THE DEATH OF THE PRIVACY POLICY?: EFFECTIVE PRIVACY DISCLOSURES AFTER *IN RE SEARS*

Yan Fang

Imagine that you are an executive at Sears Holdings Corporation (Sears), one of the nation's largest retailers.[1] You want to launch a website that allows customers to leave feedback on products and allows you to track their online and offline activities. Legally speaking, what information must you provide to those customers? How explicit must your disclosures be? Is a privacy policy enough or would you have to include other notification measures as well?

When Sears launched its online "My SHC Community" (Community) site in April 2007,[2] the company intended the Community to be an interactive website through which Sears could send participants product information and marketing surveys as well as collect consumer data and usage information through a tracking application.[3] The Privacy Statement and User License Agreement (PSULA) accompanying the Community site stated explicitly that the tracking software would collect information from participants' secure transactions, including personal financial and health data.[4] Sears also paid ten dollars to participants who retained the tracking application for at least thirty days.[5]

In June 2009, the Federal Trade Commission (FTC or Commission) indicated that Sears's privacy disclosure was not enough. Observing that the application collected consumers' information from online banking statements, video rental transactions, library borrowing histories, and online

1. Sears Holdings Corporation, http://www.searsholdings.com/ (last visited Mar. 22, 2010).

2. *In re* Sears Holdings Mgmt. Corp., Docket No. C-4264 (issued Aug. 31, 2009) (complaint), *available at* http://www.ftc.gov/os/caselist/0823099/090604searscmpt.pdf.

3. *In re* Sears Holdings Mgmt. Corp., Docket No. C-4264 (issued Aug. 31, 2009) (exhibits B and C), *available at* http://www.ftc.gov/os/caselist/0823099/090604 searscomplaintaf.pdf.

4. *In re* Sears Holdings Mgmt. Corp., Docket No. C-4264 (issued Aug. 31, 2009) (exhibit E), *available at* http://www.ftc.gov/os/caselist/0823099/090604sears complaintaf.pdf.

5. Exhibit B, *supra* note 3.

drug prescription records,[6] the Commission charged that Sears's characterization of the scope of tracking as "online browsing" was deceptive and in violation of the Federal Trade Commission Act,[7] suggesting that a privacy policy that explicitly states a company's information collection practices may no longer be adequate to comply with FTC privacy disclosure standards. Sears agreed that month to settle with the Commission over charges that it inadequately disclosed the extent to which its software tracked consumers' personal information.[8]

Both the Commission's allegations and Sears's agreement to settle surprised attorneys.[9] According to one lawyer, Sears's conduct was not "egregious" in light of the company's disclosures in the PSULA: "One imagines that the reasonable expectations of consumers who chose to be paid to have their online activities tracked is that they would have their online activities tracked."[10] That commentator took particular issue with the Commission's analysis of Sears's actions as "deceptive," arguing that previous FTC orders finding deception involved express misrepresentations in companies' privacy policies about information collection practices.[11]

This Note argues that the Commission's finding of Sears's practices as "deceptive" comports with the agency's three-part framework for analyzing

6. *In re* Sears Holdings Mgmt. Corp., Docket No. C-4264 (released June 4, 2009) (draft complaint), *available at* http://www.ftc.gov/os/caselist/0823099/090604 searscomplaint.pdf. When Sears settled by accepting the terms of a consent agreement, the FTC had only provided the company with a draft complaint. In the FTC administrative action and settlement process, a complaint is not issued formally until after a period of public comment and subsequent approval by the FTC Commissioners. *See infra* Section I.A explaining the draft complaint process.

7. Complaint, *supra* note 2.

8. Press Release, Fed. Trade Comm'n, Sears Settles FTC Charges Regarding Tracking Software (June 6, 2009), http://www.ftc.gov/opa/2009/06/sears.shtm.

9. *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*, 8 PRIVACY & SECURITY L. REP. (BNA) No. 1070, at 2 (July 20, 2009); *see also* Susan E. Gindin, *Nobody Reads Your Privacy Policy or Online Contract? Lessons Learned and Questions Raised by the FTC's Action Against Sears*, 8 NW. J. TECH. & INTELL. PROP. 1, 2–3 (2009) (noting that the Sears action may be considered "alarming" in light of precedents upholding online contracts); Amy E. Bivins and Barbara Yuill, *Attorneys, FTC Discuss Proposed Settlement Involving Tracking of Online Activity*, 8 PRIVACY & SECURITY L. REP. (BNA) No. 869, at 1–2 (June 15, 2009) (comparing private firm attorney Alan Raul's reaction that the Sears settlement could have far-reaching implications and FTC attorney Rick Quaresima's view that the case did not move the FTC's enforcement standard); Howie Perlman, *Sears Settles FTC Claims of Consumer Data Collection Without Proper Disclosure*, 8 PRIVACY & SECURITY L. REP. (BNA) No. 824, at 1 (June 8, 2009) (noting that the FTC may be signaling the inadequacy of material privacy disclosures made in a privacy policy or end user license agreement alone).

10. Raul, *supra* note 9, at 2.

11. *Id.* at 10.

deception under 15 U.S.C. § 45, more commonly known as Section 5 of the Federal Trade Commission Act. Given the extensive scope and sensitive nature of the information that Sears tracked, this Note agrees with the Commission that Sears's initial use of the broad term "online browsing" to describe its tracking practices, even if later supplemented by a complete disclosure in the PSULA, was deceptive. This Note concludes, however, that Commission's finding does not signal the end of privacy policies. Instead, the decision signals that a privacy policy alone may no longer be sufficient for disclosing material information about a company's data-tracking practices.

