Northwestern Journal of Technology and Intellectual Property

Volume 8
Issue 1 *Fall*

Article 1

Fall 2009

Nobody Reads Your Privacy Policy or Online Contract? Lessons Learned and Questions Raised by the FTC's Action Against Sears

Susan E. Gindin

N O R T H W E S T E R N
JOURNAL OF TECHNOLOGY
AND
INTELLECTUAL PROPERTY

Nobody Reads Your Privacy Policy or Online Contract? Lessons Learned and Questions Raised by the FTC's Action Against Sears

Susan E. Gindin

Fall 2009 VOL. 8, NO. 1

Volume 8, Number 1 (Fall 2009)
Northwestern Journal of Technology and Intellectual Property

Nobody Reads Your Privacy Policy or Online Contract? Lessons Learned and Questions Raised by the FTC's Action Against Sears

Susan E. Gindin[*]

I. INTRODUCTION

¶1 In September 2009, the Federal Trade Commission ("FTC") issued a final consent order in the matter of Sears Holdings Management Corp. ("Sears") regarding the FTC's charges that Sears violated Section 5 of the FTC Act[1] in connection with a software application it offered as part of its "My SHC Community Program."[2] The software application (the "Tracking Application") allowed Sears to track consumers' online behavior, as well as some offline activities. When installed, the Tracking Application ran in the background on consumers' computers and transmitted tracked information to servers maintained on behalf of Sears. Information collected and transmitted included all of the consumers' web browsing (not just on Sears' sites), online purchases, business transacted during secure sessions, completion of online application forms, online checking accounts, and some of the consumers' web-based email and instant messages.

¶2 In most respects, Sears did what nearly fifteen years of legal decisions, with only a few exceptions, have indicated make an enforceable online contract and privacy policy, *namely*, that the consumer is given a reasonable opportunity to review the terms of the agreement and that the user indicates assent to the agreement.[3] For example, Sears included a Privacy Statement and User License Agreement ("PSULA") that described the Tracking Application in detail,[4] and before a consumer could install the Tracking Application, the consumer was required to check a box stating:

---

[*] Practitioner, Denver, Colorado, B.A., UCLA; M.S., Drexel University College of Information Science; J.D., State University of New York at Buffalo. I appreciate the helpful comments of Eric Goldman, Katherine Strandburg, Lee Tien, and Rebecca Tushnet.

[1] 15 U.S.C. §§ 41 et seq. (2006).

[2] Sears Holdings Mgmt. Corp., File No. 082 3099 (Fed. Trade Comm'n June 4, 2009), http://www.ftc.gov/os/caselist/0823099/index.shtm. The final consent order was issued on September 9, 2009. On June 4, 2009, the FTC announced that Sears agreed to enter into a settlement. Press Release, Fed. Trade Comm'n, Sears Settles FTC Charges Regarding Tracking Software (June 4, 2009), http://www.ftc.gov/opa/2009/06/sears.shtm. The FTC also announced the agreement in the *Federal Register* and opened the matter to public comment. The four comments that the FTC received are available on the FTC website at http://www.ftc.gov/os/publicomments.shtm.

[3] See *infra* Part III, for a review of court decisions regarding digital contracts.

[4] The description of the functions of the Tracking Application in the PSULA read:

> Computer hardware, software, and other configuration information: Our application may collect certain basic hardware, software, computer configuration and application usage information about the computer on which you install our application, including such data as the speed of the computer processor, its memory capacities and Internet connection speed. In addition, our application may report on devices connected to your computer, such as the type of printer or router you may be using.

> I am the authorized user of this computer and I have read, agree to, and have obtained the agreement of all computer users to the terms and conditions of the Privacy Statement and User License Agreement.

¶3 The Sears action was alarming in some respects in light of the long line of legal decisions upholding online contracts. Furthermore, as later discussed, it raises many questions regarding digital contracting, notice and consent, privacy, and advertising in the digital marketplace, which includes transactions via the Internet, mobile devices, and other digital platforms.[5]

A. Where Did Sears Go Wrong?

¶4 For years courts have upheld numerous online contracts against consumers. However, the FTC's enforcement action against Sears (the "Sears Matter" or "Sears Action") raises questions as to what is different about the Sears PSULA that would cause the FTC to bring an enforcement action.

¶5 First, it is important to note that the FTC enforcement action did not question whether the PSULA was enforceable, rather the FTC questioned whether Sears' actions were unfair or deceptive. Under the FTC Act, the FTC is charged with protecting consumers against unfair or deceptive acts or practices in or affecting commerce.[6] At times, the FTC identifies the kinds of practices it finds objectionable by bringing enforcement actions that establish compliance requirements for companies to follow in avoiding similar actions being brought against them in the future. Furthermore, as discussed in this Article, the FTC's actions in the Sears Matter are consistent with many

---

> Internet usage information: Once you install our application, it monitors all of the Internet behavior that occurs on the computer on which you install the application, including both your normal web browsing and the activity that you undertake during secure sessions, such as filling a shopping basket, completing an application form or checking your online accounts, which may include personal financial or health information. We may use the information that we monitor, such as name and address, for the purpose of better understanding your household demographics; however we make commercially viable efforts to automatically filter confidential personally identifiable information such as UserID, password, credit card numbers, and account numbers. Inadvertently, we may collect such information about our panelists; and when this happens, we make commercially viable efforts to purge our database of such information.
>
> The software application also tracks the pace and style with which you enter information online (for example, whether you click on links, type in webpage names, or use shortcut keys), the usage of cookies, and statistics about your use of online applications (for example, it may observe that during a given period of use of a computer, the computer downloaded X number of bytes of data using a particular Internet enabled gaming application).
>
> Please note: Our application does not examine the text of your instant messages or e-mail messages. We may, however, review select e-mail header information from web-based e-mails as a way to verify your contact information and online usage information.

Complaint at 4, Sears Holdings Mgmt. Corp., File No. 082 3099 (Fed. Trade Comm'n June 4, 2009), http://www.ftc.gov/os/caselist/0823099/index.shtm.

[5] *See infra* Part I.B. regarding the questions raised by the enforcement action.

[6] Federal Trade Commission Act, 15 U.S.C. §§ 41-58 (2006).

years of FTC policy, statements, and enforcement actions regarding the necessity for online businesses and advertisers to provide key disclosures that are clear and conspicuous, or "transparent."[7]

¶6 The essence of the FTC's complaint is that Sears did not adequately disclose the actual functions of the Tracking Application and that a reasonable understanding of the functions would be material to consumers when deciding whether to participate in the SHC Community. Sears' disclosures regarding the Tracking Application came too late in the process. First, consumers received extensive advertising material (including such enticements as "Get Advice Before You Buy," "Join the Community. It's Free!," "Talk to Us! We're Ready to Make Things Happen," and "Connect With Others") that did not describe the functions of the Tracking Application before consumers started the registration process.[8] Sears also offered $10 to consumers who kept the Tracking

---

[7] In some respects, Sears is a victim of timing. Although the FTC has indicated the need for providing disclosures transparently in the offline context at least since the 1970s and in the online context at least since 2000, the FTC made its emphasis on transparency in the online privacy context more clear beginning in 2007. Sears offered the Tracking Application between April 2007 and January 2008 and therefore had already launched the Tracking Application when the FTC indicated its emphasis on transparency in online privacy disclosures.

[8] As alleged by the FTC, Sears presented the opportunity to download the application to visitors to the sears.com and kmart.com websites as an opportunity to join a "My SHC Community" through a pop-up box that said:

> Ever wish you could talk directly to a retailer? Tell them about the products, services and offers that would really be right for you?
>
> If you're interested in becoming part of something new, something different, we'd like to invite you to become a member of My SHC Community. My SHC Community, sponsored by Sears Holdings Corporation, is a dynamic and highly interactive on-line community. It's a place where your voice is heard and your opinion matters, and what you want and need counts!

Complaint at 2, Sears Holdings Mgmt. Corp., File No. 082 3099 (Fed. Trade Comm'n June 4, 2009), http://www.ftc.gov/os/caselist/0823099/index.shtm. The pop-up advertisement did not mention the Application and neither did the general "Privacy Policy" statement which could be accessed via the hyperlink in the pop-up advertisement box. Consumers indicated their interest by providing their email addresses, and the email response stated the following (this time with some mention of tracking):

> From shopping, current events, social networking, to entertainment and email, it seems that the Internet is playing a bigger and bigger role in our daily lives these days.
>
> If you're interested in becoming part of something new, something different, we'd like to invite you to join a new and exciting online community; My SHC Community, sponsored by Sears Holdings Corporation. *Membership is absolutely free!*
>
> 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. My SHC Community gives you the chance to help shape the future by sharing and receiving information about the products, services and offers that would really be right for you.
>
> To become a member of My SHC Community, we simply ask you to complete the registration process which includes providing us with your contact information as well as

Application on their computers for at least 30 days, making the opportunity even more enticing. However, consumers did not have the opportunity to review the detailed description of the Tracking Application until they had taken multiple steps to register, and were then required to agree to the PSULA. Even then, the description of the functions of the Tracking Application did not appear until approximately the 75th line in the PSULA[9] which was presented to the consumer in a scroll box. In the Complaint against Sears, the FTC alleged:

> Respondent failed to disclose adequately that the software application, when installed, would: monitor nearly all of the Internet behavior that occurs on consumers' computers, including information exchanged between consumers and websites other than those owned, operated, or affiliated with respondent, information provided in secure sessions when interacting with third-party websites, shopping carts, and online accounts, and headers of web-based email; track certain non-Internet related activities taking place on those computers; and transmit nearly all of the monitored information (excluding selected categories of filtered information) to respondent's remote computer servers. *These facts would be material to consumers in deciding to install the software. Respondent's failure to disclose these facts, in light of the representations made, was, and is, a deceptive practice*. . . . The acts and practices of respondent as alleged in this complaint constitute unfair or deceptive acts or practices in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act.[10]

B. Lessons Learned and Questions Raised by the Enforcement Action

¶7 Although the Sears enforcement action provides some important lessons for online businesses and advertisers, it also brings uncertainty to electronic commerce. This Article refers to various digital platforms, including the Internet and mobile devices, as "online."

> answering a series of profile questions that will help us get to know you better. You'll also be asked to take a few minutes to download software that is powered by (VoiceFive). This research software will confidentially track your online browsing. This will help us better understand you and your needs, enabling us to create more relevant future offerings for you, other community members, and eventually all shoppers. You can uninstall the software at any time through the Add/Remove program utility on your computer.
>
> During the registration process, you'll learn more about this application software and you'll always have the opportunity to ask any and every question you may have.

Id. at 2-3; *see also* Ben Edelman, *The Sears "Community" Installation of ComScore*, Jan. 1, 2008, http://www.benedelman.org/news/010108-1.html (providing images of the advertising materials and PSULA acceptance process). Ben Edelman first called the matter to the FTC's attention. *See* PC World, *Researcher Accuses Sears of Spreading Spyware*, ABC NEWS, Jan. 2, 2008, http://abcnews.go.com/Technology/PCWorld/story?id=4074931.

[9] See note 4 for the description of the functions.

[10] Complaint at 5, Sears Holdings Mgmt. Corp., File No. 082 3099 (Fed. Trade Comm'n June 4, 2009), http://www.ftc.gov/os/caselist/0823099/index.shtm.

1. Lessons Learned

¶8 First, the FTC enforcement action indicates the types of disclosures required when businesses and advertisers offer products online. Terms which are likely material to consumers in deciding to participate in the service or order the product must be presented clearly and prominently. It may not be enough to present consumers with online contracts (no matter how completely they describe the product or service) if the material terms have not been presented clearly, prominently, and in a meaningful manner.

¶9 Second, with regard to online contracts and privacy notices, the Sears Action reflects a trend toward the requirement of shorter documents that are easier to read and understand. This may be difficult for various reasons, including the need to address complex legal requirements and technical issues in such documents. The FTC has experienced firsthand the difficulties of condensing online contracts and privacy notices. It has been part of several initiatives to find a notice format that consumers will read. An example is its initiative with banking regulators to draft form financial privacy policies that comply with Gramm-Leach-Bliley requirements.[11] As a result, it may be that a two-tier privacy notice may become standard. For example, in behavioral advertising, the FTC has recommended a two-tier approach for privacy notices with a brief initial notice to consumers, and with a link to a much more detailed document for consumers who want to learn more.[12]

¶10 Third, regarding privacy notices, the Sears Action is a reminder that the FTC will require enhanced notice particularly in regard to the collection and use of "sensitive" personal information.[13] As further discussed in Part V, although a definition of "sensitive data" has not yet been decided,[14] the FTC has indicated that, before collecting sensitive data, companies must obtain affirmative express consent from consumers. Affirmative express consent is also referenced as "opt-in," where the consumer specifically chooses or agrees to allow certain uses of their personal information. The opposite of opt-in is "opt out." An example is a pre-checked box or a statement where the company tells the consumer: "we'll use your data in this manner, unless you tell us otherwise." In the Sears Matter, the FTC indicated that the crux of the issue was the inadequately disclosed collection of sensitive data (including bank account information). The Decision and Order[15] required that Sears provide very detailed and specific disclosures to consumers

[11] Financial Services Modernization Act (Gramm-Leach-Bliley Act), 15 U.S.C. §§ 6801-09 (2006). *See* FTC Privacy Initiatives, Financial Privacy Rule: Interagency Notice Research Project, http://www.ftc.gov/privacy/privacyinitiatives/financial_rule_inrp.html (last visited July 30, 2009).

[12] As further discussed in this article, some consumers do not seem to care about online privacy; witness the amount of highly personal data posted to social networking sites. However, the FTC is concerned that consumers are unaware of the privacy considerations at stake—a situation which surely resulted in a case of the "consumer" being unaware that details posted to Facebook are not private. *See* Associated Press, *The U.K. Spy Chief Who Loved Facebook*, CBS NEWS, July 5, 2009, http://www.cbsnews.com/stories/2009/07/05/tech/main5135008.shtml.

