority and did not endorse any of the privacy bills introduced by legislators.[187] Instead, the FTC appeared to recognize that privacy legislation is still premature – asking stakeholders to respond to more than fifty questions for comment.[188] This lack of clarity suggests that the FTC believes legislators should wait for more information before they move forward with privacy legislation.

2. Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework (Department of Commerce Internet Policy Task Force)

[47] The FTC is not the only administrative agency that recently published a report regarding the collection of consumer data online.[189] In December 2010, the Department of Commerce, at the direction of the Obama Administration, released a green paper on commercial data privacy.[190] Prior to its release, the Department of Commerce Assistant Secretary Lawrence Strickland stated that the green paper was not "a final position statement, but rather the beginning of a 'dialogue' that would lead to an official administration policy on information privacy."[191] Nonetheless, the Department's green paper aims to provide the administration with suggestions for establishing a new framework for Internet privacy, including recommendations for potential legislation.[192]

---

http://www.dmnews.com/microsoft-says-internet-explorer-9-will-include-behavioral-advertising-opt-out/article/ 192420/; *see* Tanzina Vega, *Microsoft, Spurred by Privacy Concerns, Introduces Tracking Protection to its Browser*, N.Y. TIMES, Dec. 7, 2010, http://www.nytimes.com/2010/ 12/08/business/media/08soft.html;

[187] *Cf.* FTC PROPOSED PRIVACY FRAMEWORK, *supra* note 162, at vii-viii.

[188] *See* FTC PROPOSED PRIVACY FRAMEWORK, *supra* note 162, at app. A.

[189] *See* Wyatt & Vega, *supra* note 183.

[190] *See generally* COMMERCE DEP'T PRIVACY FRAMEWORK *supra* note 158.

[191] Julia Angwin, *Watchdog Planned for Online Privacy,* WALL ST. J., Nov. 11, 2010, http://online.wsj.com/article/SB10001424052748703848204575608970171176014.html.

[192] *See* COMMERCE DEP'T PRIVACY FRAMEWORK, *supra* note 158, at i.

A newly established task force headed by Cameron Kerry will endeavor to turn the recommendations into federal policy.[193]

[48] Specifically, the green paper recommends the establishment of "a baseline privacy framework" through legislation that will "afford protection for consumers, and . . . clarify the U.S. approach to privacy to [the United States'] trading partners – all without compromising the current framework's ability to accommodate new technologies."[194] Currently, the privacy statutes in the United States reflect a sectoral approach to consumer privacy, which represents a legislative effort to tailor privacy protections to the individual industries being regulated.[195] However, according to the Department, this flexible approach has created "gaps" in privacy law, into which "[m]uch of the personal data traversing the Internet falls . . . ."[196] Thus, the green paper recommends updating the Fair Information Practice Principles[197] so that privacy protections would extend to data not currently covered under existing statutory frameworks.[198] In addition, the green paper also proposes that once these baseline protections exist, it might not be necessary to enact additional

[193] Angwin, *supra* note 190; Lance Whitney, *White House Wants to Beef up Internet Privacy Laws*, CNET (Nov. 12, 2010, 8:30 AM), http://news.cnet.com/8301-1009_3-20022650-83.html.

[194] COMMERCE DEP'T PRIVACY FRAMEWORK, *supra* note 158, at 2-3; *see also* Christopher Wolf, *Summary of Draft Department of Commerce Privacy Green Paper*, HOGAN LOVELLS CHRONICLE OF DATA PROTECTION (Nov. 15, 2010), http://www.hldataprotection.com/2010/11/articles/general/summary-of-draft-department-of-commerce-privacy-green-paper/ [hereinafter Wolf, *Summary of Privacy Green Paper*].

[195] *See* COMMERCE DEP'T PRIVACY FRAMEWORK, *supra* note 158, at 11-12 (citing the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Pub. L. No. 104-191, and the Gramm-Leach-Bliley Act ("GLBA"), 15 U.S.C. §§ 6801, 6809, 6821, 6827, as examples of sector-specific privacy bills).

[196] *Id.* at 12.

[197] *See infra* note 226 and accompanying text.

[198] *See* COMMERCE DEP'T PRIVACY FRAMEWORK, *supra* note 158, at 22.

legislation tailored to specific industries.[199] Rather, the FTC could enforce voluntary industry codes of conduct through its existing authority under § 5 of the FTC Act.[200]

[49] Like the FTC's recent report, the Commerce Department's report does not endorse any of the existing privacy legislation.[201] Moreover, the Department's green paper recognizes that, "[i]n many areas, the current combination of sectoral laws and general FTC Section 5 enforcement works well to protect the privacy of individuals."[202] And, although the report recommends the creation a new federal office, the Privacy Policy Office, to develop and implement new federal policies concerning commercial data privacy, it states that the FTC should remain the primary enforcer in matters concerning online consumer privacy.[203] However, in those areas where the current system is not as effective, the green paper states that a new, dynamic approach is necessary to ensure that stronger privacy protections are achieved, but not at the expense of online innovation.[204]

[199] *See id.* at 41-44 ("Voluntary, enforceable codes of conduct should address emerging technologies and issues not covered by [the] current application of baseline [Fair Information Practice Principles.]").

[200] *See* 15 U.S.C. § 45(a)(2); COMMERCE DEP'T PRIVACY FRAMEWORK, *supra* note 158, at 41-44.

[201] COMMERCE DEP'T PRIVACY FRAMEWORK, *supra* note 158, at 20-21.

[202] *Id.* at 68.

[203] *See id.* at 44-52.

[204] *See id.* at 46.

IV. THE NEXT STEP IN CONSUMER PRIVACY: THE INTRODUCTION OF PRIVACY LEGISLATION AND INDUSTRY EFFORTS TO PREVENT IT

A. Recently-Introduced Privacy Legislation: BEST PRACTICES Act and Boucher-Stearns Privacy Discussion Draft

[50] Within the last year, several members of the House Committee on Energy and Commerce introduced online privacy legislation.[205] In May 2010, Representatives Rick Boucher and Cliff Stearns released the first of these bills, a discussion draft of privacy legislation that aimed to regulate the collection and use of consumer information by online behavioral advertisers and other media providers.[206] Approximately two months later, Representative Bobby Rush introduced the BEST PRACTICES Act, which has a similar purpose.[207] Several Senators, notably Mark Pryor, John Kerry, and John McCain, are working on online privacy legislation.[208] Senator Pryor's legislation would mandate the creation of a Do-Not-Track list that would allow consumers to permanently "opt-out of having their [w]eb activities tracked for advertising purposes,"[209] while the

[205] *See Hearing on H.R. 5777*, *supra* note 14, at 1-2 (statement of Rep. Henry A. Waxman, Chairman, H. Comm. on Energy & Commerce).