This Note also recommends five measures for effective privacy disclosures after *In re Sears*. In particular, it explains how the FTC's order gives additional guidance for compliance with the privacy disclosure principles issued by the FTC in its February 2009 staff report, SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING.[12] Behavioral advertising is the practice of tracking an individual's online activities in order to deliver advertising tailored to that person's interests.[13] Although Sears was not tracking information specifically to deliver targeted ads, the company's use of a privacy statement and user license is a common practice among companies engaged in behavioral advertising. As such, identifying what the Commission found deceptive about Sears's practices offers additional guidance on how companies may comply with the FTC's principles for behavioral advertising.

Part I of this Note discusses the FTC's enforcement authority to take action against privacy violations and explains the three-part inquiry that the agency applies to determine whether a business practice is deceptive. Part II discusses the Commission's complaint and order in the *Sears* matter. Part III explains why Sears's conduct is appropriately analyzed as a deceptive practice. Part IV recommends privacy disclosure measures that companies can adopt to avoid engaging in deceptive information-tracking practices.

I. THE FEDERAL TRADE COMMISSION AND PRIVACY

The FTC was created in 1914 through the passage of the Federal Trade Commission Act (FTCA).[14] Its mission is to promote competition among

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

13. *Id.* at 2.

14. Federal Trade Commission Act, 15 U.S.C. §§ 41–58 (2006); FED. TRADE COMM'N, A GUIDE TO THE FEDERAL TRADE COMMISSION (Mar. 2004), http://www.ftc.gov/bcp/edu/pubs/consumer/general/gen03.shtm.

businesses and to protect consumers from unfair and deceptive trade practices.[15] Although the FTC initially had authority only to restrict "unfair methods of competition in or affecting commerce" between businesses,[16] the Wheeler-Lea Amendment in 1938 broadened the agency's authority to protect consumers under Section 5 of the FTCA.[17] This amendment gave the FTC general authority to police "unfair or deceptive acts or practices."[18] Under this broad power, the agency currently investigates and seeks sanctions for privacy violations,[19] including monetary equitable relief as well as preliminary and permanent injunctions.[20]

The FTC is headed by five Commissioners who are nominated by the President and confirmed by the Senate.[21] The Commissioners vote to accept, reject, or concur in enforcement actions brought by the agency's bureaus; they also vote on reports issued by the FTC staff.[22] Today, the agency serves its consumer protection mission through the Bureau of Consumer Protection (BCP), which enforces consumer protection laws enacted by Congress and trade regulation rules issued by the Commission.[23] The BCP primarily investigates business practices, undertakes administrative and judicial actions, engages in rulemaking proceedings, and promotes consumer and business education.[24] The BCP's Division of Privacy and Identity Protection enforces privacy violations by investigating and bringing actions against businesses,

15. FTC, A GUIDE TO THE FTC, *supra* note 14.

16. *Id.*

17. 15 U.S.C. § 45(a)(1) (2006) (prohibiting "[u]nfair methods of competition in or affecting commerce" and "unfair or deceptive acts or practices in or affecting commerce").

18. *Id.* § 45(a)(1).

19. The FTC also has privacy enforcement authority under the Children's Online Privacy Protection Act, the Gramm-Leach-Bliley Act, the Telemarketing and Consumer Fraud Abuse and Prevention Act, and the Fair Credit Reporting Act. In addition, the agency enforces specific consumer protection statutes such as the Telemarketing Sales Rule, the Pay-Per-Call Rule, the Truth-in-Lending Act, the Cigarette Labeling Act, and the Do-Not-Call Implementation Act. For a list of statutes related to the FTC's consumer protection mission, *see* Fed. Trade Comm'n, Legal Resources - Statutes Relating to Consumer Protection Mission, http://www.ftc.gov/ogc/stat3.shtm (last visited Mar. 22, 2010).

20. FED. TRADE COMM'N, A BRIEF OVERVIEW OF THE FEDERAL TRADE COMMISSION'S INVESTIGATIVE AND LAW ENFORCEMENT AUTHORITY, § II(A)2 (July 2008), http://www.ftc.gov/ogc/brfovrvw.shtm.

21. FTC, A GUIDE TO THE FTC, *supra* note 14.

22. The FTC's bureaus include the Bureau of Consumer Protection, the Bureau of Competition, and the Bureau of Economics. FTC, A GUIDE TO THE FTC, *supra* note 14.

23. *Id.*

24. FTC, A BRIEF OVERVIEW, *supra* note 20, § II(A).

organizations, or individuals that use deceptive or unfair practices to collect, use, share, or secure consumers' personal data.[25]

Sections I.A and I.B below describe how the FTC brings enforcement actions and how the agency distinguishes unfair practices from deceptive ones. Section I.C then highlights cases in which deceptive analysis has been applied. Lastly, Section I.D discusses an FTC report that provides additional guidance on how and when an information collection practice is deceptive.