[13] *See infra* Part V, for a discussion of the FTC's particular scrutiny regarding collection of sensitive data and sharing data with third parties.

[14] FED. TRADE COMM'N, FTC STAFF REPORT: SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING 42 (2009), *available at* http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf [hereinafter *2009 FTC Behavioral Advertising Report*].

[15] Decision and Order, Sears Holdings Mgmt. Corp., File No. 082 3099 (Fed. Trade Comm'n June 4, 2009), http://www.ftc.gov/os/caselist/0823099/index.shtm. See *infra* Part IV, for further details regarding the requirements of the Decision and Order.

before installation of any future Tracking Application regardless of whether the collected information could contain personal, financial, or health information.[16]

¶11 Fourth, this enforcement action signals the FTC's likely position in the current dialogue concerning whether or how behavioral advertising should be legislated. The FTC defines behavioral advertising or tracking as "the tracking of a consumer's online activities *over time* – including the searches the consumer has conducted, the web pages visited, and the content viewed – in order to deliver advertising targeted to the individual consumer's interests."[17] Although behavioral tracking has typically been reported to be anonymous, there are indications that information collected online is being combined with data collected offline. For example, as reported by the *New York Times*, certain companies are combining information collected offline with data collected online, and using it to serve even more targeted advertising.[18] Furthermore, according to the Electronic Frontier Foundation, social networks like Facebook, MySpace and LinkedIn make it easy for tracking applications to associate cookie and other data with "true name" using various techniques.[19] As these practices become more prevalent (or more publicized), extensive FTC scrutiny of the privacy policies of businesses that employ the services of such companies becomes more likely. Companies that have historically used privacy policies stating "we will never share your personally identifiable information," will need to be particularly careful to notify customers that their personally identifiable information will now be combined with data understood to be collected anonymously to serve more relevant advertising.[20]

¶12 Fifth, as to advertising disclosures, the Sears action serves as a reminder for advertisers about the necessity of providing effective disclosures to consumers. Advertising materials (and particularly those associated with the tracking of consumer personal data) should receive legal review to determine whether such materials comply with advertising legal requirements. Furthermore, the Sears Matter signals that advertising materials should be reviewed together with the terms of online contracts and privacy policies associated with the advertising campaign. Review will ensure that important disclosures are included clearly and conspicuously in advertising materials as well as in online contracts and/or privacy policies. The Sears PSULA likely would not have concerned the FTC if the advertising materials presented to the consumer had clearly and prominently disclosed the functions of the Tracking Application early in the process. As a practical matter, advertising is typically created shortly before its intended publication and lawyers are asked to review the advertising material under a tight time frame. However, the FTC's enforcement action will serve as a lesson that the consequences for using problematic advertising materials can be significant. Although

---

[16] *Id.*

[17] *2009 FTC Behavioral Advertising Report*, *supra* note 14, at 46.

[18] *See* Stephanie Clifford, *Ads Follow Web Users, and Get More Personal*, N.Y. TIMES, July 30, 2009, at A1, *available at* http://www.nytimes.com/2009/07/31/business/media/31privacy.html.

[19] Posting of Peter Eckersley to Electronic Frontier Foundation Deeplinks Blog, https://www.eff.org/deeplinks/2009/09/online-trackers-and-social-networks (Sept. 21, 2009) ("How Online Tracking Companies Know Most of What You Do Online (and What Social Networks Are Doing to Help Them)"); *see also* Posting of Seth Schoen to Electronic Frontier Foundation Deeplinks Blog, https://www.eff.org/deeplinks/2009/09/new-cookie-technologies-harder-see-and-remove-wide (Sept. 14, 2009) ("New Cookie Technologies: Harder to See and Remove, Widely Used to Track You").

[20] See *infra* Part VI, for more discussion of behavioral advertising including combining of personally identifiable information with the usually anonymous data collected online.

Sears was not fined by the FTC for its Tracking Application, the consequences of the enforcement action are considerable. Under the Decision and Order,[21] Sears has substantial reporting obligations to the FTC for four years, and is subject to steep fines if it violates the Decision and Order during the next twenty years. Fines can be considerable in enforcement actions.[22] Furthermore, even without a fine, dealing with an FTC enforcement action is very expensive, both in terms of legal expenses, and in time spent responding to FTC allegations.

¶13 Sixth, to some extent, the Sears Matter reflects a shift from the position that the consumer is legally responsible for his actions (and in fact has a duty to read legal documents[23]) to a more protective position. As discussed in this Article, studies show that the online consumer is impulsive and unlikely to consider the legal consequences of his or her online behavior.[24] Although there are likely many reasons why consumers are so "click-happy" online, free and instantaneous availability of many online resources probably contributes to this impulsiveness.[25] At the same time, the risk of blindly accepting online privacy notices has intensified because digital technologies enable companies to invisibly track consumers and amass huge amounts of consumer data without their knowledge. Therefore, the FTC has signaled its commitment to increase its consumer protection efforts particularly in the behavioral tracking realm.[26]

¶14 Seventh, from a consumer standpoint, the action is an important lesson for consumers that their inattention to the "fine print" may sometimes have serious unforeseen consequences. Sears' advertising suggested consumers would be joining an "online community" when in fact the Tracking Application effectively gave Sears the means to monitor personal data including bank accounts and prescription drug information. Similarly, people have inadvertently downloaded adware[27] along with free screensavers, games, and other utilities.[28] Still others have unwittingly duped their

---

[21] Decision and Order, Sears Holdings Mgmt. Corp., File No. 082 3099 (Fed. Trade Comm'n June 4, 2009), http://www.ftc.gov/os/caselist/0823099/index.shtm.

[22] For example, Zango agreed to settle its action with the FTC for $3 million. Zango, Inc., File No. 052 3130 (Fed. Trade Comm'n Nov. 3, 2006), http://www.ftc.gov/os/caselist/0523130/index.shtm.

[23] *See* Robert A. Hillman & Jeffrey J. Rachlinski, *Standard-Form Contracting in the Electronic Age*, 77 N.Y.U. L. REV. 429, 432 (2002) (asserting that although e-commerce changes some of the dynamics of standard-form contracting in interesting and novel ways and presents some new challenges, these differences do not call for the development of a radically different legal regime); *see also* Kaustuv M. Das, Comment, *Forum-Selection Clauses in Consumer Clickwrap and Browsewrap Agreements and the "Reasonably Communicated" Test*, 77 WASH. L. REV. 481 (2002).

[24] See *infra* Part V, for a discussion of studies showing that consumers uniformly do not pay attention to disclosures.

[25] *See generally* Hillman & Rachlinski, *supra* note 23 (suggesting many additional reasons why consumers do not pay attention to contracts, such as trust in the vendor).

[26] *See* Stephanie Clifford, *Fresh Views at Agency Overseeing Online Ads*, N.Y. TIMES, Aug. 4, 2009, at B1, *available at* http://www.nytimes.com/2009/08/05/business/media/05ftc.html; Douglas MacMillan, *The FTC Takes On Targeted Web Ads*, BUSINESSWEEK, Aug. 2, 2009, http://www.businessweek.com/technology/content/aug2009/tc2009082_486167.htm.

[27] Wikipedia describes adware as "any software package which automatically plays, displays, or downloads advertisements to a computer after the software is installed on it or while the application is being used." Wikipedia, *Adware*, http://en.wikipedia.org/wiki/Adware (last visited Aug. 6, 2009).

[28] *See, e.g.*, Press Release, Fed. Trade Comm'n, DirectRevenue LLC Settles FTC Charges, Will Give Up $1.5 Million in Ill-Gotten Gains for Unfair and Deceptive Adware Downloads (Feb. 16, 2007), *available at* http://www.ftc.gov/opa/2007/02/directrevenue.shtm (describing how DirectRevenue and its affiliates offered consumers free content and software, such as screensavers, games, and utilities, without disclosing adequately that downloading them would result in installation of adware which monitored consumers'

friends into enabling an email scraping operation because they did not read the "fine print."[29] As will be discussed, the FTC is pushing advertisers to include a consumer education component as part of their behavioral tracking initiatives. However, at some point, consumers should slow down to read and understand the provided disclosures before taking action online. After all, neither the clarity nor the prominence of the disclosures will matter if consumers are so anxious to partake in the online experience that they blindly click "I agree" to every offer.

2. Questions Raised

¶15 At the same time, the enforcement action also raises considerable questions. First, the Sears action raises substantial uncertainty in conducting business online. The result indicates online businesses must clearly and conspicuously disclose material terms, but it raises the question as to what terms are material (and therefore must be disclosed). Also, not all disclosures can be presented first. How does a company decide which disclosures to provide and in what order? Furthermore, some online formats provide very little room for disclosures. For example, it may be more difficult for companies to obtain effective consent from mobile device users.

¶16 Second, as discussed in Part IV, the FTC's requirements for any future Tracking Applications employed by Sears are very exacting and include stipulations that Sears provide certain detailed disclosures. These disclosures must be provided to the consumer on a distinct page prior to the display of an end user license agreement, privacy policy, terms of use, or similar document. The FTC has also placed similar requirements on other companies.[30] Is this the new standard for notice disclosure?

¶17 Third, as discussed in Part VI, although behavioral advertising has been traditionally based on anonymous data, companies are reportedly using data which is a combination of personally identifiable information ("PII") and so-called non-personally identifiable information ("non-PII")[31] collected online to serve more relevant targeted

---

Internet use in order to display targeted pop-up ads).

[29] An action was brought in July 2009 by the New York Attorney General against Tagged, a social networking site. According to the Attorney General, Tagged "scrapes" contact information in visitors' personal address books in order to send invitations to friends of the visitors, in emails disguised to make it appear as though a friend was inviting them to view personal photos. *See* Press Release, Office of the Attorney Gen., State of N.Y., Attorney General Cuomo Announces Legal Action Against Social Networking Site That Raided Email Address Books, Stole Identities, And Spammed Millions Of Americans (July 9, 2009), *available at* http://www.oag.state.ny.us/media_center/2009/july/july9a_09.html; *see also* Alina Tugend, *Typing In an E-Mail Address, and Giving Up Your Friends' as Well*, N.Y. TIMES, June 19, 2009, at B7, *available at* http://www.nytimes.com/2009/06/20/technology/internet/20shortcuts.html (describing the author's experience with Tagged).

[30] See the extended discussion of this issue in *infra* Part II; Zango, Inc., File No. 052 3130 (Fed. Trade Comm'n Nov. 3, 2006), http://www.ftc.gov/os/caselist/0523130/index.shtm.

[31] In fact, research has shown that there is really no such thing as non-personally identifiable information because nearly all so-called anonymized data can be linked to a particular person. *See* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. ___ (forthcoming 2010), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006 (identifying the failures of "anonymization" of personal information); s*ee also* Susan E. Gindin, *Lost and Found in Cyberspace: Informational Privacy in the Age of the Internet*, 34 SAN DIEGO L. REV. 1153, 1170 (1997) (discussing the ways online users may be identified individually); Posting of Seth Schoen to Electronic Frontier Foundation Deeplinks Blog, https://www.eff.org/deeplinks/2009/09/what-information-personally-identifiable (Sept. 11, 2009) ("What Information is 'Personally Identifiable'?").

advertisements. Especially in light of the FTC's emphasis on clear and conspicuous notice with regard to behavioral tracking, what type of privacy notice will the FTC find acceptable for companies using such services? Also, can notice and an opportunity to opt out be sufficient, or will companies be required to obtain express consent from consumers prior to such tracking? The Sears Matter suggests companies will be required to obtain express consent.

¶18 Fourth, as discussed in Part V, there is proposed legislation to regulate behavioral advertising, and the FTC seems increasingly likely to support such legislation. Is the time appropriate for such legislation?

¶19 Fifth, as discussed in Part V, studies show that consumers are unlikely to pay attention to any notices, from mortgage documents to privacy notices. What form of notice is most apt to capture consumer attention so that they are effectively informed?

¶20 This Article discusses the Sears Matter in light of the above learned "lessons" and questions raised. Part II discusses FTC policy and previous enforcement actions and statements; Part III reviews the enforceability of clickwrap agreements generally; Part IV focuses on the requirements for online disclosures, consents, and notices in light of the Sears Matter; and Part V focuses on privacy notices. Part VI of this Article examines the behavioral advertising dialogue and the effect of the Sears Matter, the fact that Congress is discussing legislation with more urgency, and the measures taken by the industry to address various behavioral advertising concerns. Finally, although it is very important that behavioral tracking be regulated in some manner, this Articles concludes that legislation is premature at this time and should be postponed at least for a few years to give self-regulatory principles a chance to work.[32]

II. THE SEARS ENFORCEMENT ACTION IS CONSISTENT WITH FTC POLICY AND WITH THE FTC'S PREVIOUS ENFORCEMENT ACTIONS

¶21 As noted, the Sears enforcement action is consistent with FTC policy and with the FTC's previous enforcement actions, statements, and guidelines. The FTC has long required that businesses clearly and conspicuously disclose material facts. The agency has maintained that an act or practice is deceptive and therefore a violation of the FTC Act if it is likely to mislead consumers acting reasonably under the circumstances, and is "material," that is, important to a consumer's decision to buy or use the product.[33]

¶22 What's more, the extensive tracking conducted by the Tracking Application raises consumer online privacy issues. The FTC took a very early role in online consumer protection and privacy issues, beginning with a workshop on consumer information privacy in June 1996[34] and with workshops, "town halls," reports, statements, and enforcement actions on privacy issues every year thereafter.

---

[32] In this Article, I use the terms "privacy policy" and "privacy notice" interchangeably, and I also use the terms "behavioral advertising," "behavioral marketing," "behavioral tracking," and "targeted marketing" interchangeably.

[33] FED. TRADE COMM'N, FTC POLICY STATEMENT ON DECEPTION (1983), *available at* http://www.ftc.gov/bcp/policystmt/ad-decept.htm.

[34] FED. TRADE COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS (1996), *available at* http://www.ftc.gov/reports/privacy3/priv-23a.pdf.