[206] *See* Boucher-Stearns Privacy, H.R. ___, 111th Cong. (as published by H. Subcomm. on Commc'ns, Tech., & the Internet, May 4, 2010) (Staff Discussion Draft), *available at* http://stearns.house.gov/UploadedFiles/privacy_staff__discussion__draft.pdf; s*ee also* Press Release, Cong. Rep. Cliff Stearns, *supra* note 15.

[207] *See* BEST PRACTICES Act, *H.R. 5777, 111th Cong. (as reported by H. Comm. on Energy and Commerce, July 19, 2010) supra* note 17.

[208] *See* Press Release, Senator John Kerry, Kerry, McCain Introduce Commercial Privacy (Apr. 12, 2011), *available at* http://kerry.senate.gov/press/release/?id= 59a56001-5430-4b6d-b476-460040de027b; Juliana Gruenwald, *Measure Would Give Consumers More Control over Web Tracking*, NATIONAL JOURNAL (Sept. 30, 2010, 2:43 PM), http://techdailydose.national journal.com/2010/09/measure-would-give-consumers-m.php [hereinafter Gruenwald, *Control Over Web Tracking*]; Hunton & Williams LLP, *Senator Kerry's Senior Advisor Provides Key Insight into Forthcoming Privacy Bill*, PRIVACY & INFORMATION SECURITY LAW BLOG (Dec. 10, 2010), http://www.huntonprivacyblog.com/2010/12/articles/centre-for-information-policy-2/senator-kerrys-senior-advisor-provides-key-insight-into-forthcoming-privacy-bill/ [hereinafter Hunton & Williams LLP, *Senior Advisor*].

[209] Gruenwald, *Control Over Web Tracking*, *supra* note 208.

privacy bill introduced by Senators Kerry and McCain seeks to establish the baseline privacy framework advocated by the Commerce Department's recent green paper.[210] Nonetheless, Congress's purpose in enacting any form of online privacy legislation would likely be to "make people more likely to trust electronic commerce and the [I]nternet," without stifling innovation in the online advertising industry.[211]

[51] The Boucher-Stearns Privacy Discussion Draft includes several key provisions conferring additional responsibilities on online advertising and additional privacy rights on individuals.[212] For example, the Draft would require companies that collect personally identifiable information about consumers to display a "clear and conspicuous," and easily understandable privacy policy that describes how companies collect, use, and disclose consumer data.[213] Among other things, the Draft also provides that "an individual has a reasonable expectation that a company will not share that person's information with unrelated third parties," and requires companies to obtain express consent before sharing that information with third-party advertisers.[214] Finally, the Draft grants the

[210] Press Release, Senator John Kerry, *supra* note 209; Hunton & Williams LLP, *Senior Advisor*, *supra* note 208; *see also supra* Part III.C (discussing the Commerce Department's December 2010 privacy report).

[211] Avi Goldfarb & Catherine E. Tucker, Privacy Regulation and Online Advertising 32 (Aug. 5, 2010) (unpublished manuscript) (quoting Cecilia Kang, *New Bill on the Way for Online Privacy*, WASH. POST (Sept. 8, 2009, 10:10 AM), http://voices.washingtonpost.com/posttech/2009/09/new_bill_on_way_for_online_pri.htm), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1600259.

[212] *See* Press Release, Cong. Rep. Cliff Stearns, *supra* note 15.

[213] *See* Boucher-Stearns Privacy, H.R. ___ §§ 2(5), 3(a) 111th Cong. (as published by H. Subcomm. on Commc'ns, Tech., & the Internet, May 4, 2010) (Staff Discussion Draft), *available at* http://stearns.house.gov/UploadedFiles/privacy_staff__discussion__draft.pdf (describing the personally identifiable information included in the definition of "covered information"). The bill refers to personally identifiable information, like names, physical addresses, social security numbers as "covered information;" however, notably, the definition also includes other data ordinarily referred to as non-personally identifiable information, such as IP addresses and user preferences. *Id.*

[214] Press Release, Cong. Rep. Cliff Stearns, *supra* note 15.

FTC additional rule-making authority and states that a violation of the bill's provisions is an unfair and deceptive act under Section 5 of the FTC Act.[215] Nonetheless, although the Draft extends the FTC's enforcement authority, it explicitly precludes a private right of action.[216]

[52] However, in the 2010 mid-term elections, Congressman Rick Boucher lost his congressional seat.[217] When Republicans took over the majority in the House of Representatives, many members of the industry hoped that takeover would spell the end of potential legislation regarding online consumer privacy and behavioral advertising.[218] Yet, Republican legislators have made clear that privacy is a bipartisan issue.[219] In fact,

---

[215] Boucher-Stearns Privacy, H.R. ___ § 8(a)(1)-(3), 111th Cong. (as published by H. Subcomm. on Commc'ns, Tech., & the Internet, May 4, 2010) (Staff Discussion Draft), *available at* http://stearns.house.gov/UploadedFiles/privacy_staff__discussion__draft.pdf.

[216] *Id.* § 9.

[217] *See* Hunton & Williams LLP, *Key Voice on Privacy Issues Loses Congressional Reelection Bid While Another Joins the Senate*, PRIVACY & INFORMATION SECURITY LAW BLOG (Nov. 3, 2010), http://www.huntonprivacyblog.com/2010/11/articles/online-privacy/key-voice-on-privacy-issues-loses-congressional-reelection-bid-while-another-joins-the-senate/; Mike Shields, *Online Privacy Bill: Dead in the Water?*, ADWEEK (Nov. 4, 2010), http://www.adweek.com/aw/content_display/news/politics/e3if13877e698a1cce2faa1baf6cc66750a; Christopher Wolf, *What the US Election Results Mean for Privacy*, HL CHRONICLE OF DATA PROTECTION (Nov. 3, 2010), http://www.hldataprotection.com/2010/11/articles/general/what-the-us-election-results-mean-for-privacy/ [hereinafter Wolf, *US Election Results*].