A. HOW THE FTC BRINGS AN ACTION

The FTC may initiate a consumer protection investigation independently or in response to consumer complaints, Congressional inquiries, or other impetuses, such as an article on a consumer subject.[26] Following an investigation, the FTC may initiate an enforcement action through either an administrative or a judicial process.[27] In the administrative enforcement process, one of the agency's Bureaus drafts a complaint stating its charges, which it presents to the respondent company and to the FTC Commissioners.[28]

If the company disputes the charges, the Commission may officially issue an administrative complaint.[29] If the company settles, it signs a consent agreement in which it accepts the terms of a consent order resolving allegations in the draft complaint.[30] In agreeing to the consent order, the

25. Fed. Trade Comm'n, Bureau of Consumer Prot., Div. of Privacy and Identity Protection, http://www.ftc.gov/bcp/bcppip.shtm (last visited Mar. 22, 2010); *see also* Fed. Trade Comm'n, Privacy Initiatives, Enforcing Privacy Promises: Section 5 of the FTCA, http://www.ftc.gov/privacy/privacyinitiatives/promises.html (last visited Mar. 22, 2010) [hereinafter FTC, Privacy Initiatives].

26. FTC, A GUIDE TO THE FTC, *supra* note 14. FTC investigations generally are not publicly disclosed in order to protect the investigations and the companies under investigation. FTC, A BRIEF OVERVIEW, *supra* note 20, § I(A).

27. 15 U.S.C. § 45(b) (2006).

28. FTC, A BRIEF OVERVIEW, *supra* note 20, § II(A)1.

29. *Id.*, § II(A)1. The Commission initiates an administrative or judicial action if it has "reason to believe" that the law has been or is being violated. 15 U.S.C. § 45(b); 15 U.S.C. § 53(b). The FTC's administrative complaint initiates a formal proceeding that is like a federal court trial but before an administrative law judge. Initial decisions by an administrative law judge may be appealed to the full Commission. Final decisions issued by the Commission may be appealed to the U.S. Court of Appeals and to the U.S. Supreme Court. FTC, A BRIEF OVERVIEW, *supra* note 20, § II(A)1(a).

30. *Id.*, § II(A)1; *see also In re* Sears Holdings Mgmt. Corp., Docket No. C-4264 (released June 4, 2009) (agreement containing consent order), *available at* http://www.ftc.gov/os/caselist/0823099/090604searsagreement.pdf [hereinafter Consent Agreement] (explaining the consent agreement process).

company does not admit to any violations of the law;[31] it does, however, waive the right to judicial review.[32] The consent agreement and draft complaint are then placed on public record for thirty days for public comment.[33] After considering the comments received during the comment period, if a majority of the Commissioners approves the consent agreement, the Commission officially issues the complaint as well as a final order resolving the allegations in the issued complaint.[34] The Commission has resolved the majority of its privacy actions through this administrative complaint and consent agreement process.[35]

Alternatively, the FTC may pursue a judicial action by filing a complaint in federal district court, which allows the agency to simultaneously seek injunctive relief as well as monetary equitable relief. [36] In addition, a court's order becomes effective immediately, whereas the Commission's administrative order does not take effect until sixty days after service.[37] Generally, the FTC favors administrative action in cases involving novel legal issues or fact patterns; this gives the Commission the first opportunity to make factual findings and articulate the relevant legal standards.[38] If a court later reviews the administrative decision, the court must give substantial deference to the Commission's factual findings and interpretations of the FTCA.[39]

B. UNFAIR VS. DECEPTIVE ANALYSIS

Under the FTCA, the FTC has general authority to police "unfair or deceptive acts or practices."[40] A practice may violate the FTCA if it is either unfair, deceptive, or both.[41] An act or practice is unfair if (1) it causes or is likely to cause substantial injury to consumers (2) that is not outweighed by countervailing benefits to consumers or to competition and (3) that cannot

31. FTC, A BRIEF OVERVIEW, *supra* note 20, § II(A)1(a); *see also* Consent Agreement, *supra* note 30.

32. FTC, A BRIEF OVERVIEW, *supra* note 20, § II(A)1(a).

33. 15 U.S.C. § 45(b) (2006); FTC, A BRIEF OVERVIEW, *supra* note 20, § II(A)1(a).

34. FTC, A BRIEF OVERVIEW, *supra* note 20, § II(A)1(a).

35. Marcia Hofmann, *Federal Trade Commission Enforcement of Privacy*, *in* PROSKAUER ON PRIVACY: A GUIDE TO PRIVACY AND DATA SECURITY LAW IN THE INFORMATION AGE 4–14 (2006).

36. 15 U.S.C. § 53(b); FTC, A BRIEF OVERVIEW, *supra* note 20, § II(A)2. Through the administrative process, the FTC may only obtain injunctive relief. *Id.*, § II(A)2.

37. 15 U.S.C. § 45(b); FTC, A BRIEF OVERVIEW, *supra* note 20, § II(A)2.

38. FTC, A BRIEF OVERVIEW, *supra* note 20, § II(A)2.

39. *Id.*

40. 15 U.S.C. § 45(a)(1).

41. *See id.*

be reasonably avoided by consumers.[42] The first factor—the extent of consumer injury—is most important in unfairness analysis.[43] Although monetary harm and unnecessary health or safety risk typically satisfy the substantial injury factor,[44] a small degree of harm to a large number of consumers may also suffice.[45]

In contrast, an act or practice is deceptive if it involves (1) a representation, omission, or practice that misleads or is likely to mislead (2) a consumer acting reasonably under the circumstances and (3) the representation, omission, or practice is material.[46] Here, the FTC evaluates the entire transaction or course of dealing; this means that if the initial contact between a seller and a buyer is deceptive and creates a misleading impression, that entire transaction is deceptive even if the truth is subsequently disclosed to the consumer.[47]

C. DECEPTIVE ANALYSIS IN DEPTH

Since 2000, the FTC has brought more than thirty privacy actions against various companies,[48] most of which it has settled through the administrative complaint and settlement process.[49] Substantively, the FTC has sought to enforce companies' promises about how they would collect, store, use, or secure consumers' personal information. Sections I.C.1 and I.C.2 below describe the Commission's deception analysis and discuss how that analysis has been applied in online privacy cases.