¶23 In 2000, the FTC issued *Dot Com Disclosures*,[35] important guidelines for online businesses and advertisers conducting business online. *Dot Com Disclosures* is a detailed tutorial regarding what makes advertising acceptable in an online setting, and a review is helpful in understanding the reasons the FTC took action against Sears. The primary focus of the tutorial is that all disclosures to consumers must be clear and conspicuous, and it provides a lengthy list of actions advertisers should take to ensure that disclosures are clear and conspicuous, including

> [p]lac[ing] disclosures near, and when possible, on the same screen as the triggering claim. Use text or visual cues to encourage consumers to scroll down a Web page when it is necessary to view a disclosure. . . .
>
> In evaluating whether disclosures are likely to be clear and conspicuous in online ads, advertisers should consider the *placement* of the disclosure in an ad and its *proximity* to the relevant claim. Additional considerations include: the *prominence* of the disclosure; whether items in other parts of the ad *distract attention* from the disclosure; whether the ad is so lengthy that the disclosure needs to be *repeated*; . . . and, whether the language of the disclosure is *understandable* to the intended audience.[36]

Along with publication of *Dot Com Disclosures*, the FTC further emphasized its policy regarding online disclosures by holding multiple and repeated workshops entitled *Green Lights & Red Flags: FTC Rules of the Road for Advertisers* in numerous U.S. cities in the 2000's.[37]

¶24 Following publication of *Dot* Com *Disclosures* and presentation of the *Green Lights* workshops, the FTC also indicated concern that online businesses and advertisers have not been making online disclosures clear and conspicuous. For example, in January 2007, the FTC held a Workshop on Negative Options[38] in which commentators indicated that traditional means of making disclosures and obtaining consumer acceptance of online terms may not be enough. At the Negative Options Workshop, commentators from the UC Berkeley School of Information presented results of a survey concluding that online vendors:

> [F]ace challenges in getting consumers to see and read their disclosures. The panelists revealed that many online consumers exhibit certain characteristics, including inattention, unwarranted confidence, exuberance, and a desire for immediate gratification, which make them less likely to see and read disclosures. Panelists further explained that, as result of these online characteristics, consumers become "click-happy" and quickly navigate through webpages,

---

[35] FED. TRADE COMM'N, DOT COM DISCLOSURES: INFORMATION ABOUT ONLINE ADVERTISING (2000), *available at* http://www.ftc.gov/bcp/edu/pubs/business/ecommerce/bus41.pdf [hereinafter *Dot Com Disclosures*].

[36] *Id.* at 1.

[37] Fed. Trade Comm'n, Green Lights & Red Flags: FTC Rules of the Road for Advertisers, http://www.ftc.gov/greenlights (last visited Oct. 21, 2009).

[38] A "negative option" is any provision under which the consumer's silence or failure to take an affirmative action to reject goods or services or to cancel the agreement is interpreted by the seller as acceptance of the offer. 16 C.F.R. § 310.2(t) (2009).

> without paying much attention because they believe nothing will go wrong and want to complete the transaction as rapidly as possible. As a result, consumers often do not read or understand the terms of the agreements they accept. To combat consumers' exuberance and inattention, the panelists recommended using short notices that include only the information material to consumers.[39]

Other commentators, including FTC staff, gave examples of what would constitute effective disclosures.[40]

¶25 In addition, the FTC brought enforcement actions against online businesses based partly on inadequate disclosure of material terms, including two which involved behavioral tracking software. In 2006, the FTC brought an action against Zango, Inc.,[41] and in 2007, the FTC brought an action against DirectRevenue[42] alleging that the companies offered consumers free content and software—such as screensavers, games, and utilities—without adequately disclosing that downloading the software would result in simultaneous installation of adware which monitored consumers' Internet use in order to display targeted pop-up ads. Zango settled with the FTC for $3 million[43] and DirectRevenue settled for $1.5 million.[44]

¶26 However, as next discussed, while the FTC has become increasingly active in requiring that companies provide conspicuous notice of material terms, the courts have almost unanimously enforced online contracts against consumers, even those with so-called "hidden terms."

III. CLICKWRAP AGREEMENTS

> Has this happened to you? You plunk down a pretty penny for the latest and greatest software, . . . 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 on 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, at least in the case described below . . . .[45]

---

[39] FED. TTRADE COMM'N, NEGATIVE OPTIONS: A REPORT BY THE STAFF OF THE FTC'S DIVISION OF ENFORCEMENT ii-iii (2009), *available at* http://www.ftc.gov/os/2009/02/P064202negativeoptionreport.pdf.

[40] *Id.*

[41] Zango, Inc., File No. 052 3130 (Fed. Trade Comm'n Nov. 3, 2006), http://www.ftc.gov/os/caselist/0523130/index.shtm.

[42] DirectRevenue LLC, File No. 052 3131 (Fed. Trade Comm'n Feb. 16, 2007), http://www.ftc.gov/os/caselist/0523131/index.shtm.

[43] Press Release, Fed. Trade Comm'n, Zango, Inc. Settles FTC Charges, Will Give Up $3 Million in Ill-Gotten Gains for Unfair and Deceptive Adware Downloads (Nov. 3, 2006), *available at* http://www.ftc.gov/opa/2006/11/zango.shtm.

[44] Press Release, Fed. Trade Comm'n, DirectRevenue LLC Settles FTC Charges, Will Give Up $1.5 Million in Ill-Gotten Gains for Unfair and Deceptive Adware Downloads (Feb. 16, 2007), *available at* http://www.ftc.gov/opa/2007/02/directrevenue.shtm.

[45] i.LAN Sys., Inc. v. NetScout Serv. Level Corp., 183 F. Supp. 2d 328, 329 (D. Mass. 2002). This case involved two businesses but the court's reference to his personal experience with "pesky legalese" that delays the installation of his software is apt.

¶27 The above quote from a 2002 Massachusetts case exemplifies the rulings in most of the cases which have reviewed contracts, like the Sears PSULA, for electronic products. Generally such contracts, which are referred to as "clickwrap" agreements,[46] have been found enforceable if the online business can demonstrate the consumer has had reasonable notice of the terms and the consumer has assented to the terms.[47]

¶28 One of the first judicial decisions regarding an electronic contract was *ProCD, Inc. v. Zeidenberg*,[48] decided by Judge Easterbrook on the Court of Appeals for the Seventh Circuit in 1996. Although it involved the acquisition of physical software, the decision set important principles for electronic agreements.[49] First, it acknowledged the enforceability of electronic contracts with standardized terms, where the user agrees by clicking on a box labeled "I agree" or something similar.[50] The court reasoned that since the defendant inspected the package, tried out the software, learned of the license, and did not reject the goods in accordance with the seller's proposed contract (which the buyer accepts by using the software after having an opportunity to read the license), the shrinkwrap license was valid under U.C.C. § 2-204(1), and the defendant had agreed to the terms when he did not reject the product (as provided in U.C.C. § 2-606).[51] Further, Judge Easterbrook indicated that the pop-up presentation type of clickwrap terms constitutes reasonable notice of the terms.[52] With this foundation, courts following *ProCD* have regarded clickwrap terms as equivalent to terms in boilerplate paper contracts, and have upheld most of the clickwrap agreements which have been challenged.

¶29 The first case involving an actual clickwrap agreement was also decided in 1996. In *CompuServe v. Patterson*,[53] the Court of Appeals for the Sixth Circuit held that uploading shareware onto a computer subjects the user to the jurisdiction where the computer is located. CompuServe sought a declaratory judgment in Ohio that its product, CompuServe Navigator, did not infringe defendants' trademark in "Windows Navigator." The court assumed without further discussion that the clickwrap agreements entered into were valid, stating that the defendant "entered into a *written* contract with CompuServe which provided for the application of Ohio law,"[54] and noting that the defendant had been

---

[46] *Id.* Clickwrap agreements are electronic agreements that require that consumers indicate assent by clicking an "I Accept," "Yes," or "I Agree" icon before proceeding to use the product or service. Another type of online contract is referred to as a browsewrap, which usually means a contract, posted online but which does not require the user to expressly manifest assent. *See* Christina L. Kunz et al., *Browse-Wrap Agreements: Validity of Implied Assent in Electronic Form Agreements*, 59 BUS. LAW. 279 (2003).

[47] Kunz et al., *supra* note 46, lists a number of cases demonstrating this. In addition: *see* Das, *supra* note 23; Nathan J. Davis, *Presumed Assent: The Judicial Acceptance of Clickwrap*, 22 BERKELEY TECH. L.J. 577 (2007); Margaret Jane Radin, *Boilerplate Today: the Rise of Modularity and the Waning of Consent*, 104 MICH. L. REV. 1223, 1231 (2005) (stating that the "traditional picture of contract" as "the time-honored meeting of the minds" has been transformed; that "[t]he idea of voluntary willingness first decayed into consent, then into assent, then into the mere possibility or opportunity for assent, then to merely fictional assent, then to mere efficient rearrangement of entitlements without any consent or assent"); Todd Rakoff, *The Law and Sociology of Boilerplate*, 104 MICH. L. REV. 1235 (2006).

[48] 86 F.3d 1447 (7th Cir. 1996).

[49] *See* Hillman & Rachlinski, *supra* note 23, at 487.

[50] *Id.*

[51] *ProCD*, 86 F.3d at 1452-53.

[52] Hillman & Rachlinski, *supra* note 23, at 488.

[53] 89 F.3d 1257, 1260-61 (6th Cir. 1996).

[54] *Id.* at 1264 (emphasis added).

required to type "'AGREE' at various points in the document, '[i]n recognition of your online agreement to all the above terms and conditions.'"[55]

¶30 Similarly, in 1998, the District Court for the Northern District of California upheld Terms of Service of the free e-mail site Homail, in *Hotmail Corporation v. Van Money Pie Inc.*[56] The court enjoined the defendants from sending spam in violation of Hotmail's contract, because in order to use Hotmail's service, defendants, after being given the opportunity to view the Terms of Service, clicked on a box indicating their assent to be bound.[57]

¶31 Generally, the only cases where a court refused to enforce a contract against the consumer were those cases where the user was not required to assent to the terms or was asked to consent to the terms only after he downloaded the product. For example, in *Williams v. America Online, Inc.*,[58] AOL subscribers' computers were allegedly damaged after they downloaded Version 5.0 of the AOL software (causing unauthorized changes to the configuration of their computers so they could no longer access non-AOL Internet service providers or access personal information and files).[59] The *Williams* court denied AOL's motion to dismiss the case based on the forum clause, because AOL required assent to the AOL terms *after* the subscribers downloaded the software. The court reasoned that since the customers had not had an opportunity to review or accept the online contract before starting the download, the contract did not apply.[60]

¶32 There has been much litigation regarding AOL's agreement (or lack of one in the *Williams* case), with some courts finding the AOL member agreement enforceable and others finding it unenforceable. In 1998, in *Groff v. America Online, Inc.*,[61] the Rhode Island Superior Court found the AOL contract binding because AOL's online contract acceptance procedure, required a user to first click on an "I agree" button indicating his assent to be bound by AOL's Terms of Service before he could access AOL's system. The court stated:

> [T]he general rule [is] that a party who signs an instrument manifests his assent to it and cannot later complain that he did not read the instrument or that he did not understand its contents. Here, plaintiff effectively "signed" the agreement by clicking "I agree" not once but twice. Under these circumstances, he should not be heard to complain that he did not see, read, etc. and is bound to the terms of his agreement.[62]

---

[55] *Id.*

[56] No. C98-20064, 1998 WL 388389 (N.D. Cal. Apr. 20, 1998).

[57] *Id.*

[58] No. 00-0962, 2001 WL 135825 (Mass. Super. Ct. Feb. 8, 2001).

[59] *Id.* at *2.

[60] *Id.*; *see also* Specht v. Netscape Commc'ns Corp., 306 F.3d 17 (2d Cir. 2002) (refusing to enforce Netscape's contract because a user downloading free software would not see the End User License Agreement covering the SmartDownload software posted on the Netscape site until *after* already initiating the download).

[61] No. PC 97-0331, 1998 WL 307001 (R.I. Super. Ct. May 27, 1998).

[62] *Id.* at *5; *see also* Caspi v. The Microsoft Network, L.L.C., 732 A.2d 528 (N.J. Super. Ct. App. Div. July 2, 1999) (upholding a forum selection clause in a clickwrap agreement, finding that the terms of this agreement appear in a scrollable window next to blocks containing the words "I agree" or "I disagree").

¶33 In fact, this position echoes the long-held acknowledgement that consumers generally do not read form contracts, yet are still bound to the terms of the agreement.[63] For example, in 1983, Todd D. Rakoff, in his article critical of adhesion contracts, wrote that traditional doctrine for the previous several decades constituted the following four propositions:

> (1) The adherent's signature on a document clearly contractual in nature, which he had an opportunity to read, will be taken to signify his assent and thus will provide the basis for enforcing the contract.
> (2) It is legally irrelevant whether the adherent actually read the contents of the document, or understood them, or subjectively assented to them.
> (3) The adherent's assent covers all the terms of the document, and not just the custom-tailored ones or the ones that have been discussed.
> (4) Exceptions to the foregoing principles are narrow. In particular, failure of the drafting party to point out or explain the form terms does not constitute an excuse. Instead, in the absence of extraordinary circumstances, the adherent can establish an excuse only by showing affirmative participation by the drafting party in causing misunderstanding.64

Although standardized contracts, whether in paper or electronic format, have been widely criticized because they are full of legalese, give users no bargaining power,[65] or are incomprehensible,[66] they have also been praised[67] and determined to be "essential." For

---

[63] *See* Arthur Allen Leff, *Contract as a Thing*, 19 AM. U. L. REV. 131, 157 (1970) ("[S]ome people would sign a contract even if 'THIS IS A SWINDLE' were embossed across its top in electric pink."); *see also* Michael I. Meyerson, *The Reunification of Contract Law: The Objective Theory of Consumer Form Contracts*, 47 U. MIAMI L. REV. 1263, 1269-70, 1275 (1993) ("It is no secret that consumers neither read nor understand standard form contracts. . . . Moreover, businesses hardly want the consumer to read form contracts.").