[218] *See* Shields, *supra* note 217 ("The Interactive Advertising Bureau, which has spent the past two years rallying the online ad industry to take the regulation threat seriously, isn't hiding its pleasure at [the 2010 election] results.").

[219] *See* Press Release, Senator John Kerry, Kerry, McCain Introduce Commercial Privacy (Apr. 12, 2011), *available at* http://kerry.senate.gov/press/release/?id= 59a56001-5430-4b6d-b476-460040de027b; *see also* Sara Jerome, *Analysts: Privacy Bills Will Survive the Election Storm*, HILLICON VALLEY: THE HILL'S TECHNOLOGY BLOG (Nov. 1, 2010, 1:45 PM), http://thehill.com/blogs/hillicon-valley/technology/126829-online-privacy-to-remain-an-issue-for-gop-or-dem-led-house (noting that Congressman Cliff Stearns has demonstrated a "'serious concern about ensuring American consumers are fairly treated when they go online.'" (quoting Jeff Chester, Exec. Dir., Ctr. for Digital Democracy)); Shields, *supra* note 217 ("Privacy appeals to both lefty progressives and Tea Partiers."

Republican Congressman Joe Barton stated shortly after the 2010 elections that he would be "'very, very willing to legislate in [the privacy] area.'"[220] Additionally, House Democrats remain equally committed to moving forward on privacy legislation.[221] Representative Bobby Rush, author of the BEST PRACTICES Act, sought to oversee the House Subcommittee on Communications, Technology and the Internet.[222] This displays his commitment to pursuing online privacy legislation actively and, perhaps, additional efforts he will take to garner support for the BEST PRACTICES ACT.[223]

[53] Unlike the Boucher-Stearns Privacy Discussion Draft, the BEST PRACTICES Act received outspoken support from the members of the online media industry.[224] Recently, Intel, eBay and Microsoft voiced their support for the BEST PRACTICES Act, stating:

(statement of Jeff Chester, Exec. Dir., Ctr. for Digital Democracy)); Wolf, *US Election Results*, *supra* note 217.

[220] *The Communicators: Rep. Joe Barton (R-TX)* (C-SPAN television broadcast Nov. 6, 2010), *available at* http://www.cspan.org/Events/Rep-Joe-Barton-R-TX/19686-1/; *Barton "Very, Very Willing to Legislate*," IAPP DAILY DASHBOARD (Nov. 8, 2010), https://www.privacyassociation.org/publications/2010_11_08_barton_very_very_willing_to_legislate/.

[221] Cecilia Kang, *House to Hold Do Not Track Hearing on Internet Privacy*, POST TECH (Nov. 15, 2010, 5:10 PM), http://voices.washingtonpost.com/posttech/2010/11/the_house_subcommittee_for_com.html.

[222] *See* Tony Romm, *Rush Wants to Lead Tech Panel Dems*, POLITICO (Nov. 12, 2010, 4:36 PM), http://www.politico.com/news/stories/1110/45053.html.

[223] *See id.*

[224] *See* Juliana Gruenweld, *Three Major Tech Firms Back Rush's Privacy Bill*, TECH DAILY DOSE (Oct. 7, 2010, 1:59 PM), http://techdailydose.nationaljournal.com/2010/10/thee-major-tech-firms-back-rus.php [hereinafter Gruenweld, *Three Major Tech Firms*]; *Privacy Bills Comparison Chart*, CTR. FOR DEMOCRACY & TECH., 1-12 (2010), http://www.cdt.org/files/pdfs/Privacy bills comparison chart_CDT_0.pdf (supplementing Leslie Harris' testimony before the House Committee on Energy and Commerce, Subcommittee on Commerce, Trade, and Consumer Protection on "The BEST PRACTICES Act of 2010 and Other Federal Privacy Legislation"). *Contra* Tony Romm, *supra* note 222 (describing the ensuing debate between both critics and supporters over legislation addressing the collection of consumer information on the web).

> We support the bill's overall framework, which is built upon the Fair Information Practices regime. We appreciate that the BEST PRACTICES Act is technology neutral and gives flexibility to the Federal Trade Commission to adapt to changes in technology . . . . The bill also strikes the appropriate balance by providing businesses with the opportunity to enter into a robust self-regulatory program.[225]

Despite their general support for the BEST PRACTICES Act, the companies voiced concerns about the bill's private right of action, which would likely cause "unnecessary litigation costs and uncertainty for businesses."[226] Therefore, they urged Representative Rush to remove that provision from his bill.[227]

[54] In general, the BEST PRACTICES Act is more inclusive than the Boucher-Stearns Privacy Discussion Draft.[228] For example, the Draft

[225] Gruenweld, *Three Major Tech Firms*, *supra* note 224; *see also* FED. TRADE COMM'N, FAIR INFORMATION PRACTICE PRINCIPLES, *available at* http://www.ftc.gov/reports/privacy3/fairinfo.shtm. The Fair Information Practices are "the rights and responsibilities associated with the transfer and use of personal information." DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 657 (3d ed. 2009). They include the following: (1) Collection limitation ("There must be no personal data record keeping systems whose very existence is secret."); (2) Disclosure ("There must be a way for an individual to find out what information about him is in a record and how it is used."); (3) Secondary usage ("There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent."); (4) Record correction ("There must be a way for an individual to correct or amend a record of identifiable information about him."); and (5) Security ("Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data."). *Id.* at 655-57 (citing DEP'T OF HEALTH, EDUC. & WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS: REPORT OF THE SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS 29-30, 41-42 (1973)).

[226] Gruenweld, *Three Major Tech Firms*, *supra* note 225 (citation omitted) (internal quotations marks omitted).