---

42. *Id.* § 45(n).

43. Letter from Fed. Trade Comm'n to Hon. Wendell H. Ford, Chairman, and Hon. John C. Danforth, Ranking Minority Member, S. Comm. on Commerce, Science, and Transp., Consumer Subcomm., FTC Policy Statement on Unfairness (Dec. 17, 1980), *available at* http://www.ftc.gov/bcp/policystmt/ad-unfair.htm [hereinafter FTC, Unfairness Policy].

44. *Id.*

45. J. Howard Beales III, Former Dir., Bureau of Consumer Prot., Fed. Trade Comm'n, Speech at the Marketing and Public Policy Conference: The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection (May 30, 2003), *available at* http://www.ftc.gov/speeches/beales/unfair0603.htm.

46. Letter from Fed. Trade Comm'n to Hon. John D. Dingell, Chairman, H. Comm. on Energy and Commerce, FTC Policy Statement on Deception, § V (Oct. 14, 1983), *available at* http://www.ftc.gov/bcp/policystmt/ad-decept.htm [hereinafter FTC, Deception Policy].

47. *Id.*, § III.

48. The majority of these cases are listed at Fed. Trade Comm'n, Privacy Initiatives, Enforcement Cases, http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html (last visited Mar. 22, 2010).

49. *See* Hofmann, *supra* note 35, at 14.

1. The FTC Policy Statement on Deception

In 1983, the FTC issued a Policy Statement on Deception (Deception Policy) in response to a Congressional request for clarification on what constitutes a deceptive act or practice under Section 5 of the FTCA.[50] The Policy laid out a three-factor inquiry that the Commission continues to use in determining whether a practice is deceptive. This inquiry asks (1) whether the act or practice involves a representation, omission, or practice that misleads or is likely to mislead; (2) whether the consumer acted reasonably under the circumstances; and (3) whether the representation, omission, or practice was material to the consumer's conduct or decision with respect to the product or services.[51]

Under this inquiry, the Commission first considers whether the act or practice "misleads" or is "likely to mislead" rather than whether it causes actual deception.[52] For a written representation, for example, the Commission determines its likelihood to mislead by comparing phrases in the document, the nature of the claim, and the nature of the transactions.[53] For omissions, the Commission may either presume that reasonable consumers are likely to be misled or require evidence establishing that likelihood.[54]

Next, the Commission assesses whether the consumer's interpretation or reaction is reasonable by considering the practice from the perspective of a reasonable consumer.[55] This inquiry is fact-specific and presumes that a consumer's interpretation of an act or omission is reasonable if that interpretation is intended by the seller.[56] If the seller's representation conveys multiple meanings to a reasonable consumer, and at least one meaning is false, the act or omission is deemed deceptive.[57] If the practice targets a particular group of consumers, such as children or the elderly, the FTC also considers the practice from the perspective of an ordinary, reasonable member of that group.[58] When assessing this second factor, the Commission has emphasized that "written disclosures or fine print may be insufficient to

50. 15 U.S.C. § 45 (2006). The FTC also issued a Policy Statement on Unfairness in 1980 in response to Congressional request for the Commission's views on unfairness under Section 5. *See* FTC, Unfairness Policy, *supra* note 43.

51. FTC, Deception Policy, *supra* note 46, § V.

52. *Id.*, § II.

53. *Id.*

54. *Id.*

55. *Id.*, § III.

56. *Id.*

57. *Id.*

58. *Id.*

correct a misleading representation."[59] Thus, "when the first contact between a seller and a buyer occurs through a deceptive practice, the law may be violated even if the truth is subsequently made known to the purchaser."[60]

Third, the Commission determines whether the deception is material. A "material" misrepresentation or omission is one that is "likely to affect a consumer's choice of or conduct regarding a product."[61] It is information that is "important" to consumers, and if inaccurate or omitted, would likely cause injury to consumers.[62] The Commission considers certain categories of information presumptively material, including express and implied claims.[63] The Commission is also likely to infer materiality when the seller's claims involve health, safety, or other main characteristics of a product or service, such as price, purpose, efficacy, or durability.[64]

2. Deception Cases

As companies have established online presences, the FTC has used its three-part deception analysis to determine whether a company's privacy practices have been deceptive.[65] Although the FTC often finds companies' practices to be "unfair or deceptive" without indicating whether the practice was specifically deceptive or unfair,[66] findings of deception often involve companies' per se violations of their own privacy policies. As such, FTC complaints generally discuss whether a practice is false, misleading, or likely to mislead (first factor), but tend to presume consumer reasonableness (second factor) and materiality (third factor).