[64] Todd D. Rakoff, *Contracts of Adhesion: An Essay in Reconstruction*, 96 HARV. L. REV. 1174, 1185 (1983). The example of an exception given in the fourth point is particularly relevant here because the FTC likely would claim that Sears affirmatively participated in causing misunderstanding.

[65] *See id.*; John E. Murray, Jr., *The Standardized Agreement Phenomena in the Restatement (Second) of Contracts*, 67 CORNELL L. REV. 735, 740 (1982) ("This process does not deserve to be called contractual. It is not democratic and, in a society based on mass production which requires standardized forms even among competitors, it is essentially unfair.").

[66] *See, e.g.*, The Future of the Internet and How to Stop It, Facebook's Privacy Storm, http://futureoftheinternet.org/facebooks-privacy-storm (Feb. 18, 2009).

> One lesson is that plain English (and its other-language counterparts!) works better these days than legalese. When talented lawyers sit down to draft something like a set of terms of service, they naturally want terms that protect their client as much as possible — both in its current practices and for any future practices it could conceivably undertake. Plus they know that courts will hold this language against them in a dispute if there's any wiggle room, since the company itself drafted it and the users couldn't negotiate. So the writers tend to (1) reuse terms from other companies' agreements like old holiday fruitcakes getting passed around, since venerable terms must be good ones and (2) they write broadly and at length.

Id.

[67] *See* Richard Epstein, *Unconscionability: A Critical Reappraisal*, 18 J.L. & ECON. 293, 294-95 (1975) (arguing that courts interfere with efficient business practices).

instance, as noted in the Restatement (Second) of Contracts, Section 211, Comment (a), contracts with standardized terms are *essential* for mass production and distribution and beneficial to all:

> Scarce and costly time and skill can be devoted to a class of transactions rather than to details of individual transactions. Legal rules which would apply in the absence of an agreement can be shaped to fit the particular type of transaction. . . . Operations are simplified and costs are reduced, to the advantage of all concerned.[68]

They are particularly beneficial for companies offering products at little or no cost. Companies can contractually reduce their potential costs of dealing with disputes by requiring binding arbitration and/or prohibiting class actions to discourage consumers from suing, and pre-selecting a business-oriented tribunal and convenient forum.[69] Companies can then offer products less expensively (and often free) using such mass market contracts.[70]

¶34 However, while long accepting that standardized contracts may be beneficial, it was also expected that courts would offer redress in egregious situations, such as those involving fraud, or where enforcing the contracts would be unconscionable or against public policy.[71] The Restatement, section 211(3), specifically delineates situations where certain contract terms would be unexpected: "Where the other party has reason to believe that the party manifesting such assent would not do so if he knew that the writing contained a particular term, the term is not part of the agreement."[72] Some courts have looked more critically at clickwrap agreements, particularly in the context of unconscionability and violation of public policy. There has been a string of decisions based on California law,[73] all involving situations in which the consumers had consented to the terms of the contracts at issue.

¶35 An early example is *America Online, Inc. v. Superior Court* ("*Mendoza*")[74] which was decided in 2001. In *Mendoza*, a California state appellate court refused to uphold the forum selection provision in AOL's member agreement in a putative class action suit in which the plaintiffs claimed that AOL continued to charge their credit cards for membership fees after they canceled their memberships. The court held that the forum selection clause in the AOL contract was unenforceable because it was "unfair and unreasonable" and that the legal remedies of AOL's selected forum, Virginia, were not comparable to those in California. In addition, the court found that because one of the causes of action sought class action relief under California's Consumers Legal Remedies Act, which includes a provision that voids any purported waiver of rights under the act as being contrary to California public policy, enforcement of forum selection and choice of

---

[68] RESTATEMENT (SECOND) OF CONTRACTS § 211, cmt. a. (1979).
[69] Hillman & Rachlinski, *supra* note 23, at 439 (noting the various benefits of standardized agreements).
[70] *Id.*
[71] *Id.* at 456.
[72] RESTATEMENT (SECOND) OF CONTRACTS § 211(3) (1979).
[73] Unconscionability is judged somewhat differently across jurisdictions. *See* Kunz et al., *supra* note 46. In California, for instance, unconscionability must be both procedural and substantive.
[74] 90 Cal. App. 4th 1 (Cal. Ct. App. 2001).

law clauses in the contract "would be the functional equivalent of a contractual waiver of the consumer protections" under the Act and was thus prohibited under California law.

¶36 In *Comb v. PayPal, Inc.*,[75] which was decided in 2002, and which involved PayPal's clickwrap agreement, the U.S. District Court for the Northern District of California refused to uphold the arbitration clause in PayPal's contract against users who had filed a class action suit. The court determined that the PayPal contract was an adhesion contract and was both procedurally and substantively unconscionable under California law. The court stated:

> The procedural component can be satisfied by showing the existence of unequal bargaining positions and surprise through hidden terms common in the context of adhesion contracts. The substantive component can be satisfied by overly harsh or one-sided results that "shock the conscience."
>
> . . .
>
> A contract of adhesion, in turn, is a "standardized contract, which, imposed and drafted by the party of superior bargaining strength, relegates to the subscribing party only the opportunity to adhere to the contract or reject it."[76]

¶37 The court further explained that the contract and its arbitration clause were unconscionable because they: (1) permitted PayPal to make binding amendments to the User Agreement at any time without prior notice to users; (2) permitted PayPal to freeze and hold customer funds in customer accounts until any dispute is resolved; (3) required users to bring claims individually and to arbitrate their disputes pursuant to the commercial rules of the American Arbitration Association (which the Court found seemed to be an attempt by PayPal "to insulate itself contractually from any meaningful challenge to its alleged practices"[77]); and (4) required users throughout the U.S. to arbitrate in California where PayPal is located.[78]

¶38 Using similar reasoning, and applying California law, in 2007, in *Bragg v. Linden Research, Inc.*,[79] the District Court for the Eastern District of Pennsylvania cited *Comb. v. PayPal* when refusing to uphold an arbitration clause in a contract for virtual real estate on the virtual website Second Life. The court held that the procedural element of unconscionability also "focuses on . . . surprise."[80] In determining whether surprise exists, the court stated that California courts focus not on the plaintiff's subjective reading of the contract, but rather, more objectively, on "the extent to which the supposedly agreed-upon terms of the bargain are hidden in the prolix printed form drafted by the party seeking to enforce the disputed terms."[81] In *Gutierrez*,[82] the court had found such surprise where an arbitration clause was "particularly inconspicuous;" "printed in

---

[75] 218 F. Supp. 2d 1165 (N.D. Cal. 2002).
[76] *Id.* at 1171.
[77] *Id.* at 1176.
[78] *Id.* at 1176-77.
[79] 487 F. Supp. 2d 593 (E.D. Pa. 2007).
[80] *Id.* at 606 (quoting Gutierrez v. Autowest, Inc., 7 Cal. Rptr. 3d 267, 275 (Cal. Ct. App. 2003)).
[81] *Id.* at 606.
[82] Gutierrez v. Autowest, Inc., 7 Cal. Rptr. 3d 267 (Cal. Ct. App. 2003).

eight-point typeface on the opposite side of the signature page of the lease."[83] The *Linden* court went on to state: "Here, although the [Terms of Service] are ubiquitous throughout Second Life, Linden buried the TOS's arbitration provision in a lengthy paragraph under the benign heading 'GENERAL PROVISIONS.'"[84]

¶39 It is notable that in 2009, two federal courts refused to uphold clickwrap agreements against consumers suing for privacy issues. In *Doe 1 v. AOL LLC*,[85] an action was brought in California by AOL members alleging violations of federal electronic privacy law,[86] after AOL made publicly available the Internet search records of more than 650,000 of its members.[87] In this case, which was decided in January 2009, the Court of Appeals for the Ninth Circuit based its refusal to uphold the same forum provision in AOL's member agreement on the *Mendoza* case decided eight years earlier.[88]

¶40 In *Harris v. Blockbuster Inc.*,[89] decided in April 2009, the District Court for the Northern District of Texas refused to uphold the Blockbuster clickwrap agreement against a consumer who alleged that Blockbuster violated the federal Video Privacy Protection Act[90] by sharing information about her movie selections with third parties without first obtaining her consent.[91] The alleged violation arose out of Blockbuster's participation in Facebook's "Beacon" advertising program, which allowed companies partnered with Facebook to advertise by posting notices in Facebook users' "news feeds" when the user took an action, such as making a purchase from a third-party website that participated in the Beacon program. When the program originally launched, Facebook users had the right to opt-out, but, in response to consumer complaints, Facebook changed Beacon to an opt-in system, and later retired the system.[92] In *Harris*, which has been appealed to the Court of Appeals for the Fifth Circuit, the court ruled that because Blockbuster reserves the right to modify the Terms and Conditions, including the section that contains the arbitration provision, "at its sole discretion" and "at any time," and such modifications will be effective immediately upon being posted on the site, Blockbuster's arbitration provision in its clickwrap agreement is illusory, and thus unenforceable.[93]

¶41 Of course, two federal court cases do not make a trend, especially when one has been appealed, but it is notable that both 2009 cases noted above involve alleged violations of consumer privacy. They are otherwise exceptions to the general rule that clickwrap agreements and notices are enforceable as long as the user has a reasonable opportunity to review the terms of the agreement and the user indicates assent. Over the

---

[83] *Id.* at 276.
[84] Bragg v. Linden Research, Inc., 487 F. Supp. 2d 593, 606 (E.D. Pa. 2007).
[85] Doe 1 v. AOL LLC, 552 F.3d 1077 (9th Cir. 2009).
[86] 18 U.S.C. § 2702(a) (2006).
[87] *Doe 1*, 552 F.3d at 1083.
[88] *See supra* note 74.
[89] 622 F. Supp. 2d 396 (N.D. Tex 2009).
[90] 18 U.S.C. § 2710 (2006).
[91] The Act prohibits movie rental providers from disclosing consumers' personally identifiable information, including movie choices, to third parties without the informed written consent of the consumer at the time of the disclosure. 18 U.S.C. § 2710.
[92] Posting of David Sarno to L.A. Times Technology Blog, http://latimesblogs.latimes.com/technology/2009/09/facebook-beacon-advertising.html (Sept. 21, 2009, 6:39pm PST) (describing the pitfalls of Facebook's Beacon advertising program and its ultimate withdrawal).
[93] Harris v. Blockbuster Inc., 622 F. Supp. 2d 396, 400 (N.D. Tex 2009).

nearly fifteen years since the first case involving a clickwrap, there have been numerous additional cases upholding the validity of a variety of clickwrap agreement terms, for example, over arbitration or dispute resolution clauses,[94] forum selection clauses,[95] disclaimers of warranty,[96] and limitations of liability[97] provisions.

IV. REQUIREMENTS FOR ONLINE DISCLOSURES

¶42 Although some courts have taken a consumer-protective stance in the cases decided since the first clickwrap agreement over fourteen years ago, the majority have upheld clickwrap agreements against consumers. Companies have long relied on this fact in drafting contracts and privacy policies. However, the Sears Matter indicates that current industry standard practices for obtaining consent may no longer be appropriate, and that material terms can no longer be posted only in an online contract or privacy policy. As will be discussed, this is particularly true in situations where consumers would likely be surprised to learn of certain terms, and where advertising or other notices have given a misleading message.

¶43 Whether such contracts will be upheld against consumers in the future, it is clear that the FTC will take action if online disclosures, particularly those that would likely be material to consumers, are not clear and conspicuous. The requirements imposed by the Decision and Order are quite exacting. In accordance with the Decision and Order, Sears is prohibited from including material disclosures *only* in a privacy policy or user license agreement. The Decision and Order requires that, in connection with the advertising, promotion, offering for sale, sale, or dissemination of any Tracking Application, prior to the consumer downloading or installing it, Sears must:

> (1) Clearly and prominently, and prior to the display of, and ***on a separate*** screen from, any final "end user license agreement," "privacy policy," "terms of use" page, or similar document, disclose: (1) all the types of data that the Tracking Application will monitor, record, or transmit, including but not limited to whether the data may include information from the consumer's interactions with a specific set of websites or from a broader range of Internet interaction, whether the data may include transactions or information exchanged between the consumer and third parties in secure sessions,

---

[94] *See, e.g.*, *In re* RealNetworks, Inc., No. 00 C 1366, 2000 WL 631341 (N.D. Ill. May 8, 2000) (rejecting claim that arbitration clause in a click-wrap agreement was not enforceable; defendant's online click-wrap agreement was sufficient to meet the "writing" requirement of the Federal Arbitration Act).

[95] *See, e.g.*, Universal Grading Serv. v. eBay, Inc., No. 08-CV-3557, 2009 U.S. Dist. LEXIS 49841 (E.D.N.Y. June 10, 2009); Forrest v. Verizon Commc'ns, Inc., 805 A.2d 1007 (D.C. 2002) (upholding forum selection clause in Verizon's clickwrap where the plaintiff entered into an Internet access subscription by clicking the "Accept" button at the end of the agreement which was presented in a scroll box).

[96] *See, e.g.*, Scott v. Bell Atlantic Corp., 726 N.Y.S.2d 60 (N.Y. App. Div. 2001) *amended by* Goshen v. Mut. Life Ins. Co., 774 N.E.2d 1190 (N.Y. 2002) (upholding disclaimer of warranty for problematic DSL services despite extensive advertising regarding reliability).