[227] *Id.*

[228] *See generally Privacy Bills Comparison Chart*, *supra* note 224.

applies only to companies that collect sensitive data directly from consumers, exempting businesses that utilize data collected by other companies.[229] By contrast, the BEST PRACTICES Act applies not only to companies that collect consumer data online, but also to companies that handle the information, like data brokers.[230] Additionally, the BEST PRACTICES Act contains a broader definition of "sensitive information," and specifically includes all types of "geolocation information," [231] which has been at the heart of many recent legal disputes.[232]

[55] Another notable difference between the two bills is that the Boucher-Stearns Privacy Discussion Draft lacks a provision requiring online behavioral advertisers to conduct internal audits and develop other accountability mechanisms.[233] By contrast, the BEST PRACTICES Act

---

[229] *See* Boucher-Stearns Privacy, H.R. ___ § 2(4), 111th Cong. (as published by H. Subcomm. on Commc'ns, Tech., & the Internet, May 4, 2010) (Staff Discussion Draft), *available at* http://stearns.house.gov/UploadedFiles/privacy_staff__discussion__draft.pdf.

[230] *See* The BEST PRACTICES Act, H.R. 5777 § 2(3), 111th Cong. (as reported by H. Comm. on Energy & Commerce, July 19, 2010); *see also Privacy Bills Comparison Chart*, *supra* note 225, at 1.

[231] *See Privacy Bills Comparison Chart*, *supra* note 225, at 2. *Compare* Boucher-Stearns Privacy, H.R. ___ § 2(10), 111th Cong. (as published by H. Subcomm. on Commc'ns, Tech., & the Internet, May 4, 2010) (Staff Discussion Draft), *available at* http://stearns.house.gov/UploadedFiles/privacy_staff__discussion__draft.pdf (defining sensitive information as one's medical records, race or ethnicity, religious beliefs, sexual orientation, financial records, and precise location), *with* The BEST PRACTICES Act, H.R. 5777 § 2(8), 111th Cong. (as reported by H. Comm. on Energy and Commerce, July 19, 2010) (defining sensitive information as including any information about one's medical history, physical or mental health, or the provision of health care, race or ethnicity, religious beliefs or affiliation, sexual orientation or sexual behavior, income, financial records, or financial status, information about an individual's location or activities and relationships association with an individual's location, biometric data like fingerprints or retina scans, and social security numbers).

[232] *See generally* United States v. Maynard, 615 F.3d 544, 555-66 (D.C. Cir. 2010) (discussing whether individuals have a reasonable expectation of privacy regarding geolocation data of their whereabouts, like GPS coordinates).

[233] *See Privacy Bills Comparison Chart*, *supra* note 224, at 9.

includes several accountability provisions.[234] First, entities covered by the BEST PRACTICES Act must "provide a process for individuals to make complaints concerning the covered entity's policies and procedures . . . ."[235] In addition, covered entities must also conduct privacy assessments "prior to the implementation of commercial projects, marketing initiatives, business models, applications, and other products and services" if the entity concludes that the practice will result in the collection of data from more than one million consumers.[236]

[56] The accountability provisions in the BEST PRACTICES Act are of particular importance because they dovetail with the industry's efforts to increase accountability in online behavioral advertising through new compliance programs.[237] Furthermore, since it appears that neither the Boucher-Stearns Privacy Discussion Draft nor the BEST PRACTICES Act will receive additional consideration for the next several months, the success of the industry's compliance program may directly influence the need and/or desire for Congress to enact formal legislation.[238] At the very least, the success of the industry's compliance program will determine

[234] *See id.*

[235] The BEST PRACTICES Act, H.R. 5777 § 302(a), 111th Cong. (as reported by H. Comm. on Energy & Commerce, July 19, 2010).

[236] *Id.* § 302(b).

[237] *See infra* Part IV.B. The Commerce Department also promoted accountability in it recent green paper, encouraging companies to conduct "privacy impact assessments (PIAs)" to "identify and evaluate privacy risks arising from the use of personal information." COMMERCE DEP'T PRIVACY FRAMEWORK, *supra* note 158, at 34.

[238] *See* Juliana Gruenwald, *Finding Common Ground, but No Agreement*, TECH DAILY DOSE (Sept. 24, 2010, 10:21 AM) [hereinafter Gruenwald, *Finding Common Ground*], http://techdailydose.nationaljournal.com/2010/09/finding-common-ground-but-no-a.php; Juliana Gruenwald, *Privacy Likely to Remain on Agenda in House Next Year*, TECH DAILY DOSE (Sept. 23, 2010, 1:35 PM), http://techdailydose.nationaljournal.com/2010/09/privacy-likely-to-remain-on-ag.php; Kashmir Hill, *Future of Privacy Forum Founder Does Not Expect Online Privacy Bills to Pass This Year*, Comment to *The Not-So Private Parts*, FORBES (Sept. 15, 2010, 5:53 PM), http://blogs.forbes.com/kashmirhill/2010/09/15/future-of-privacy-forum-head-does-not-expect-online-privacy-bills-to-pass-this-year/?boxes=Homepagechannels.

whether the legislation, if enacted, might actually change how companies protect consumer privacy online.

B. Industry Efforts to Enhance Self-Regulation of Online Behavioral Advertising

[57] Although the advertising and media industries first implemented their Self-Regulatory Guidelines for Online Behavioral Advertising in July 2009,[239] critics argue that the self-regulatory model has not been effective.[240] Moreover, until recently, the industry had taken no real action in response to the FTC's directives to increase transparency and provide consumers with more control over the collection of data regarding their online activities.[241]

[58] Following the introduction of the Boucher-Stearns Privacy Discussion Draft and the BEST PRACTICES Act, however, several advertising industry trade associations announced a new coalition, the Digital Advertising Alliance, formed to oversee a new phase in the industry's self-regulatory efforts.[242] As part of the new initiative, the

[239] *See generally* Industry Guidelines, *supra* note 150150, at 12-18.

[240] *See* Ira S. Rubinstein, *Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes* 9-12 (Pub. Law & Legal Theory Research Paper Series, Working Paper No. 10-16, 2010), *available at* http://papers.ssrn.com/sol3/papers.cfrm?abstractid=1510275.

[241] *See* Robert D. Forbes, *Update: Internet Advertising Groups Launch Self-Regulation Program*, Comment to *Privacy Law Blog*, PROSKAUER (Oct. 5, 2010, 11:51 AM), http://privacylaw.proskauer.com/2010/10/articles/behavioral-marketing/update-internet-advertising-groups-launch-selfregulation-program/ [hereinafter Forbes, *Update*]; Tanzina Vega, *Ad Group Unveils Plan to Improve Web Privacy*, N.Y. TIMES, Oct. 4, 2010, http://www.nytimes.com/2010/10/04/business/media/04privacy.html [hereinafter Vega, *Ad Group*].