In *Federal Trade Commission v. Toysmart.com, LLC*, for example, the FTC charged that an online toy seller violated Section 5 of the FTCA when it offered to sell customers' personal information in contradiction to its original policy stating that such information would "never" be shared with a third

59. *Id.*
60. *Id.*
61. *Id.*, § IV.
62. *Id.*
63. *Id.*
64. *Id.*
65. *See generally* Hofmann, *supra* note 35, at 17–30.
66. In the following cases, the FTC alleged that the company's failure to implement reasonable and appropriate security measures to protect sensitive consumer information violated the company's online privacy policies and "constituted unfair or deceptive acts or practices." *In re* Petco Animal Supplies, Inc., 139 F.T.C. 102 (2005); *In re* MTS, Inc., 137 F.T.C. 444 (2004); *In re* Guess?, Inc., 136 F.T.C. 507 (2003); *In re* Microsoft Corp., 134 F.T.C. 709 (2002); *In re* Eli Lilly & Co., 133 F.T.C. 20 (2002); *see also In re* Liberty Fin. Co. Inc., 128 F.T.C. 240 (1999) (alleging that an investor website's failure to maintain consumer survey responses anonymous despite initial survey description that responses would be anonymous was unfair or deceptive under Section 5).

party.[67] In its course of business, Toysmart collected personal information from customers, such as names, addresses, billing information, shopping preferences, and family profiles.[68] When the company ran into financial difficulty and initiated bankruptcy proceedings, however, it offered to sell its customer lists.[69] Although the Commission did not explicitly analyze Toysmart's actions under each deception factor, it alleged that Toysmart misrepresented its actions, which addresses the first factor requiring that practices be misleading or be likely to mislead. For the second factor, the Commission likely presumed that a reasonable consumer would not expect Toysmart to sell his or her information. Here, the Commission presumes that a consumer's interpretation of an act or omission is reasonable if the seller intended that interpretation.[70] Since Toysmart expressly stated that it would never share customers' information with third parties, the company likely intended for customers to believe that it would never share this information. For the third factor, the Commission likely presumed that Toysmart's claims were material because the company made express claims about never selling consumer information.[71]

In the matter of *Gateway Learning Corp.*, the Commission similarly found Gateway's failure to notify consumers of changes to the company's privacy policy to be deceptive.[72] Beginning in 2000, Gateway marketed its Hooked on Phonics products under a privacy policy that promised not to sell, rent, or loan consumers' personal identification information to third parties without express consumer consent.[73] The policy also provided that if any changes were made to the policy, Gateway would notify customers and allow them to opt out of the new practices.[74] In 2003, however, Gateway began to rent consumers' information to marketers without their consent.[75] A few months later, Gateway revised its online privacy policy to state that it would provide consumers' personal information to third parties "from time to time."[76]

67. Trial Order, FTC v. Toysmart.com, LLC, No. 00-11341-RGS (D. Mass. July 21, 2000), *available at* http://www.ftc.gov/os/2000/07/toysmartconsent.htm.

68. First Amended Complaint, FTC v. Toysmart.com, LLC, No. 00-11341-RGS (D. Mass. July 21, 2000), *available at* http://www.ftc.gov/os/2000/07/toysmartcomplaint.htm.

69. *Id.*

70. *See supra* note 56 and accompanying text; FTC, Deception Policy, § III.

71. The Commission presumes that a company's express and implied claims are material. *See supra* note 63 and accompanying text.

72. Decision and Order, *In re* Gateway Learning Corp., 138 F.T.C. 443 (Sept. 10, 2004) (No. C-4120).

73. *Id.* at 444.

74. *Id.* at 445.

75. *Id.* at 446.

76. *Id.*

Gateway did not, however, notify consumers of the change or give them the option to opt out, as was promised in the initial policy.[77]

The Commission charged that Gateway's failure to notify consumers of changes to its privacy policy was deceptive,[78] emphasizing that Gateway made "false or misleading" representations (first factor). Although the Commission did not specifically address its analysis under the other factors, it likely presumed that a reasonable consumer would not expect Gateway to change its policy without notification because Gateway expressly stated that it would notify consumers of changes to its privacy policy (second factor). The Commission likely also presumed that the claim was material because the claim was express (third factor).[79]

The FTC has also found omissions to be deceptive in adware cases.[80] In the matters of *Zango, Inc.* and *DirectRevenue LLC*, online companies offered consumers free content and software, such as screensavers, peer-to-peer file sharing software, games, or utilities, without adequately disclosing that downloading the free materials would install adware on users' computers.[81] Although neither company violated any privacy policies, the Commission charged that the two businesses acted deceptively in not disclosing that

77. *Id.*

78. *Id.* at 450. The Commission also charged that Gateway's retroactive application of a materially changed privacy policy to previously collected information was unfair. *Id.* at 449.

79. The FTC has also found a company's failure to encrypt and secure users' information despite representations otherwise to be deceptive. *See* Complaint, FTC v. Rennert, No. CV-S-00-0861-JBR (D. Nev. 1999) (alleging that an online pharmacy's failure to encrypt user data or to transmit information using a Secure Sockets Layer, despite representations otherwise, was deceptive), *available at* http://www.ftc.gov/os/2000/07/iogcomp.htm; Complaint, United States v. ValueClick, Inc., No. CV-08-01711-MMM (C.D. Cal. 2008) (alleging that defendant companies' failure to encrypt sensitive information or implement other "reasonable and appropriate measures" to protect against unauthorized access to consumers' sensitive personal information was deceptive), *available at* http://www.ftc.gov/os/caselist/0723111/080317complaint.pdf.