[97] *See, e.g.*, A.V. v. iParadigms, LLC, 544 F. Supp. 2d 473 (E.D. Va. 2008) (enforcing limitation on liability in clickwrap agreement in copyright lawsuit brought by high school students required to submit their papers to Turnitin website limitation of liability provision, rejecting students' attempts to modify provision by disclaimer on papers), *aff'd*, 562 F.3d 630 (4th Cir. 2009).

interactions with shopping baskets, application forms, or online accounts, and whether the information may include personal financial or health information; (2) how the data may be used; and (3) whether the data may be used by a third party; and

(2) Obtain express consent[98] from the consumer to the download or installation of the Tracking Application and the collection of data by having the consumer indicate assent to those processes by clicking on a button or link that is not pre-selected as the default option and that is clearly labeled or otherwise clearly represented to convey that it will initiate those processes, or by taking a substantially similar action.[99]

¶44 Although the Decision and Order uses the terms "clear and prominent," rather than "clear and conspicuous" as used in *Dot Com Disclosures*,[100] their meanings are equivalent. The Decision and Order defines "clearly and prominently" to mean:

(1) In textual communications (*e.g.*, printed publications or words displayed on the screen of a computer), the required disclosures are of a type, size, and location sufficiently noticeable for an ordinary consumer to read and comprehend them, in print that contrasts with the background on which they appear;
(2) In communications disseminated orally or through audible means (*e.g.*, radio or streaming audio), the required disclosures are delivered in a volume and cadence sufficient for an ordinary consumer to hear and comprehend them;
(3) In communications disseminated through video means (*e.g.*, television or streaming video), the required disclosures are in writing in a form consistent with subparagraph (A) of this definition and shall appear on the screen for a duration sufficient for an ordinary consumer to read and comprehend them, and in the same language as the predominant language that is used in the communication;
(4) In communications made through interactive media, such as the Internet, online services, and software, the required disclosures are unavoidable and presented in a form consistent with subparagraph (A) of this definition, in addition to any audio or video presentation of them; and
(5) In all instances, the required disclosures are presented in an understandable language and syntax, and with nothing contrary to, inconsistent with, or in mitigation of the disclosures used in any communication of them.[101]

[98] As noted, Sears did obtain what many would considered affirmative consent from consumers prior to allowing installation of the Tracking Application. However, the FTC disregarded the consent because it was not *informed* consent.

[99] Decision and Order, Sears Holdings Mgmt. Corp., File No. 082 3099 (Fed. Trade Comm'n June 4, 2009), http://www.ftc.gov/os/caselist/0823099/index.shtm.

[100] *Dot Com Disclosures*, *supra* note 35.

[101] Decision and Order, Sears Holdings Mgmt. Corp., File No. 082 3099 (Fed. Trade Comm'n June 4, 2009), http://www.ftc.gov/os/caselist/0823099/index.shtm.

A. Questions Regarding Disclosures

¶45 In light of the very specific requirements for placement of disclosures imposed on Sears, questions are raised as to whether this will become a standard for e-commerce disclosures. This is an important issue for e-commerce because consent and notice are required under so many mechanisms, not only for contract acceptance but also for various forms of permissive marketing and notice procedures. However, although the Decision and Order places very specific requirements on Sears, it does not necessarily indicate that the FTC's position is that no such disclosures could be made in user license agreements or privacy notices. Rather, the FTC has clarified that disclosures made in user license agreements (also referred to as end user license agreements or "EULAs") or privacy notices may not be sufficient to correct a *misleading impression* created elsewhere (for example, in advertising materials). The FTC's statements regarding EULA disclosure to the Direct Marketing Association in response to questions about another case involving the sufficiency of material disclosures is helpful:

> [I]t is important for industry to recognize that a EULA disclosure alone may not be sufficient to correct a misleading impression created elsewhere. *See, e.g.*, FTC, *Dot Com Disclosures* (adequacy of disclosure required to prevent deception is based on the overall net impression) (available at www.ftc.gov/bcp/conline/pubs/buspubs/dotcom/index.html); *cf. FTC v. Cyberspace.com, LLC*, 453 F.3d 1196, 1200 (9th Cir. 2006) (fine print notices are insufficient to undo deceptive net impression); *FTC v. Gill*, 71 F. Supp. 2d 1030, 1046 (C.D. Cal. 1999), *aff'd* 265 F.3d 944, 956 (9th Cir. 2001) (disclaimers and truthful statements that are made outside the context of a deceptive representation do not automatically undo the deception and exonerate deceptive activities). Accordingly, the Commission will analyze EULA-only disclosure on a case-by-case basis, weighing what information is material to consumers and the overall, net impression upon the consumer regarding the transaction.[102]

Therefore, it is possible that the FTC will accept disclosures that are made only in privacy policies or contracts which otherwise meet FTC notice requirements.

¶46 However, the Sears Matter raises the concern that typically it is necessary to make many disclosures, which brings up a question as to how to determine what is most important. Not everything can be disclosed first. This is even more of a concern with mobile devices.

B. Advertising Materials Should Be Reviewed In The Context of Online Contracts and Privacy Policies

¶47 As noted in the Introduction, the Sears Matter is a reminder that advertising materials (and particularly advertising associated with tracking of consumer personal data) should receive legal review to determine whether such materials comply with advertising legal requirements. In addition, the Sears matter signals that advertising

[102] Letter from Donald S. Clark, Sec'y, Fed. Trade Comm'n, to Jerry Cerasale, Senior Vice President, Direct Mktg. Ass'n, (Mar. 7, 2007), *available at* http://www.ftc.gov/os/caselist/0523130/0523130c4186lettercommenterDMA.pdf.

materials should also be reviewed together with the terms of online contracts and privacy policies associated with the advertising campaign. This is to ensure that material disclosures are included clearly and conspicuously in advertising materials so that they do not leave the consumer with a misleading impression of the transaction. The Sears PSULA likely would not have concerned the FTC if the advertising materials presented to the consumer had clearly and prominently disclosed the functions of the Tracking Application early in the process.

V. REQUIREMENTS FOR PRIVACY NOTICES

A. If the "Perfect" Privacy Notice is Written, Will Anyone Read It?

¶48 In 2007, Jon Leibowitz, then Commissioner of the FTC, stated:

> Initially, privacy policies seemed like a good idea. But in practice, they often leave a lot to be desired. In many cases, consumers don't notice, read, or understand the privacy policies. They are often posted inconspicuously via a link at the very bottom of the site's homepage – and filled with fine-print legalese and technotalk. A recent study submitted as a comment for this Town Hall examined privacy policies of Fortune 500 companies and found that they were essentially incomprehensible for the majority of Internet users.[103]

Similarly, the University of California, Berkeley, School of Information recently cited several reasons why privacy policies are ineffective:

> (1) **Privacy policies are too difficult to read . . . .**
> (2) **[P]rivacy policies lead consumers to believe that their privacy is protected. . . . .**
> (3) Even if they could understand them, **the amount of time required to read privacy policies is too great**. A 2008 study estimated that if users actually read privacy policies, it would take approximately 200 hours a year to read the policy for every unique website visited in a year, not to mention updated policies for sites visited on a repeating basis . . . .[104]

However, the problem is larger than simply that notices are too long and complex. Studies show that consumers generally will not read policies and disclosures no matter how short they are. As discussed, the fact is that consumers often do not want to be bothered with reading "pesky legalese."[105] Studies have shown that consumers do not read mortgage documents,[106] disclosures in magazines,[107] video disclosures (supers),[108]

---

[103] Jon Leibowitz, Comm'r, Fed. Trade Comm'n, Remarks at the FTC Town Hall Meeting on "Behavioral Advertising: Tracking, Targeting & Technology" 4 (Nov. 1, 2007), *available at* http://www.ftc.gov/speeches/leibowitz/071031ehavior.pdf.

[104] UNIV. OF CAL. BERKELEY, SCHOOL OF INFORMATION, KNOWPRIVACY 11 (June 1, 2009) (emphasis in original), *available at* http://knowprivacy.org/report/KnowPrivacy_Final_Report.pdf.

[105] i.LAN Sys., Inc. v. NetScout Serv. Level Corp., 183 F. Supp. 2d 328, 329 (D. Mass. 2002).

[106] *See* Pauline M. Ippolito, Acting Dir., Bureau of Econ., Fed. Trade Comm'n, Consumer Research in Policymaking: Applying Recent Findings Regarding Consumer Literacy and Behavior, Remarks at the 2009 ABA Consumer Protection Conference (June 19, 2009) (recording on file with ABA Section of

and privacy policies.[109] Also, according to Michael B. Mazis, marketing claims trump disclosures. If the disclaimer doesn't have as much power as the claim, the claim will totally overwhelm it.[110]

¶49 As reported at a FTC Workshop in January 2007, consumers do not pay attention to disclosures (including online contracts and privacy notices) because they are "click-happy" and believe that nothing can go wrong:

> [M]any online consumers exhibit certain characteristics, including inattention, unwarranted confidence, exuberance, and a desire for immediate gratification, which make them less likely to see and read disclosures. Panelists further explained that, as result of these online characteristics, consumers become "click-happy" and quickly navigate through webpages, without paying much attention because they believe nothing will go wrong and want to complete the transaction as rapidly as possible. As a result, consumers often do not read or understand the terms of the agreements they accept.[111]

Such "click-happiness" has also been confirmed in the context of social networks (and specifically Facebook) by researchers at Carnegie Mellon University.[112] Their recent brief studies indicate that even when Facebook users become aware of privacy risks, they tend to ignore them. Participants in the studies said that they "had nothing to hide" and "they don't really care if other people see their information."[113] The Carnegie Mellon study concluded that it will take an unfortunate incident such as identity theft or stalking to shock Facebook users into being more selective about the information that they make

---

Antitrust Law); *see also* Alan Levy, Senior Scientist, Food & Drug Admin., Consumer Research in Policmaking: Applying Recent Findings Regarding Consumer Literacy and Behavior, Remarks at the 2009 ABA Consumer Protection Conference (June 19, 2009) (recording on file with ABA Section of Antitrust Law). The remarks by Ippolito and Levy are summarized by Rebecca Tushnet on her blog at http://tushnet.blogspot.com/2009/06/aba-consumer-protection-conference.html.

[107] Michael B. Mazis, Consumer Research in Policymaking: Applying Recent Findings Regarding Consumer Literacy and Behavior, Remarks at the 2009 ABA Consumer Protection Conference (June 19, 2009) (recording on file with ABA Section of Antitrust Law). The remarks by Mazis are summarized by Rebecca Tushnet on her blog at http://tushnet.blogspot.com/2009/06/aba-consumer-protection-conference.html.

[108] *Id.*

[109] *See* UNIV. OF CAL. BERKELEY, SCHOOL OF INFORMATION, *supra* note 104.

[110] *See* Mazis, *supra* note 107.

[111] FED. TRADE COMM'N, *supra* note 39, at ii-iii. Moreover, as reported by Hillman & Rachlinski:

> The cognitive factors undermine many of the benefits to consumers of electronic contracting. Indeed, they may explain why the Internet has failed to produce the efficient competition that theorists have anticipated. E-consumers who are satisfied with limited information about businesses have no use for the extra search time that Internet shopping offers. E-consumers also might worry about accumulating too much information, impairing their decisionmaking processes.

Hillman & Rachlinski, *supra* note 23, at 484.

[112] *See generally* Tabreez Govani & Harriet Pashley, Student Awareness of the Privacy Implications When Using Facebook (2005), http://lorrie.cranor.org/courses/fa05/tubzhlp.pdf; Ralph Gross & Alessandro Acquisti, Information Revelation and Privacy in Online Networks (The Facebook Case) (Nov. 7, 2005), http://www.heinz.cmu.edu/~acquisti/papers/privacy-facebook-gross-acquisti.pdf.

[113] Govani & Pashley, *supra* note 112, § 6.

available to other users.[114] Another study conducted on behalf of Canada's Office of the Privacy Commissioner indicates that Facebook users may be aware of privacy risks but provide extensive personal information in order to be popular. Participants reported caring about privacy, but because Facebook is where they experience their social lives, it might be too risky not to participate.[115] What's more, as noted earlier, consumer decisions to ignore disclosures are not limited to the online world. Consumers have long ignored disclosures in the offline world as well. Consumers have signed contracts without reading them for decades.[116] As Arthur Allen Leff wrote in 1970, "[s]ome people would sign a contract even if 'THIS IS A SWINDLE' were embossed across its top in electric pink."[117] Michael Froomkin contends that consumers using the Internet myopically ignore important information in standard terms, particularly terms that relate to privacy issues.[118] Froomkin also acknowledges that it may be more accurate that consumers ignore privacy notices because they do not care about their Internet privacy,[119] a point that has also been expressed by industry leaders such as Microsoft's Bill Gates and Sun Microsystems' Scott McNealy.[120]

¶50 In addition, not every privacy risk can be addressed with a privacy notice. Jonathan Zittrain points out that in addition to privacy risks from government and institutions, there are substantial risks to privacy from third parties, for example, friends tagging unflattering photos on Facebook and unrelated third parties who snap candid

---

[114] *Id.*

[115] *See* News Release, University of Guelph, Popularity Fuels Disclosure on Facebook, Study Finds (Aug. 18, 2009), http://www.uoguelph.ca/news/2009/08/popularity_fuel.html.

[116] *See, e.g.*, Hillman & Rachlinski, *supra* note 23, at 461.

[117] Leff, *supra* note 63, at 157.

[118] A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1501-05 (2000).

[119] *Id.* Froomkin wrote:

> The ultimate effect of consumer privacy myopia depends upon a number of things. First, it depends on the intrusiveness of the profile. If the profile creates a privacy intrusion that is noticeably greater than disclosing an occasional individual fact—that is, if aggregation not only adds value but aggravation—then privacy myopia is indeed a problem. I suspect that this is, in fact, the case and that many people share my intuition. It is considerably more intrusive to find strangers making assumptions about me, be they true or painfully false, than it is to have my name and address residing in a database restricted to the firms from which I buy. On the other hand, if people who object to being profiled are unusual, and aggregation does not cause harm to most people's privacy, the main consequence of privacy myopia is greatly reduced. For some, it is only distributional. Consumers who place a low value on their information privacy - people for whom their average valuation is less than the average valuation of a profiler - would have agreed to sell their privacy even if they were aware of the long-run consequences. The only harm to them is that they have not extracted the highest price possible. But consumers who place a high value on information privacy will be more seriously harmed by their information myopia. Had they been aware of the average value of each datum, they might have preferred not to sell.

Id. at 1503.