[242] Wendy Davis, *Industry Coalition Bows Self-Regulation Info Web Site, Readies New Trade Organization*, MEDIAPOSTNEWS (Sept. 30, 2010, 7:08 PM), http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=136831 [hereinafter Davis, *Industry Coalition*]. The "Digital Advertising Alliance" is currently comprised of seven trade associations, including the Interactive Advertising Bureau, American Association of Advertising Agencies, American Advertising Federation, Association of National Advertisers, Better Business Bureau, Direct Marketing Association, and the Network Advertising Initiative. *Id.*

Digital Advertising Alliance launched a website: http://www.aboutads.info.[243] Among other things, the website displays the Industry Guidelines for self-regulation in online behavioral advertising, offers information to companies about how to register for the self-regulatory compliance program, and, most importantly, educates consumers about what online behavioral advertising is and how they can control the collection of data regarding their online activity.[244]

[59] Principally, this phase of the industry's self-regulation efforts promotes the use of a universal icon, the "Power I," that publishers and advertisers can place *inside* advertisements to inform consumers about when behavioral tracking is taking place.[245] When consumers click on the icon, they "will be directed to a page explaining why they are seeing a particular advertisement and how to opt out of being tracked online."[246] This use of an icon:

> [R]epresents a major shift in how consumers are notified about a company's use of behavioral advertising. Historically, sites have included notice of their practices and consumers' choice with respect to them solely within their privacy policies. With the icon, both notice and choice will be presented in a far more clear and conspicuous manner.[247]

---

[243] DIGITAL ADVERTISING ALLIANCE, http://www.aboutads.info/ (last visited May. 9, 2011).

[244] *See id.*

[245] *See* Forbes, *Update*, *supra* note 241. The "Power I" icons are blue triangles, similar to "play" buttons, with the letter placed in the center, and are expected to go live on websites that comply with the program's requirements in the near future. *See* Davis, *Industry Coalition*, *supra* note 244.

[246] Forbes, *Update*, *supra* note 241.

[247] REED FREEMAN, JR., ET AL., MORRISON & FOERSTER, MORRISON & FOERSTER CLIENT ALERT: INDUSTRY ASSOCIATIONS LAUNCH BEHAVIORAL ADVERTISING SELF REGULATORY PROGRAM INVOLVING ICON, 2 (2010) [hereinafter MOFO CLIENT ALERT], *available at* http://www.mofo.com/files/Uploads/Images/101006-Behavioral-Advertising.pdf.

In addition, the language on the Digital Advertising Alliance's website is clearer than the traditional "legalese" included in online privacy policies.[248]

[60] "The compliance program, like the self-regulatory principles, is part of the industry's effort to demonstrate that no new privacy laws are needed."[249] Companies will instead be incentivized to maintain compliance with Industry Guidelines in exchange for use of the "Power I" icon on their website.[250] In fact, before a company can include the "Power I" icon in advertisements it distributes or posts on its website, the coalition requires a third party "Approved Provider" to ensure that the entity complies with the self-regulatory principles in the Industry Guidelines.[251] To participate in the compliance program, companies must also pay a registration fee and make a commitment, which may be enforceable by the FTC, to comply with the Industry Guidelines.[252] The Digital Advertising Alliance is not the only industry-generated effort to ensure compliance

[248] *Compare Understanding Online Advertising*, THE SELF REGULATORY PROGRAM FOR ONLINE BEHAVIORAL ADVERTISING, http://www.aboutads.info/consumers/ (last visited April 16, 2011), *with In re Gateway Learning Corp.*, 138 F.T.C. 443, 451-66, 2004 WL 5662254, at *4 (F.T.C. Sept. 10, 2004) (containing Gateway's online privacy policies).

[249] Davis, *Industry Coalition*, *supra* note 242.

[250] *See id.*

[251] *See Advertising Option Icon Application,* THE SELF REGULATORY PROGRAM FOR ONLINE BEHAVIORAL ADVERTISING, http://www.aboutads.info/participants/icon (last visited April 16, 2011) (instructing that a company must acquire the approval of an Approved Provider as evidence of compliance). Better Advertising was the first company designated as an Approved Provider to enforce compliance with the Self-Regulatory Principles of the Digital Advertising Alliance; *see, e.g.* Davis, *Industry Coalition*, *supra* note 241; Press Release, EVIDON, Digital Advertising Alliance Endorses Better Advertising as the First Approved Technology Provider for Industry Self-Regulatory Program (October 10, 2010), *available at* http://www.evidon.com/releases/daa_release.

[252] MOFO CLIENT ALERT, *supra* note 247, at 3.

with the FTC and Industry Guidelines.[253] Unlike the Digital Advertising Alliance's initiative, which is a non-profit coalition of industry trade organizations,[254] TRUSTe is a for-profit company that has also created an icon-based compliance program for online advertisers.[255]

[61] TRUSTe is a company that monitors the privacy policies of various websites to determine if they are adequate.[256] Once a privacy policy is certified, TRUSTe allows the website to place an icon on the website's home page.[257] Because of its background with privacy policies and compliance, TRUSTe has recently created a similar compliance program for the advertising industry, TRUSTed Ads.[258] Like the Digital Advertising Alliance's program, the TRUSTed Ads program utilizes an icon, which consumers can click on to access information regarding data collection for behavioral targeting purposes and "an easy-to-use opt-out option."[259] However, unlike the "Power I" icon, which will appear inside an advertisement,[260] the TRUSTed Ads icon will appear *adjacent* to the advertisement.[261] Therefore, consumers might not notice the TRUSTed Ads icon as easily as the "Power I" icon because, theoretically, an icon

[253] *See, e.g.,* Tom Foremski, *TRUSTe Tries to Manage the Massive Problem of Internet User Privacy*, ZDNET BLOG (Oct. 7, 2010, 5:05 AM), http://www.zdnet.com/blog/foremski/truste-tries-to-manage-the-massive-problem-of-internet-user-privacy/1523.