80. Because the *Sears* matter involved the downloading of tracking software that is arguably spyware (Sears did not adequately disclose the scope of the software's tracking), it is helpful to see what kinds of practices the FTC has found to be deceptive in the adware and spyware context. Although an exact definitional difference between spyware and adware remains elusive, the Commission has described spyware as "software that aids in gathering information about a person or organization without their knowledge and which may send such information to another entity without the consumer's consent, or asserts control over a computer without the consumer's knowledge." Fed. Trade Comm'n, Spyware Workshop, Monitoring Software on Your PC: Spyware, Adware, and Other Software, http://www.ftc.gov/bcp/workshops/spyware/ (last visited Mar. 22, 2010).

81. *In re* Zango, Inc., Docket No. C-4186 (issued Mar. 7, 2007) (complaint), *available at* http://www.ftc.gov/os/caselist/0523130/0523130c4186complaint.pdf; *In re* DirectRevenue LLC, Docket No. C-4194 (issued June 26, 2007) (complaint), *available at* http://www.ftc.gov/os/caselist/0523131/0523131cmp070629.pdf.

adware would be installed along with the free materials:[82] "[Defendants] failed to disclose, or failed to disclose adequately, that such software is bundled with [] adware, which tracks and stores information regarding consumers' Internet use and displays pop-up[s]."[83] Again, the Commission did not explain how the companies' practices met each of the three deception factors. Because the companies' practices involved omissions of information, however, the Commission likely presumed that a consumer would be misled under the first factor. The Commission likely also presumed that a consumer's interpretation of the "lureware" to be free of adware was reasonable because the companies likely intended for consumers to believe that only the advertised freeware would be downloaded.[84] For the third factor, however, the Commission did specify that the bundling would be material to consumers in their initial decision to install the freeware.[85]

In the cases above, the Commission generally required companies to pay monetary equitable relief.[86] In *Gateway*, for example, the settlement order required that Gateway give up the $4,608 it earned from renting the data.[87] In *Zango* and *DirectRevenue*, the post-settlement final orders required that the defendant companies disgorge $3 million and $1.5 million respectively.[88]

D. PRIVACY AND BEHAVIORAL ADVERTISING

In addition to bringing administrative and judicial actions, the FTC undertakes other activities to evaluate and provide guidance on when a privacy practice is deceptive. The Commission, for example, often issues staff reports and hosts town halls, roundtables, and workshops to examine and solicit public opinion on privacy concerns.[89] The reports and workshops

82. *Zango* Complaint, *supra* note 81; *DirectRevenue* Complaint, *supra* note 81.

83. *DirectRevenue* Complaint, *supra* note 81.

84. *Zango* Complaint, *supra* note 81.

85. *In re* Zango, Inc., Docket No. C-4186 (issued Mar. 7, 2007) (decision and order), *available at* http://www.ftc.gov/os/caselist/0523130/0523130c4186decisionorder.pdf; *In re* DirectRevenue LLC, Docket No. C-4194 (issued June 26, 2007) (decision and order), *available at* http://www.ftc.gov/os/caselist/0523131/0523131do070629.pdf.

86. Since Toysmart was in bankruptcy proceedings, the Commission's settlement did not require the company to pay a specific amount. Rather, it prohibited Toysmart from selling its customer list as a stand-alone asset and allowed the sales of lists only as a part of a package including the entire website. In addition, any lists could only be sold to a "Qualified Buyer," defined as an entity in the "family commerce market" that expressly agreed to be Toysmart's successor-in-interest as to the customer information. Toysmart Trial Order, *supra* note 67.

87. Gateway, 138 F.T.C. at 470.

88. Zango Decision and Order, *supra* note 85; DirectRevenue Decision and Order, *supra* note 85.

89. FTC, Privacy Initiatives, *supra* note 25.

do not necessarily bind industry participants, but do establish informal standards for assessing a company's privacy practices. In 2007, for example, the FTC held a two-day public town hall to discuss privacy concerns raised by behavioral advertising, such as consumers' unawareness of data collection processes and the inadequacies of existing disclosures.[90] Following the Town Hall, the FTC staff released for public comment a set of proposed principles for behavioral advertising designed to incite industry self-regulation.[91] After receiving and reviewing sixty-three comments on the proposed principles, the FTC issued a final report, Self-Regulatory Principles for Online Behavioral Advertising (BAPs).[92]

The BAPs emphasized the need for "transparency and consumer control" with respect to disclosure:[93] "[C]ompanies that collect information for behavioral advertising should provide meaningful disclosures to consumers about the practice and choice about whether to allow the practice."[94] The FTC recommended that companies provide consumers notice and choice if the data reasonably could be associated with a particular consumer or with a particular computer or device, regardless of whether the data is personally identifying.[95]

---

90. Fed. Trade Comm'n, Ehavioral Advertising: Tracking, Targeting, and Technology, http://www.ftc.gov/bcp/workshops/ehavioral/index.shtml (last visited Mar. 22, 2010).

91. FED. TRADE COMM'N, ONLINE BEHAVIORAL ADVERTISING: MOVING THE DISCUSSION FORWARD TO POSSIBLE SELF-REGULATORY PRINCIPLES (Dec. 2007), http://www.ftc.gov/os/2007/12/P859900stmt.pdf.