[120] *See, e.g.*, Heather Timmons, *Gates Faults U.S. on Data Privacy and Immigration*, N.Y. TIMES, July 24, 2009, *available at* http://www.nytimes.com/2009/07/25/technology/companies/25soft.html (reporting that Mr. Gates was critical of the United States government's unwillingness to adopt a national identity card); Polly Sprenger, *Sun on Privacy: 'Get Over It'*, WIRED, Jan. 26, 1999, http://www.wired.com/politics/law/news/1999/01/17538 (reporting comments by Scott McNearly—head of Sun Microsystems—that consumer privacy issues are a "red herring").

photos and post them online.[121] Such third parties certainly do not provide privacy notices with such postings, unlike government and institutions which usually post some type of notice. Moreover, there are indications that consumers' seeming lack of concern about privacy issues stems more from unawareness rather than from informed unconcern. For example, consider the uproar over privacy issues when Facebook introduced the Beacon advertising program and made other changes in its privacy policies. Beacon allowed companies partnered with Facebook to advertise by posting notices in Facebook users' "news feeds" when the user took an action, such as making a purchase from a third-party website that participated in the Beacon program. When the program originally launched, Facebook users had the right to opt-out, but, in response to consumer complaints, Facebook changed Beacon to an opt-in system, and later retired the system.[122]

¶51 Consumer disregard of privacy risks may be related to consumers' inability to do more to control the uses of their personal information. Daniel Solove states that:

> People often surrender personal data to companies because they perceive that they do not have much choice. They might also do so because they lack knowledge about the potential future uses of the information. Part of the privacy problem in these cases involves people's limited bargaining power respecting privacy and inability to assess the privacy risks.[123]

In fact, a 2009 study conducted by the University of Pennsylvania and University of California at Berkeley shows that about two-thirds of Americans object to online tracking by advertisers, and once they learn the different ways marketers are following their online movements, that number rises to 73%. An additional 7 percent said behavioral advertising was not acceptable when they were tracked on a website, an additional 18 percent said it was not acceptable when they were tracked via other websites, and an additional 20 percent said it was not acceptable when they were tracked offline.[124] Then again, consumers who are concerned about privacy might not object to collection and uses of data about them if they were aware of such collection and uses and had an opportunity to control what is known about them.[125] According to Joseph Turow, lead author of the University of Pennsylvania/University of California study:

---

[121] The Future of the Internet and How to Stop It, Facebook's Privacy Storm, http://futureoftheinternet.org/facebooks-privacy-storm (Feb. 18, 2009). Zittrain optimistically envisions a time when prospective employers (who have also had Facebook pages), and others who have reason to view a person's online history, will view each person's positive history along with the negative. *Id.*

[122] Posting of David Sarno to L.A. Times Technology Blog, *supra* note 92.

[123] DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 73 (2008). On the other hand, maybe the problem is that it is not well articulated. As noted by Solove, "Privacy problems are often not well articulated, and as a result, we frequently lack a compelling account of what is at stake when privacy is threatened and what precisely the law must do to solve these problems." *Id.* at 2.

[124] Joseph Turow et al., Americans Reject Tailored Advertising and Three Activities that Enable It (Sept. 29, 2009), *available a*t http://ssrn.com/abstract=1478214 [hereinafter *University of Pennsylvania/University of California Study*].

[125] At least that was the viewpoint of Louis Brandeis and Samuel D. Warren in their seminal law review article on privacy. *See* Louis Brandeis and Samuel D. Warren, *The Right to Privacy*, 4 HARV. L. REV. 193, 198 (1890) ("The common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others.").

> "I don't think that behavioral targeting is something that we should eliminate, but I do think that we're at a cusp of a new era, and the kinds of information that companies share and have today is nothing like we'll see 10 years from now," Professor Turow said. He said he would like "a regime in which people feel they have control over the data that marketers collect about them. The most important thing is to bring the public into the picture, which is not going on right now."[126]

¶52 Of course, the University of Pennsylvania/University of California study also raises the issue of how many of the participants, newly aware of how they are tracked, will now take steps to protect their privacy. Katherine Strandburg notes that people often disclose personal information frequently despite having indicated a preference for keeping such information private, and this is particularly true in the context of online disclosures.[127] Alessandro Acquisiti and Jens Grossklags have reported that few individuals take affirmative steps to protect their online privacy,[128] and the Carnegie Mellon Facebook study discussed above showed that 84% of participants reported that they are aware that they can change their privacy settings, but less than 48% of the 84% made use of the privacy settings.[129]

¶53 Assuming that privacy notices of some type are necessary, the problem is further complicated because privacy policies are necessarily complex. A certain amount of "fine-print legalese and technotalk" are inherently necessary because the technical issues are usually very complicated and the legal requirements make policies fairly detailed. The FTC has seen firsthand how difficult it is to draft effective form privacy policies through its participation in the ongoing, eight-year interagency notice research project (along with banking regulators and the Securities & Exchange Commission) to draft model privacy forms for use under the Gramm-Leach-Bliley Act.[130] Furthermore, it is

---

[126] *See* Stephanie Clifford, *Two-Thirds of Americans Object to Online Tracking*, N.Y. TIMES, Sept. 29, 2009, *available at* http://www.nytimes.com/2009/09/30/business/media/30adco.html. Interestingly, fewer participants in the University of Pennsylvania/University of California study objected to tracking related to customized discounts and customized news than to tracking in general; 51% of the participant said that customized discounts were acceptable and 58% said that customized news was fine. See *University of Pennsylvania/University of California Study*, *supra* note 124.

[127] Katherine J. Strandburg, *Privacy, Rationality, and Temptation: A Theory of Willpower Norms*, 57 RUTGERS L. REV. 1235, 1264 (2005).

[128] Alessandro Acquisiti & Jens Grossklags, *Privacy Attitudes and Privacy Behavior: Losses, Gains, and Hyperbolic Discounting*, *in* THE ECONOMICS OF INFORMATION SECURITY (J. Camp & R. Lewis eds., Kluwer 2004), *available at* http://www.heinz.cmu.edu/~acquisti/papers/acquisti_grossklags_eis_refs.pdf.

[129] *See* Govani & Pashley, *supra* note 112, § 5.3.

[130] Gramm-Leach-Bliley Financial Act, 15 U.S.C §§ 6801-09 (2006); *see* FTC, Privacy Initiatives, Financial Privacy Rule: Interagency Notice Research Project, http://www.ftc.gov/privacy/privacyinitiatives/financial_rule_inrp.html (last visited July 30, 2009). Joel Winston, the FTC's former Associate Director for the Division of Privacy and Identity Protection questioned the value of disclosures:

> I think there's a serious question here about whether it's simply not feasible for businesses or for consumers to go -- use this sort of notice and choice model. Is it more information than consumers can handle? Is it too difficult for businesses to explain in a way that gives consumers sort of both sides of the equation? Is it too much to expect of consumers?

Joel Winston, former Assoc. Dir., Fed. Trade Comm'n, Div. of Privacy and Identity Protection, Welcome and Introductory Remarks, FTC Town Hall Meeting on "Behavioral Advertising: Tracking,

not just consumers without legal backgrounds who are not reading disclosures, privacy policies, and online contracts; judges and lawyers exhibit this "click-happy" behavior as well.[131]

B. What Makes a Good Privacy Notice?

¶54 Federal agencies, including the FTC, as well as universities,[132] businesses,[133] advertisers, and a policy institute[134] are working towards drafting models of effective disclosures and policies.[135] Over the past few years in particular, the FTC has concluded that privacy policies should be presented (at least initially) in short statements. For example, in its February 2009 report to the U.S. Congress on behavioral advertising,[136] the FTC explained:

> [P]rivacy policies have become long and difficult to understand, and may not be an effective way to communicate information to consumers. Staff therefore encourages companies to design innovative ways – outside of the privacy policy – to provide behavioral advertising disclosures and choice options to consumers.
>
> . . . . [A] disclosure (e.g., "why did I get this ad?") that is located in close proximity to an advertisement and links to the pertinent section of a privacy policy explaining how data is collected for purposes of delivering targeted advertising, could be an effective way to communicate with consumers. Indeed, such a disclosure is likely to be far more effective than a discussion (even a clear one) that is buried within a company's privacy policy. Further . . . some businesses have already begun to experiment with designing other creative and effective disclosure mechanisms. Staff encourages these efforts and notes that they may be most effective if combined with consumer education programs that explain not only what information is collected from consumers and how it is

---

Targeting & Technology" 59 (Nov. 1, 2007), *available at* http://www.ftc.gov/bcp/workshops/ehavioral/71102wor.pdf.

[131] i.LAN Sys., Inc. v. NetScout Serv. Level Corp., 183 F. Supp. 2d 328, 329 (D. Mass. 2002) (district judge's primary account of "pesky legalese").

[132] *See, e.g.*, Press Release, Carnegie Mellon Univ., Carnegie Mellon's Lorrie Cranor Receives NSF Funding for Interdisciplinary Doctoral Program in Privacy and Security (Aug. 24, 2009), *available at* http://www.cit.cmu.edu/media/press/2009/08_24_cranor_nsf_funding.html.

[133] *See, e.g.*, Google, Inc., Choose Your Google Toolbar Configuration, http://toolbar.google.com/prdlg.html (last visited Sept. 3, 2009) (describing the terms of use for Google's "Toolbar" software).

[134] Press Release, Future of Privacy Forum, Future of Privacy Forum Announces Research Initiative To Develop Effective Messages to Communicate with Users about Online Data Use (May 19, 2009), *available at* http://www.futureofprivacy.org/2009/05/19/future-of-privacy-forum-announces-research-initiative-to-develop-effective-messages-to-communicate-with-users-about-online-data-use/.

[135] *See, e.g.*, U.S. Food and Drug Admin., Consumer Research on Food Labels, http://www.fda.gov/Food/ScienceResearch/ResearchAreas/ConsumerResearch/ucm080407.htm (last visited Aug. 4, 2009); Press Release, Fed. Trade Comm'n, FTC Releases Staff Report on Improving Consumer Mortgage Disclosures (June 13, 2007), *available at* http://www.ftc.gov/opa/2007/06/mortgage.shtm; Press Release, Bd. of Governors of the Fed. Reserve Sys. et al., Federal Regulators Seek Public Comment on Model Privacy Notice (Mar. 21, 2007), *available at* http://www.ftc.gov/opa/2007/03/jointrelease.shtm.

[136] *2009 FTC Behavioral Advertising Report*, *supra* note 14.

> used, but also the tradeoffs involved – that is, what consumers obtain in exchange for allowing the collection and use of their personal information.[137]

The FTC seems to have found an effective format for mortgage notices. Disclosure form testing has shown that the prototype mortgage notices, which the FTC prepared as part of an effort to make mortgage notices more understandable for consumers, have been successful.[138] The FTC has suggested a similar format for privacy notices. In addition, Lorrie Cranor and her students at Carnegie Mellon advocate use of a very short notice similar to a nutrition label,[139] so that consumers wanting to know more about the privacy of a particular site can check the label.[140] The Carnegie Mellon and FTC models will likely be successful in providing the necessary information in an easy-to-read format for consumers who are concerned about privacy risks. However, they will not be effective for consumers who remain unconcerned or unaware of those risks.

¶55 Another example of a seemingly effective privacy notice is that accompanying the installation of Google's "Toolbar" software. That privacy notice is introduced with a short notice in red caps: "PLEASE READ THIS CAREFULLY, IT'S NOT THE USUAL YADA YADA."[141]

C. Particular Scrutiny When "Sensitive" Data is Collected and When Collected Data is Shared with Third Parties

¶56 With the exacting requirement for future tracking applications in the Sears Matter and its current dialogue regarding behavioral advertising, the FTC has indicated that online businesses and advertisers must obtain affirmative express consent to (or prohibition against) using sensitive data for tracking purposes. Although there is lack of agreement on the exact definition of "sensitive data," there is consensus within the FTC that such data merits some form of heightened protection.[142] As generally described in the 2009 FTC Behavioral Advertising Report,[143] sensitive data categories include information about children and adolescents, medical information, financial information and account numbers, social security numbers, sexual orientation information,

---

[137] *Id.* at 35-36.

[138] FED. TRADE COMM'N, BUREAU OF ECONOMICS, IMPROVING CONSUMER MORTGAGE DISCLOSURES: AN EMPIRICAL ASSESSMENT OF CURRENT AND PROTOTYPE DISCLOSURE FORMS (2007), *available at* http://www.ftc.gov/os/2007/06/P025505MortgageDisclosureexecutivesummary.pdf. The FTC's report produced four major findings: (1) current mortgage cost disclosures failed to convey key mortgage costs to many consumers; (2) prototype disclosures developed for the study significantly improved consumer recognition of mortgage costs, demonstrating that better disclosures are feasible; (3) both prime and subprime borrowers failed to understand key loan terms, and both groups benefitted from the improved disclosures; and (4) improved disclosures provided the greatest benefit for more complex loans, where both prime and subprime borrowers had the most difficulty understanding loan terms). *Id.* at 5-6.

[139] *See* Larry Dobrow, *Privacy's Nutrition Label*, INSIDE 1TO1: PRIVACY (Int'l Ass'n of Privacy Prof'ls, York, Me.), Aug. 2009, *available at* http://archive.constantcontact.com/fs025/1101351458623/archive/1102647447169.html#LETTER.BLOCK26 (on file with the author).

[140] *See id.*

[141] Google, Inc., Choose Your Google Toolbar Configuration, http://toolbar.google.com/prdlg.html (last visited Sept. 3, 2009) (describing the terms of use for Google's "Toolbar" software).

[142] *2009 FTC Behavioral Advertising Report*, *supra* note 14, at 42.