[254] *See* Davis, *Industry Coalition*, *supra* note 242.

[255] *See* Foremski, *supra* note 253.

[256] *Id.*

[257] *Id.*

[258] *See* Press Release, TRUSTe, TRUSTe Launches TRUSTed Ads Privacy Platform (Oct. 4, 2010), *available at* http://www.marketwire.com/press-release/TRUSTe-Launches-TRUSTed-Ads-Privacy-Platform-1329164.htm.

[259] *Id.*

[260] *See* Forbes, *Update*, *supra* note 241.

[261] *See* Press Release, TRUSTe, *supra* note 258.

that is out-of-place in a regular advertisement would stand out more than an icon placed outside the advertisement's border.

[62] These efforts at increased self-regulation have received considerable support from the industry, particularly in light of its desire to avoid regulation.[262] However, critics of self-regulation remain unconvinced, calling this effort "the latest version in a long series of failed self-regulatory efforts" and asking "the government to step in and set rules for the industry."[263] Despite the lack of enthusiasm among privacy watchdogs and regulators about the industry's recent efforts to further the self-regulatory model, recent studies suggest that this program could be the perfect middle ground.[264] First, Evidon (formerly Better Advertising), one of the companies enforcing compliance with the Digital Advertising Alliance's program,[265] released a research study examining how consumers interacted with advertisements containing the "Power I" icon and how that interaction affected their views of the brand advertised.[266] The study confirmed that consumers do, in fact, have a strong desire for the transparency in data collection practices and control over their information that the FTC and the Industry Self-Regulatory Guidelines call

[262] *See* Vega, *Ad Group*, *supra* note 241 (describing how members of the industry as "a big step forward," but "privacy advocates say self-regulation is not enough").

[263] *Id.* (citation omitted) (internal quotation marks omitted).

[264] *See* Scott Klass, *Research: Consumers Feel Better About Brands that Give Them Transparency and Control over Ads*, EVIDON BLOG (Nov. 10, 2010, 2:30 PM), http://blog.evidon.com/2010/11/10/research-consumers-feel-better-about-brands-that-give-them-transparency-and-control-over-ads/; Tanzina Vega, *Studies Find Success in Use of Privacy Icons*, N.Y. TIMES MEDIA DECODER BLOG (Nov. 16, 2010, 9:00 AM) [hereinafter Vega, *Studies*], http://mediadecoder.blogs.nytimes.com/2010/11/16/studies-find-success-in-use-of-privacy-icons/; *see also* John Eggerton, *Brill: FTC Will Monitor Behavioral Ad Self-Regs*, MULTICHANNEL NEWS BLOG (Oct. 22, 2010, 9:41 AM), http://www.multichannel.com/article/458855-Brill_FTC_Will_Monitor_Behavioral_Ad_Self_Regs.php.

[265] Scott, *Better Advertising's Assurance Platform Endorsed by Digital Advertising Alliance*, EVIDON BLOG (Oct. 4, 2010, 11:30 AM), http://blog.evidon.com/2010/10/04/better-advertisings-assurance-platform-endorsed-by-the-digital-advertising-alliance/.

[266] *See* Klass, *supra* note 265.

for.[267] For example, 76 percent of consumers wanted information about which companies were involved in targeting advertisements they received.[268] In addition, nearly 90 percent of respondents also wanted full control over their information (i.e., they "want to be able to pick and choose which individual companies to opt out of.").[269]

[63] Nonetheless, the Evidon/Better Advertising study also revealed that consumers responded positively to the "Power I" icon, with 67 percent of consumers "feel[ing] better about brands when they [were] given more 'control' by those brands, including the ability to opt out" of having their data collected.[270] Likewise, 36 percent of participants stated they were more likely to purchase products from brands that were transparent about their data collection practices.[271]

[64] However, the highlight of the study for members of the behavioral advertising industry was that even if consumers viewed the "Power I" icon in their ads and received a clear opportunity to opt-out, the opt-out rate was "extremely low [at] 0.0001 percent."[272] Essentially, after learning about behavioral targeting associated with a given advertisement, only one person in every thousand consumers chose not to allow online advertisers to continue collecting his data.[273] As a result, the survey's coordinators argued that the participation in the Digital Advertising Alliance's program would not hurt online advertisers; in fact, the study showed that

[267] *See id*; *see also* FTC SELF-REGULATORY GUIDELINES, *supra* note 8, at 46 (stating that behavioral advertisers should "provide a clear, concise, consumer-friendly, and prominent statement" about the types of data collected and information about how consumers can opt-out of having their data collected); Industry Guidelines, *supra* note 150, at 2-3, 12-14.

[268] Klass, *supra* note 264.

[269] *Id.*

[270] *Id.*

[271] *Id.*

[272] *Id.*

[273] Klass, *supra* note 264.

"providing evidence of compliance" with the FTC and Industry Guidelines "can build brands and help generate [a] better ROI [return on investment]."[274]

[65] Similarly, a second research study, conducted jointly by TRUSTe and the Publishers Clearing House, examined the effectiveness of the TRUSTed Ads program.[275] For the study, TRUSTe placed its TRUSTed Ads icon near ads displayed on a Publishers Clearing House website.[276] Clicking on the icon placed near the ad redirected consumers to a website that explained targeted advertisements and offered consumers a means to learn more about the ads as well as an opportunity to opt-out of receiving them.[277]

[66] First, the study revealed that people were much more likely to click on the TRUSTed Ads icon than they were to click on a website's privacy policy.[278] Second, the study also showed that "more than half of the people who saw the icon and clicked through" found the information about the targeting advertisements "helpful."[279] Finally, like the Better Advertising study, only a small percentage of visitors exercised the option to opt-out of all behavioral targeting.[280]

[67] Although the results of these studies seem focused on garnering additional participation in the self-regulatory programs by members of the

[274] *Id*.

[275] Press Release, TRUSTe, *supra* note 258; Vega, *Studies*, *supra* note 264.

[276] Vega, *Studies*, *supra* note 264.

[277] *Id.*

[278] *Id.* ("The click-through rate on the icon was 2.5 percent higher than the click-through rate on privacy policies.").