92. FTC, BAPs, *supra* note 12, at 30. The Commissioners voted to approve the staff report 4–0. Commissioners Jon Leibowitz and Pamela Harbour also filed concurring statements. Chairman Leibowitz emphasized that the report's endorsement of self-regulation "is viewed neither as a regulatory retreat by the Agency nor an imprimatur for current business practice":

> Industry needs to do a better job of meaningful, rigorous self-regulation or it will certainly invite legislation by Congress and a more regulatory approach by our Commission. Put simply, this could be the last clear chance to show that self-regulation can—and will—effectively protect consumers' privacy in a dynamic online marketplace.

Concurring Statement of Commissioner Jon Leibowitz, Chairman of Fed. Trade Comm'n (Feb. 2009), *available at* http://www.ftc.gov/os/2009/02/P085400behavadleibowitz.pdf. Commissioner Harbour stated that a self-regulatory approach is not effective in part because consumers lack the information to exercise privacy choices. Concurring Statement of Commissioner Pamela Harbour, Commissioner of Fed. Trade Comm'n (Feb. 2009), *available at* http://www.ftc.gov/os/2009/02/P085400behavadharbour.pdf.

93. FTC, BAPs, *supra* note 12, at 11. The other BAPs are outside the scope of this Note, but include reasonable security and limited data retention, *id.* at 37–39, affirmative consent from consumers for material changes to privacy policies, *id.* at 39–41, and affirmative consent from consumers for use of sensitive data. *Id.* at 42–44.

94. *Id.* at 11.

95. *Id.* at 25.

Notably, the BAPs encouraged companies to "design innovative ways—*outside of the privacy policy*—to provide behavioral advertising disclosures and choice options to consumers."[96] The report noted possibilities such as:

> (i) providing "just-in-time" notice at the point at which a consumer's action triggers data collection;
>
> (ii) placing a text prompt next to, or imbedded in, the advertisement; and
>
> (iii) placing a prominent disclosure on the website that links to the relevant area within the site's privacy policy for a more detailed description.[97]

The FTC's report highlighted the possibility of placing near an advertisement a linked disclosure such as "why did I get this ad?" that would open to the pertinent section of a privacy policy explaining how and why the data would be collected.[98] According to the agency, 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."[99] Despite these possible disclosure mechanisms, the BAPs did not endorse one specific way in which companies should disclose tracking to consumers outside the privacy policy. The FTC's order in *Sears*, which requires Sears to disclose any tracking prior to and on a separate screen from any privacy policy, thus exemplifies the BAPs' recommendation that companies notify consumers outside of the privacy policy.[100]

II. *IN RE SEARS* COMPLAINT AND ORDER

When Sears launched its My SHC Community website, it intended the Community to be an interactive site through which Sears could send product information and market surveys to participants. To join the Community, consumers were required to download tracking software that would collect their personal data and computer usage information. Before consumers consented, Sears provided a Privacy Statement and User License Agreement (PSULA) listing the types of data that the application would collect, such as

96. *Id.* at 35 (emphasis added).
97. *Id.* at 33.
98. *Id.* at 35–36.
99. *Id.* at 36.
100. *See In re* Sears Holdings Mgmt. Corp., Docket No. C-4264 (issued Aug. 31, 2009) (decision and order), *available at* http://www.ftc.gov/os/caselist/0823099/090604 searsdo.pdf.

personal financial and health information transmitted in secure transactions.[101]

Despite Sears's PSULA, however, the FTC alleged that Sears's actions in promoting the My SHC Community were deceptive. It emphasized that (1) the company's initial invitation email stating that the software would track "online browsing" was inadequate, (2) the full disclosure of the scope of tracking was buried in the 75th line of the PSULA, (3) the installation box did not disclose the scope of the tracking application, and (4) the company failed to provide any desktop tray icons or other signs to indicate the running of the application on computers.[102] In so doing, the FTC signaled to businesses that privacy policies may no longer be adequate for disclosing material information about a company's information-tracking practices. In particular, if a company advertises or promotes a tracking application to consumers, it must disclose the types of data that the application tracks as well as how the data is to be used. Sections II.A and II.B below review the My SHC Community sign-up process as described in the Commission's complaint and summarize the requirements of the final order.

A. THE SIGN-UP PROCESS

From April 2007 until January 2008, Sears implemented a market research program that invited users of sears.com and kmart.com to join Sears's My SHC Community.[103] In order to participate, customers needed to download a software application that would track their behavior online and offline. The sign-up process involved a series of interactions with and messages from Sears, including an email invitation that the FTC found particularly deceptive because it did not disclose the scope of the Community application's tracking.

1. The Pop-Up Box Invitation

For a period of less than a year, fifteen out of every hundred visitors to the sears.com and kmart.com websites were presented with a My SHC Community pop-up box.[104] The pop-up box asked, "Ever wish you could talk directly to a retailer? Tell them about the products, services and offers that would really be right for you?"[105] It then invited visitors to become

101. Exhibit E, *supra* note 4.

102. *See* Complaint, *supra* note 2.

103. *Id.*

104. *In re* Sears Holdings Mgmt. Corp., Docket No. C-4264 (issued Aug. 31, 2009) (exhibit A), *available at* http://www.ftc.gov/os/caselist/0823099/090604searscomplaintaf.pdf.