[143] Described in note 14, *supra*.

government-issued identifiers, and precise geographic location.[144] The report went on to address specifically the collection of sensitive data in the behavioral advertising context:

> [P]re-checked boxes or disclosures that are buried in a privacy policy or a uniform licensing agreement are unlikely to be sufficiently prominent to obtain a consumer's "affirmative express consent." . . . Indeed, this protection is particularly important in the context of online behavioral advertising, where data collection is typically invisible to consumers who may believe that they are searching anonymously for information about medications, diseases, sexual orientation, or other highly sensitive topics.[145]

As next discussed, the dialogue regarding regulation of behavioral advertising has intensified in part due to the behavioral tracking Sears was conducting without adequate disclosures to affected consumers. The FTC's concerns about transparency in the collection and use of consumer information, particularly sensitive information, are very similar for behavioral advertising. In fact, since announcement of its enforcement action against Sears in June 2009, the FTC has also mentioned the Sears Matter in its high-profile discussions of behavioral advertising.[146] The behavioral advertising dialogue is next discussed.

VI. PORTENTS FOR BEHAVIORAL ADVERTISING

> Most of the online world is based on a simple, if unarticulated, agreement: consumers browse Web sites free, and in return, they give up data — like their gender or income level — which the sites use to aim their advertisements.
>
> The new head of the Bureau of Consumer Protection at the Federal Trade Commission, David C. Vladeck, says it is time for that to change. In an interview, Mr. Vladeck outlined plans that could upset the online advertising ecosystem. Privacy policies have become useless, the commission's standards for the cases it reviews are too narrow, and some online tracking is "Orwellian," Mr. Vladeck said.
>
> After eight years of what privacy advocates and the industry saw as a relatively pro-business commission, Mr. Vladeck, has made a splash. In June, the commission settled a case with Sears that was a warning shot to companies that thought their privacy policies protected them. In just over six weeks on the job, he has asked Congress for a bigger budget and for a streamlined way to create regulations. And he said he would hire technologists to help analyze online marketers' tracking. . . .

---

[144] *2009 FTC Behavioral Advertising Report*, *supra* note 14, at 42, 44.

[145] *Id*. at 44.

[146] *See, e.g.*, Editors, An Interview with David Vladeck of the F.T.C., http://mediadecoder.blogs.nytimes.com/2009/08/05/an-interview-with-david-vladeck-of-the-ftc/ (Aug. 5, 2009, 2:24pm EST); Letter from Fed. Trade Comm'n to the Honorable Bobby Rush et al. (June 16, 2009), *available at* http://www.ftc.gov/os/2009/06/P095413onlineadvertising.pdf [hereinafter *Letter to Honorable Bobby Rush*].

> But marketers say such a tactic would be disastrous. "It's impossible to communicate the value proposition to a consumer at the point of an advertisement," said Matt Wise, chief executive of Q Interactive, a Chicago online marketing firm. Mandatory opt-in "would be a tremendous setback in innovation," he said.[147]

¶57 The above report of the *New York Times* interview with the FTC's new head of the Bureau of Consumer Protection illustrates many of the issues running throughout the current dialogue about how behavioral advertising should be regulated. The Sears Matter also provides lessons for online businesses and advertisers that use behavioral advertising methods because it addresses several of the same concerns the FTC has expressed regarding online behavioral advertising (also referred to as "behavioral tracking," "behavioral marketing," and "targeted marketing"). It also suggests the types of acts or practices in the behavioral advertising arena that may prompt the FTC to take enforcement action.

¶58 The FTC defines "online behavioral advertising" to mean "the tracking of a consumer's online activities *over time* – including the searches the consumer has conducted, the web pages visited, and the content viewed – in order to deliver advertising targeted to the individual consumer's interests."[148] Behavioral advertising uses targeting technologies to collect information regarding a user's web-browsing behavior, such as the pages they have visited or the searches they have made, and sometimes with data collected by third parties outside the Internet,[149] to serve ads to consumers.

¶59 In the ongoing behavioral advertising dialogue, the Sears Matter is notable because it is the FTC's first enforcement action for behavioral tracking brought against a prominent "brick and mortar" company with an online presence, and using Internet technologies as part of its advertising campaigns. In contrast, in previous enforcement actions involving behavioral tracking, the companies were fairly typical Internet entrepreneurial endeavors – only a few years old and launched with minimal, if any, legal advice, by a few entrepreneurs using Internet technologies entirely on the Internet. The fact that Sears was fully embracing the behavioral tracking technologies signaled that such uses are now mainstream. Therefore, it intensified the behavioral advertising dialogue and the concern that consumers are not aware of the data which is collected about them as they navigate online.

¶60 Generally, the data which is collected through behavioral advertising is not personally identifiable information in that it does not personally identify particular individuals but rather identifies users through anonymous cookies[150] or other anonymous

---

[147] Clifford, *supra* note 18.

[148] *2009 FTC Behavioral Advertising Report*, *supra* note 14, at 46. This definition refers to "third-party" uses as distinguished from "first party" advertising, where no data is shared with third parties, or contextual advertising, where an ad is based on a single visit to a web page or single search query.

[149] *See* Clifford, *supra* note 18.

[150] A cookie is information about the Web site visit, which the Web browser receives from the Web site, and then stores on the visitor's hard drive. The Web site then "reads" the information each time the user visits the site. This information may include the visitor's Internet service provider, the kind of computer and software used, the Web site linked from, as well as which files were accessed and the amount of time spent on each page. The information is used to track visits to the Web site to learn what visitors like and dislike about the site, and to personalize the site so that options the user selects at the first visit can be used automatically for each successive visit. *See* Gindin, *supra* note 31, at 1170.

tracking technologies. However, in fact, researchers have shown that there is really no such thing as "non-personally identifiable information" because researchers, using surprisingly little additional information, have been successful in identifying individuals in data containing so-called anonymized or non-personally identifiable information.[151] This is significant because most privacy protection laws distinguish between personally identifiable information ("PII") and non-personally identifiable information ("non-PII") with PII receiving substantially greater protection.[152] However, with a few exceptions, such as in 2006, when AOL published the search engine queries of its users (and unintentionally revealed the identity of certain searchers),[153] "re-identifying" anonymized data has so far been primarily the province of resourceful researchers.

¶61 However, with the reports that advertisers are now combining anonymous data with PII (some of it likely based on historical purchases and actions) in order to serve more targeted ads, the issue is no longer purely academic. For example, as reported by the *New York Times*:

> Companies like Acxiom and a competitor, Datran Media, make the connection between online and offline data when a person registers on a Web site or clicks through on an e-mail message from a marketer. . . . Acxiom estimates it has 1,500 pieces of data on every American, based on information from warranty cards, bridal and birth registries, magazine subscriptions, public records and even dog registrations with the American Kennel Club.[154]

The Electronic Frontier Foundation also reported that tracking companies may be identifying specific individuals through social networks:

> When you visit a webpage, there's a good chance that it contains tiny images or invisible JavaScript that exists for the sole purpose of tracking and recording your browsing habits. This sort of tracking is performed by many dozens of different firms. In this post, we're going to look at how this tracking occurs, and how it is being combined with data from accounts on social networking sites to build extensive, identified profiles of your online activity.[155]

The FTC briefly touched on such secondary uses in its 2009 report, *Self-Regulatory Principles for Online Behavioral Advertising* ("*2009 FTC Behavioral Advertising Report*")[156] but declined to provide guidelines since reports of such uses were not yet substantiated.[157]

---

[151] *See, e.g.*, Ohm, *supra* note 31.

[152] In this regard, see the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), which provides substantially greater rights for "individually identifiable health information"—information which identifies an individual (or there is a reasonable basis to believe that the information can be used to identify the individual)—than for information which has been anonymized or de-identified.

[153] See the discussion of Doe 1 v. AOL LLC, 552 F.3d 1077 (9th Cir. 2009), discussed *supra* in text accompanying notes 85-87.

[154] Clifford, *supra* note 18.

[155] Eckersley, *supra* note 19.

[156] *2009 FTC Behavioral Advertising Report*, *supra* note 14, at 44-45.

[157] *Id.*

¶62 Since commercialization of the Internet, commentators have noted the potential for third parties to track users as they navigate the Internet, whether for advertising or other purposes:

> The Internet has the capacity to be the most effective data-collector in existence.. . The information collected from Web site visits reveals much about the user. Even without providing personal information when registering to use a site, a user's interests can be inferred based on Web site or online service use. Accordingly, there is concern that this information will be misused by marketers and others.
>
> . . . .
>
> An Internet user's privacy may be invaded by certain features used by some online services and World Wide Web site operators to maintain and improve their service. Some Web sites collect "cookies." . . . . As such, the information collected does not usually identify a specific individual. However, when combined with on-site registration data, which the Internet user provides when visiting some sites, cookie data may be used to build a profile of the specific Internet user. Many Web sites require on-site registration, including name, address, e-mail address, and sometimes interests, in order to obtain access or certain benefits.[158]

The FTC has long been concerned about online behavioral advertising, and in 1999, the FTC first held a joint workshop with the Department of Commerce on behavioral advertising.[159] There has been increasing concern, particularly in the past few years, in U.S. government agencies and Congress and among consumer groups, that users are being tracked too much online, with information about their Web browsing, shopping habits and overall interests being collected for advertising purposes. Indeed, for years, the FTC has urged companies to self-regulate as an industry practice, and has recently asked companies to redouble their efforts to develop self-regulatory programs, and to ensure that such programs include meaningful enforcement.[160] The FTC issued guidelines and requests for comments regarding behavioral advertising in 2007,[161] and in 2009, the FTC followed with a report regarding the comments received and issued revised guidelines.[162] As part of the *2009 FTC Behavioral Advertising Report*, the FTC articulated four principles regarding requirements for behavioral advertising:

(1) Transparency and Consumer Control
(2) Reasonable Security, and Limited Data Retention, for Consumer Data
(3) Affirmative Express Consent for Material Changes to Existing Privacy Promises

---

[158] *See* Gindin, *supra* note 31, at 1164, 1170.

[159] FTC and Dep't of Commerce, Public Workshop: Online Profiling, Nov. 8, 1999, http://www.ftc.gov/bcp/workshops/profiling/index.shtm.

[160] See *Letter to Honorable Bobby Rush*, *supra* note 146.

[161] See Press Release, Fed. Trade Comm'n, FTC Staff Proposes Online Behavioral Advertising Privacy Principles (Dec. 20, 2007), *available at* http://www.ftc.gov/opa/2007/12/principles.shtm.

[162] *2009 FTC Behavioral Advertising Report*, *supra* note 14.

(4) Affirmative Express Consent to (or Prohibition Against) Using Sensitive Data for Behavioral Advertising[163]

These principles also apply outside the behavioral advertising realm, as seen in other FTC enforcement actions. For example, the Sears Matter, and also the FTC's action against ValueClick in part because of its failure to clearly and conspicuously disclose key terms in an advertising campaign which offered free merchandise in exchange for consumer participation in third party offers, can be seen as enforcement of the transparency principle.[164] The FTC actions against retailer TJX and data brokers Reed Elsevier and Seisint for failing to provide adequate security for consumers' data demonstrate FTC

---

[163] *2009 FTC Behavioral Advertising Report*, *supra* note 14, at 46-47. With regard to transparency and consumer control, the FTC stated:

> Every website where data is collected for behavioral advertising should provide a clear, concise, consumer-friendly, and prominent statement that (1) data about consumers' activities online is being collected at the site for use in providing advertising about products and services tailored to individual consumers' interests, and (2) consumers can choose whether or not to have their information collected for such purpose. The website should also provide consumers with a clear, easy-to-use, and accessible method for exercising this option. ***Where the data collection occurs outside the traditional website context, companies should develop alternative methods of disclosure and consumer choice that meet the standards described above (i.e., clear, prominent, easy-to-use, etc.)***

Id. at 46 (emphasis in original). Regarding security and limited data retention, it said:

> Any company that collects and/or stores consumer data for behavioral advertising should provide reasonable security for that data. Consistent with data security laws and the FTC's data security enforcement actions, such protections should be based on the sensitivity of the data, the nature of a company's business operations, the types of risks a company faces, and the reasonable protections available to a company. ***Companies should also retain data only as long as is necessary to fulfill a legitimate business or law enforcement need.***

Id. at 46-47 (emphasis in original). As for affirmative express consent for material changes to existing privacy policies, it said:

> As the FTC has made clear in its enforcement and outreach efforts, a company must keep any promises that it makes with respect to how it will handle or protect consumer data, even if it decides to change its policies at a later date. Therefore, before a company can use ***previously collected*** data in a manner materially different from promises the company made when it collected the data, it should obtain affirmative express consent from affected consumers. This principle would apply in a corporate merger situation to the extent that the merger creates material changes in the way the companies collect, use, and share data.

Id. at 47 (emphasis in original). Regarding sensitive data, it said:

> Companies should collect sensitive data for behavioral advertising only after they obtain affirmative express consent from the consumer to receive such advertising.

Id.

[164] United State v. ValueClick, Inc., No. 2:08-CV-01711 (C.D. Cal. Mar. 13, 2008), http://www.ftc.gov/os/caselist/0723111/index.shtm. The action included allegations of CAN-SPAM Act violations and of misrepresentations that ValueClick and affiliates secured customers' sensitive financial information.

enforcement of the requirements of Reasonable Security, and Limited Data Retention for Consumer Data.[165] With regard to the principle of Affirmative Express Consent for Material Changes to Existing Privacy Promises, the FTC brought an action against Gateway Learning (known for "Hooked on Phonics") because it rented its customers' personal information to target marketers contrary to explicit promises made in its privacy policy, and because, after collecting consumers' information, Gateway Learning changed its privacy policy to allow it to share the information with third parties without notifying consumers or getting their consent.[166] The FTC's action against Sears for its extensive behavioral tracking without informed affirmative consent is an example of the principle of Affirmative Express Consent to (or Prohibition Against) Using Sensitive Data for Behavioral Advertising.