[279] *Id.*

[280] *Id.* ("[V]ery few visitors, 1.1 percent, chose to opt out of all advertising networks.").

behavioral advertising industry,[281] they also represent a clear attempt to demonstrate that privacy legislation is still premature. In fact, these studies reflect increasing efforts by members of the behavioral advertising industry to show the government that the use of in-ad icons could be the most effective means of informing consumers about advertisers' data collection practices, giving them a real opportunity to control the collection and use of their information without hindering innovation.[282]

C. The Industry's New Self-Regulatory Programs Expand the FTC's Role and Make Recently Proposed Privacy Bills Unnecessary

[68] Though privacy advocates continue to insist that legislation is necessary to provide adequate protection for online consumer privacy, the industry's recent efforts to improve the self-regulatory model offer the FTC a new opportunity to bring enforcement actions against online advertisers, without the aid of formal regulation.[283] Currently, the FTC does not bring enforcement actions against online behavioral advertisers if they disclose the collection and use of data about consumers' online activities in their privacy policies.[284] Therefore, they are not engaging in a deceptive practice, unless they misinform or mislead customers about how they collect or use that information.[285] In addition, it is difficult for the FTC to utilize its unfairness authority to attack behavioral advertising, because although consumers may suffer some abstract harm due to the collection of information about their online activity, consumers do receive

---

[281] *See, e.g.*, Vega, *Studies*, *supra* note 264 (quoting TRUSTe's President, who stated, "This [study] is to tell Industry, 'Do a good job on this, because [it's] really not going to hurt your business.'").

[282] *See generally* Klass, *supra* note 264; Vega, *Studies*, *supra* note 264.

[283] *See* MOFO CLIENT ALERT, *supra* note 247, at 3 (noting that the downside of participating in the industry's compliance program is that the commitment to abide by the Industry's Self-Regulatory Guidelines is an enforceable agreement subject to enforcement under § 5 of the FTC Act); Vega, *Ad Group*, *supra* note 241.

[284] *See* note 78 and accompanying text.

[285] *See, e.g.*, *In re* Gateway Learning Corp., 138 F.T.C. 443, 474-75, 2004 WL 5662254 (F.T.C. Sept. 10, 2004).

an offsetting benefit – like the ability to read online newspapers without a paid subscription.[286]

[69] However, by participating in either of the industry's compliance programs and placing icons in or near advertisements they publish or distribute, companies that engage in behavioral advertising will be making material representations to the public that their data collection practices comply with the Industry (and, effectively, the FTC) Guidelines.[287] Therefore, if a company displays either the "Power I" or TRUSTed Ads icon and, in fact, fails to comply with the privacy principles set forth in the FTC and Industry Guidelines, the FTC can bring an enforcement action against the entity under its authority to prohibit deceptive practices.[288]

[70] Using similar reasoning, the FTC has brought numerous enforcement actions against companies that have asserted compliance with the U.S.-EU Safe Harbor Agreement in their website's privacy policy and, yet, failed to remain compliant with the program.[289] "The U.S.-EU Safe Harbor Framework provides a method for U.S. companies to transfer personal data outside of Europe that is consistent with the requirements of

[286] *See* JOHN BATTELLE, *supra* note 42, at 194 (describing behavioral advertising as the "quid pro quo" for free online services); HARBOUR CONCURRENCE, *supra* note 12, at 1 (acknowledging that consumers receive access to numerous, "free" online services in exchange for the collection of personal information); *see also infra* Part III.C.1.

[287] *See* MOFO CLIENT ALERT, *supra* note 247, at 4; *see also* FTC Statement on Deception, *supra* note 99, at *192 (stating that an express claim is necessarily material under the FTC's deception authority because companies do not include material in advertising unless it is likely to affect a consumer's choice).

[288] *See* 15 U.S.C. § 45(a)(1). *See generally* FTC Statement on Deception, *supra* note 99, at *167-93.

[289] *See, e.g.*, *In re* Collectify LLC, No. 092-3142, 2009 WL 3239634 (F.T.C. Oct. 6, 2009); *In re* Directors Desk LLC, No. 092-3140, 2009 WL 3239632 (F.T.C. Oct. 6, 2009); *In re* Expatedge Partners, LLC, No. 092-3138, 2009 WL 3239629 (F.T.C. Oct. 6, 2009); *In re* Onyx Graphics, Inc., No. 092-3139, 2009 WL 3239631 (F.T.C. Oct. 6, 2009); *In re* Progressive Gaitways LLC, No. 092-3141, 2009 WL 3239633 (F.T.C. Oct. 6, 2009); *In re* World Innovators, Inc., No. 092-3137, 2009 WL 3239628 (F.T.C. Oct. 6, 2009).

the European Union Directive on Data Protection ("Directive")."[290] The Directive, which became effective in 1998, is a comprehensive approach to privacy legislation that, ordinarily, would prevent companies from transferring personal data to non-European Union nations unless those nations met European standards for consumer privacy protection.[291] However, to ensure that U.S. companies could:

> [S]atisfy the EU adequacy standard for certain commercial transfers, the U.S. Department of Commerce . . . and the [European Commission] negotiated the U.S.-EU Safe Harbor Framework, which went into effect in 2000. The Safe Harbor allows U.S. companies to transfer personal data lawfully from the EU. To join the Safe Harbor, a company must self-certify to Commerce that it complies with seven principles and related requirements that have been deemed to meet the EU's adequacy standard.[292]

[71] As part of the Safe Harbor program, the Department of Commerce maintains a website, which lists all the companies who have notified the agency of past or current compliance with the U.S.-EU Safe Harbor Framework.[293] "An organization's self-certification . . . and its appearance on this list pursuant to the self certification, constitute a representation to the Department of Commerce and the public that it adheres to a privacy policy that meets the safe harbor framework."[294] If a company self-

[290] *See, e.g.*, *In re Progressive Gaitways*, 2009 WL 3239633, at *1.

[291] *See* Issuance of Safe Harbor Principles and Transmission to European Commission, 65 Fed. Reg. 45,666 (July 24, 2000); Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 1, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML; *see also U.S.-EU Safe Harbor Overview*, EXPORT.GOV, *available at* http://www.export.gov/safeharbor/eu/eg_main_018476.asp (last updated Apr. 11, 2011).