¶63 In the behavioral advertising dialogue, Representative Rick Boucher of Virginia has announced plans to introduce behavioral advertising legislation in 2009.[167] However, many have urged Congress and the FTC to postpone legislation and to give self-regulation a chance to work. In July 2009, a behavioral advertising consortium (composed of the American Association of Advertising Agencies, Association of National Advertisers, Council of Better Business Bureaus, Direct Marketing Association, and Interactive Advertising Bureau) (the "Behavioral Advertising Consortium") issued *Self-Regulatory Principles for Online Behavioral Advertising*.[168] These reflect the guidelines in the *2009 FTC Behavioral Advertising Report*. With regard to transparency, the Consortium provides a two-tier notice system, with a brief notice calling attention to the fact that they will be tracking, and with a link to a more detailed policy. Moreover, the Consortium will require opt-in consent for collection of financial account numbers, Social Security numbers, and medical and prescription records, and they will not collect "personal information," as defined in the Children's Online Privacy Protection Act ("COPPA"),[169] from children they know are under thirteen or from sites directed to children under thirteen for behavioral advertising. Further, the guidelines also require reasonable security and limited data retention, and affirmative express consent for material changes to existing privacy promises, as also required by the *2009 FTC Behavioral Advertising Report*. As part of the initiative, the Consortium has committed to implement 500 million online advertising impressions to educate consumers regarding online behavioral advertising over an 18 month period.[170]

---

[165] *See* Press Release, Fed. Trade Comm'n, Agency Announces Settlement of Separate Actions Against Retailer TJX, and Data Brokers Reed Elsevier and Seisint for Failing to Provide Adequate Security for Consumers' Data (Mar. 27, 2008), *available at* http://www.ftc.gov/opa/2008/03/datasec.shtm.

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

[167] *See* Rick Boucher, *Behavioral Ads: The Need for Privacy Protection*, THE HILL, Sept. 24, 2009, http://thehill.com/special-reports/technology-september-2009/60253-havioral-ads-the-need-for-privacy-protection.

[168] AM. ASS'N OF ADVER. AGENCIES ET AL., SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING (2009), http://www.iab.net/insights_research/public_policy/behavioral-advertisingprinciples [hereinafter *Behavioral Advertising Consortium Principles*].

[169] 15 U.S.C. §§ 6501-6508 (2006). Under COPPA, the term "personal information" includes individually identifiable information about an individual collected online, including any persistent identifier that is tied to such identifying information. 15 U.S.C. § 6501(8) (2006).

[170] *Behavioral Advertising Consortium Principles*, *supra* note 168, at 12.

¶64 The Consortium's *Self-Regulatory Principles for Online Behavioral Advertising* strikes an appropriate balance *at this time* for behavioral advertising *using non PII*, in the U.S based on the culture of the Internet as it now exists. As noted in the *New York Times* interview with David Vladeck, behavioral advertising is an important component of the online ecosystem. The Internet is supported almost entirely by advertising, with online businesses being able to provide free content in exchange for online advertising.[171] There are also certain advantages to receiving targeted advertisements (especially in contrast to unsolicited email, much of which is clearly untargeted). Congressman Rick Boucher, a major proponent of behavioral advertising legislation, has acknowledged the economic benefits of behavioral advertising and embraces the advantages to receiving targeted advertising:

> I personally appreciate the convenience that arises from ads that are targeted to my specific interests delivered by websites that I frequently visit for online shopping. It is also important to note that online advertising supports much of the commercial content, applications and services that are available to Internet users today without charge, and I have no intention of disrupting this well-established and successful business model.[172]

Furthermore, the FTC has previously recognized that there are tradeoffs. For example, Jon Leibowitz, Chairman of the FTC stated in 2007 that "[b]ehavioral marketing is complicated. In some cases the privacy tradeoff may make sense."[173]

¶65 A potential problem with self regulation is that unless there are formal sanctions available for violations of established guidelines, some companies may be inclined to ignore industry guidelines or to minimize their significance. However, in addition to addressing all of the other principles in the *2009 FTC Behavioral Advertising Report*, the Consortium's Principles also include an Accountability Principle,[174] which calls on the Council of Better Business Bureaus and the Direct Marketing Association (which have

---

[171] *See, e.g.*, HAMILTON CONSULTANTS, ECONOMIC VALUE OF THE ADVERTISING-SUPPORTED INTERNET ECOSYSTEM (2009), http://www.iab.net/insights_research/947883/economicvalue; Grant Gross, *Can Privacy and Consumer Protection Coexist Online?*, PC WORLD, July 24, 2009, http://www.pcworld.com/printable/article/id,169040/printable.html; Mitch Joel, *There's a Price to Pay in Lost Privacy For All That Free Stuff on the Internet*, VANCOUVER SUN, July 30, 2009, *available at* http://www.vancouversun.com/news/There+price+lost+privacy+that+free+stuff+Internet/1844090/story.html.

[172] Boucher, *supra* note 167.

[173] Jon Leibowitz, Comm'r, Fed. Trade Comm'n, Remarks at the FTC Town Hall Meeting on "Behavioral Advertising: Tracking, Targeting & Technology" 6 (Nov. 1, 2007), *available at* http://www.ftc.gov/speeches/leibowitz/071031ehavior.pdf. In full, Liebowitz said:

> So what should the Commission do? Well, sometimes the answer to problems in cyberspace is clear, like in the case of unfair and deceptive nuisance adware. Put the malefactors under order. Disgorge their profits. Pass a law giving the FTC the authority to impose fines. For behavioral marketing, the solution is not so certain. Behavioral marketing is complicated. In some cases the privacy tradeoff may make sense. But one thing is clear: the current "don't ask/don't tell" mentality in online tracking and profiling needs to end.

Id.

[174] *Behavioral Advertising Consortium Principles*, *supra* note 168, at 17-18.

both successfully handled such regulatory programs) to jointly develop a mechanism by which they can police entities engaged in online behavior advertising and help bring entities into compliance.[175] In cases of non-compliance, the FTC and state attorneys general will continue to take action against companies that overstep the boundaries set out in the FTC's Principles.

¶66 On the other hand, it is another matter that businesses are collecting personally identifiable offline data and combining it with data understood to be anonymous in order to serve ads. As noted by the *New York Times* in its report about Acxiom and Datran Media connecting online and offline data:

> [C]onsumer advocates say such unseen tracking is troubling. On the old Internet, nobody knew you were a dog. On the new targeted Internet, they now know what kind of dog you are, your favorite leash color, the last time you had fleas and the date you were neutered. . . .
>
> Datran's cookies include 50 to 100 pieces of information. Both companies say cookie data is anonymous and generalized. Datran and Acxiom then sell advertising on Web sites like NBC.com, Facebook and Yahoo to companies that use their data.[176]

As these practices becomes more prevalent (or more widely publicized), there is likely to be extensive FTC scrutiny of businesses that combine PII offline data with anonymous online data. These practices will intensify the behavioral advertising debate because they use PII along with non-PII in a manner that has previously been based only on non-PII. It will also raise issues that were addressed in the FTC's action against Gateway Learning for making retroactive changes to its privacy policy. There will likely be increased FTC scrutiny of the privacy policies of those businesses which employ the services of companies like Datran Media and Acxiom, to ensure that they have not previously committed to not share personally-identifiable information. Also, the FTC is likely to require that companies obtain consumers' informed express confirmative consent that their personally identifiable information will now be combined with the non-personally identifiable data, and an opportunity to control such uses.

VII. CONCLUSION

¶67 While the Sears Matter provides lessons to businesses, advertisers, and also consumers, it also raises a number of unanswered questions which have been discussed in this Article. Some commentators have argued that the FTC action is unprecedented because it contradicts court decisions and industry practices, and further that the FTC should publish clear rules for how the FTC expects companies to communicate online with their consumers.[177] Although the Sears Matter creates some uncertainty regarding exactly what will constitute effective online communication, the FTC has provided clear

---

[175] *Id.* at 41.

[176] Clifford, *supra* note 18.

[177] *See, e.g.*, Alan Charles Raul et al., *End of the Notice Paradigm?: FTC's Proposed* Sears *Settlement Casts Doubt On the Sufficiency of Disclosures in Privacy Policies and User Agreements*, E-COMMERCE LAW DAILY, July 7, 2009, *available at* http://www.ftc.gov/os/comments/searsholdings/542583-00006.html.

rules for disclosures, for example, in *Dot Com Disclosures* in 2000. Additional questions will be answered as the FTC provides more guidance, or brings more enforcement actions against companies that overstep the boundaries. Although there are gray areas regarding which disclosures are material and which should be displayed first in notices, the FTC has been very clear regarding its major principles for actions that involve privacy issues.

¶68 The Sears Matter has been a watershed moment in the behavioral advertising dialogue. As noted, while previously the companies involved in FTC enforcement actions for overstepping the behavioral tracking boundaries were new initiatives launched by Internet entrepreneurs which seemed to be deviations from more standard Internet practices, the employment of similar technologies by a prominent and long-established "brick and mortar" retailer signaled that behavioral targeting has gone mainstream. This has further intensified the FTC's concerns about behavioral advertising.

¶69 Behavioral advertising is beneficial in several ways, primarily because it largely funds the Internet and allows online companies to offer consumers access to substantial resources at little or no expense.[178] It also is beneficial because the advertising that is delivered to consumers is more likely to be of interest to them.[179] At the same time, behavioral advertising raises significant concerns because of the capacity of online technologies to collect and use consumers' personal information without their knowledge. Recent incidents such as the posting of family photos and details on Facebook by the wife of the head of the U.K.'s MI-6,[180] and Facebook users' uproar when Facebook changed privacy settings indicate that consumers' seeming unconcern about privacy is more likely due to lack of awareness. The FTC is correct to emphasize the importance of ensuring that consumers are educated about the behavioral tracking that is taking place.

¶70 Meanwhile, there has been persistent talk of federal legislation, and Representative Rick Boucher has outlined his plans to introduce legislation in 2009. However, legislation would be premature at this time. First, it is not clear what type of legislation is appropriate to regulate behavioral advertising. For example, although some privacy advocates have suggested requiring opt-in consent from consumers prior to sharing of non-PII by third parties, this would not be advantageous. Particularly in light of the studies showing that consumers rarely pay attention to notices no matter how short they are, it seems likely that consumers who are asked to consent to tracking will continue to blindly click "I agree" without understanding the consequences. Moreover, an opt-in system would likely interfere with the online ecosystem of which behavioral advertising is a part, and potentially result in the loss of free online resources because they are funded largely by advertising. Also, the FTC did not present its final principles for behavioral advertising until February 2009. The Behavioral Advertising Consortium

---

[178] *See, e.g.*, HAMILTON CONSULTANTS, *supra* note 171.

[179] *See generally* Eric Goldman, *A Coasean Analysis Of Marketing*, 2006 WISC. L. REV. 1151, 1221 (2006) (arguing that consumers need marketing and do not always recognize its benefits); *see also* Jules Polonetsky, *Behavioral Advertisers Need to Change Their Behavior*, ROLL CALL, June 22, 2009, http://www.rollcall.com/news/36108-1.html (encouraging CEOs to fully use personal data to make their customers' online experiences more useful, but at the same time urging CEOs not to use sensitive data, to erase long-term data that could be lost or misused, and to consider how to best provide customers with real transparency and control).

[180] Associated Press, *The U.K. Spy Chief Who Loved Facebook: Holiday Snapshots, Family Details about Head of Britain's MI6 Intel Agency Removed from Web Site*, CBS NEWS, July 5, 2009, http://www.cbsnews.com/stories/2009/07/05/tech/main5135008.shtml.

responded in July 2009 by adopting self-regulatory principles that were substantially similar. The Consortium's principles include an enforcement mechanism to be developed jointly by the Council of Better Business Bureaus and Direct Marketing Association through which they can police entities engaged in online behavioral advertising and help bring entities into compliance. Since both entities have successfully handled regulatory programs before, these principles should be given some time to work.

¶71 The first goal of the FTC's behavioral advertising initiative is to ensure transparency and consumer control, so that consumers are aware behavioral advertising is taking place in order to make choices about uses of their personal data. For example, an educated and interested consumer may opt out of certain uses, or not use particular resources for which behavioral advertising may be necessary for economic reasons. Consumer education is a major component of this goal. In light of this goal, the Behavioral Advertising Consortium is uniquely positioned to inform consumers about behavioral advertising. The Consortium includes the same companies that have been the innovators of the Internet and digital technologies, and that are expert at reaching consumers. In addition, a Washington think tank, Future of Privacy Forum, which is supported by some of these innovators, has already embarked on such an initiative with the assistance of the large advertiser, WPP Group, to develop privacy notices that consumers will read. As discussed, previous notices guided by federal regulation have not captured consumers' attention. However, the members of the Behavioral Advertising Consortium (and other advertisers like them) possess the means and the motivation to really reach consumers[181] and ensure that they understand that they are being tracked (along with the reasons why). While some would argue that consumer education is contrary to the interests of the Consortium in that consumers that have more knowledge of tracking might try to avoid behavioral advertising-supported websites, these companies are also the group with the most to lose if behavioral tracking becomes heavily regulated and therefore should have some motivation to ensure that consumers more completely understand behavioral tracking and the privacy risks involved. As part of its initiative, the Behavioral Advertising Consortium has committed 500,000,000 online advertising impressions to educate consumers regarding online behavioral advertising over an eighteen month period.

¶72 These advertisers should be given the opportunity to make a difference in educating consumers, along with ensuring that they comply with all of their other behavioral advertising principles. If successful, this may not eliminate concerns about behavioral advertising altogether but should accomplish the FTC's current goals. In the meantime, the FTC, individual companies, think tanks like the Future of Privacy Forum, and universities like Carnegie Mellon will continue their efforts to educate consumers. Furthermore, the FTC will continue to bring enforcement action against those companies which overstep the behavioral advertising boundaries, and will undoubtedly provide additional further guidance regarding acceptable notice procedures.

---

[181] *See, e.g.*, U.S. Patent Application No. 20090265214 (filed Oct. 22, 2009) (Apple Inc.'s patent application for an "Advertisement in Operating System" that disables one or more functions of a computer device while serving an audible or visual advertisement to the user, and that enables those functions only after the user demonstrates that he has paid attention to the advertisement—thereby forcing users' devices to pay attention to advertisements); *see also* Randall Stross, *Apple Wouldn't Risk Its Cool Over a Gimmick, Would It?*, N.Y. TIMES, Nov. 14, 2009, at BU4, *available at* http://www.nytimes.com/2009/11/15/business/15digi.html.