[292] *In re World Innovators*, 2009 WL 3239628, at *1.

[293] *See Safe Harbor List*, EXPORT.GOV, http://www.safeharbor.export.gov/list.aspx (last visited Apr. 13, 2011).

[294] *Id.*

certifies to the Department of Commerce that its privacy practices comply with the U.S.-EU Safe Harbor Framework, then the certification lasts for a twelve-month period; however, the company must re-certify its compliance each year to remain "current."[295] In addition, next to each company on the Safe Harbor List, the Department displays information about whether the company has a current self-certification on file with the agency.[296]

[72] The FTC has authority to enforce compliance with the U.S.-EU Safe Harbor Framework under Section 5 of the FTC Act.[297] As previously mentioned, the Act provides that all "unfair or deceptive acts or practices in or affecting commerce" are illegal.[298] In addition, the FTC Act also gives the agency plenary power to bring enforcement actions against companies that engage in practices the Act proscribes.[299] Using this authority, the FTC has brought numerous enforcement actions against companies that have engaged in "deceptive practices" by falsely asserting compliance with the U.S.-EU Safe Harbor Framework.[300]

[73] For example, in 2009, the FTC filed an action against Progressive Gaitways, LLC for violating the FTC Act in connection with the U.S.-EU Safe Harbor Framework.[301] Progressive sold medical equipment online and, as early as 2007, began representing in its websites' privacy policies

[295] *See id.*

[296] *See id.*

[297] *See* 15 U.S.C. § 45; Issuance of Safe Harbor Principles and Transmission to European Commission, 65 Fed. Reg. 45,666 (July 24, 2000).

[298] 15 U.S.C. § 45(a)(1).

[299] *See id.* § 45(a)(2), (b).

[300] *See, e.g.*, *In re* Collectify LLC, No. 092-3142, 2009 WL 3239634, at *2 (F.T.C. Oct. 6, 2009); *In re* Directors Desk LLC, No. 092-3140, 2009 WL 3239632, at *2 (F.T.C. Oct. 6, 2009); *In re* Expatedge Partners, LLC, No. 092-3138, 2009 WL 3239629, at *2 (F.T.C. Oct. 6, 2009).

[301] *See In re* Progressive Gaitways LLC, No. 092-3141, 2009 WL 3239633, at *1 (F.T.C. Oct. 6, 2009).

that it participated in the Safe Harbor program.[302] However, although Progressive filed its self-certification of compliance with the Safe Harbor in 2004 and re-certified in 2005, it failed to renew its self-certification in 2006 and, thus, was listed on the Commerce Department's Safe Harbor List as "not current."[303] Consequently, because Progressive made material representations in its online privacy policies that it actively participated in the Safe Harbor program, when, in fact, it did not,[304] the FTC alleged that Progressive had engaged in a deceptive practice, in violation of the FTC Act.[305] Eventually, the FTC and Progressive negotiated a consent decree, under which Progressive agreed to refrain from making similar misrepresentations regarding its participation in any government and/or third party compliance programs in the future.[306]

[74] Like the FTC's Safe Harbor enforcement actions, even without the aid of additional privacy legislation, the agency can still bring enforcement actions against website operators and online behavioral advertisers that "mislead consumers about privacy . . . by failing to honor their privacy polices [as in *Gateway*], or circumventing users' opt-out preferences by, say, using Flash cookies to recreate deleted HTTP cookies."[307] Similarly, if a company represents through the use of "Power I" or TRUSTed Ads icons that they have complied with both the FTC and Industry Guidelines for the collection and use of data regarding consumers' online activities, the FTC can bring an enforcement action

[302] *See id.*

[303] *See id.* at *2.

[304] *See id.* at *2-3.

[305] *See id* at *3; *see also* 15 U.S.C. § 45(a).

[306] *See In re* Progressive Gaitways LLC, 2009 WL 3239633, at *3-5.

[307] Wendy Davis, *Self-Regulation Vs. Legislation: FTC, Commerce Dept. Set to Offer Differing Takes on Privacy*, THE DAILY ONLINE EXAMINER (Nov. 12, 2010, 6:30 PM), http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=139481 [hereinafter Davis, *Self-Regulation*].

against the entity under its authority to attack deceptive practices, if the company, in fact, fails to comply with the self-regulatory framework.[308]

[75] Thus, because of the online advertising industry's new compliance programs, the FTC's enforcement authority allows the agency to ensure that online behavioral advertisers comply with the self-regulatory principles.[309] As a result, the Boucher-Stearns Privacy Discussion Draft, the BEST PRACTICES Act, and similar privacy bills, if passed, will do nothing more than formalize the privacy framework already in place through the industry's enhanced version of self-regulation.

V. CONCLUSION

[76] The existing system of self-regulation allows the FTC to utilize a flexible approach to enforcement as new technologies and methods of behavioral advertising increase in popularity and create privacy concerns.[310] In addition, the advertising industry has only recently taken steps to ensure that its members comply with the FTC's self-regulatory model.[311] Thus, even though privacy advocates argue that it took the industry too long to take online consumer privacy seriously, regulators should wait and see if the industry's efforts are successful in creating widespread transparency regarding online advertisers' data collection practices. The FTC should also give the industry time to educate consumers, by providing clear privacy notices and showing consumers how they can control how data about their online activities is collected and used. At best, the recently-introduced privacy bills are likely to maintain the status quo; but, at worst, the bills could increase litigation and uncertainty costs for online advertisers and, as a result, stifle innovation.

[77] Therefore, the FTC should seize the opportunity the advertising industry's new compliance programs present. The agency should

[308] *See* 15 U.S.C. § 45(a)(1); FTC Statement on Deception, *supra* note 99, 175-83.

[309] *See* Davis, *Self-Regulation*, *supra* note 307.

[310] *See supra* Part III.B.

[311] *See supra* Part IV.B (discussing the advertising industry's reaction to the proposed legislation).

encourage all members of the online advertising industry to participate in these programs, work with the industry's existing initiatives to educate consumers about online privacy, and, finally, bring additional enforcement actions against online behavioral advertisers using their existing power to combat unfair and deceptive commercial practices. Based on recent industry efforts, the FTC can do all of these things now without the aid of additional rule-making authority or the assistance of new privacy legislation.