105. *Id.*

members of the My SHC Community and to provide an email address to receive a follow-up email from Sears.[106] The FTC noted that neither the pop-up box nor the privacy policy accessed via a hyperlink in the pop-up box mentioned the tracking software application.[107]

2. The Email Invitation

To users who entered their addresses in the pop-up box, Sears emailed invitations to join the My SHC Community. The email described the Community as a "dynamic and highly interactive" online community sponsored by Sears where "your voice is heard and your opinion matters, and what you want and need counts!"[108] As community members, consumers could "help shape the future by sharing and receiving information about the products, services and offers that would really be right for you."[109] Participation was also "always on your terms and always by your choice."[110] The email stated:

> 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 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.[111]

In the subsequent paragraph, the email continued:

> We'll ask you to journal your shopping and purchasing behavior. Again, this will be when you want and how you want to record it—always on your terms and always by your choice. We'll also collect information on your internet usage. Community engagements are always fun and always voluntary![112]

In exchange for participation, members received ten dollars and registration in a sweepstakes.[113] Consumers who wished to join needed to click the "Join Today!" button located at the bottom of the invitation

106. *Id.*

107. Complaint, *supra* note 2. In the complaint exhibits, the FTC does not provide a screen shot of the privacy policy that was accessed via the hyperlink in the pop-up box.

108. Exhibit B, *supra* note 3.

109. *Id.*

110. *Id.*

111. *Id.* VoiceFive is an Internet market research company. *See* VoiceFive, Home Page, http://www.voicefive.com/About.aspx (last visited Mar. 22, 2010).

112. Exhibit B, *supra* note 3.

113. *Id.*

email.[114] If they retained the software on their computer for at least thirty days, they would receive the ten dollars.[115]

3. The Landing Page

Consumers who clicked on the "Join Today!" button were directed to a landing page that again highlighted the benefits of membership.[116] The landing page also noted that "community functions are fun and always voluntary."[117] The landing page featured a "Join Today!" button, above which Sears stated, "My SHC Community does NOT sell personal information."[118]

4. The Registration Page

Consumers who clicked on the "Join Today!" button in the landing page were directed to a registration page where they had to complete a user profile by submitting their name, address, age, and email address.[119] Below the entry fields, the registration page presented the My SHC Community PSULA in a scroll box that displayed ten lines of the document at a time.[120] A link to a printable version of the PSULA appeared below the scroll box.[121]

This PSULA described (1) the requirements for participation in the program; (2) the types of information collected, which included demographic information, survey response information, internet usage information, and computer hardware, software, and other configuration information; (3) how the information would be collected; (4) how the collected information would be used; (5) how the information would be secured; (6) whether cookies would be used; (7) how the consumer could stop participating; (8) how children were regarded; and (9) how changes to the PSULA would be communicated.[122]

The PSULA presented the scope of the tracking application on approximately the 75th line of the scroll box or the 35th line of the printable

114. *Id.*
115. *Id.*
116. Exhibit C, *supra* note 3.
117. *Id.*
118. *Id.*
119. *In re* Sears Holdings Mgmt. Corp., Docket No. C-4264 (issued Aug. 31, 2009) (exhibit D), *available at* http://www.ftc.gov/os/caselist/0823099/090604sears complaintaf.pdf.
120. *Id.*
121. *Id.*
122. Exhibit E, *supra* note 4. The PSULA also sets out participants' obligations to Sears and vice versa, as well as the other legal terms and conditions for participation. *Id.*

version.[123] The section on "Internet usage information" provided that the application would

> monitor[] 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.[124]

The application would also

> track[] 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 . . . .[125]

The PSULA also provided that the application did "not examine the text of . . . instant messages or e-mail messages," but could "review select e-mail header information from web-based e-mails as a way to verify . . . contact information and . . . online usage information."[126]

The section on "Computer hardware, software, and other configuration information" provided that

> [the] 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.[127]

The PSULA also stated that Sears would make "commercially viable efforts to automatically filter confidential, personally identifiable information such as UserID, password, credit card numbers, and account numbers."[128] If it inadvertently collected such information, Sears promised to make "commercially viable efforts to purge [its] database of such information."[129] The PSULA also described how consumers could stop participating in the online community and remove the application from their computers, but

123. *Id.*
124. *Id.*
125. *Id.*
126. *Id.*
127. *Id.*
128. *Id.*
129. *Id.*

Sears reserved the right to continue to use any information collected prior to the consumer's "resignation."[130]

A blank checkbox appeared below the scroll box PSULA and next to the statement: "I am the authorized user of this computer and I have read, agreed to, and have obtained the agreement of all computer users to the terms and conditions of the Privacy Statement and User License Agreement."[131] To continue with the registration process, consumers needed to check the box and click the "Next" button.[132]

5. The Installation Page

Once consumers submitted the requisite information, checked the box, and clicked "Next," they were directed to an installation page explaining the steps for downloading and installing the software.[133] Consumers had to click on the "Yes" or the "Install" button in the "Security Warning" dialogue box to install the application.[134] The FTC's complaint noted that the installation page did not provide information on the scope of the information the software would track.[135]

6. Desktop and System Tray Icons

Once installed, the tracking application ran continuously on consumers' computers and transmitted consumer data to Sears's servers.[136] The application did not display on the desktop or system tray area any visible indications that it was running.[137]

B. THE ORDER

The Commission's order did not require Sears to pay any monetary equitable relief.[138] Rather, it prevented Sears from engaging in further deceptive acts and practices by requiring that the company disclose its

130. *Id.*

131. *Id.*

132. Exhibit D, *supra* note 119.

133. *In re* Sears Holdings Mgmt. Corp., Docket No. C-4264 (issued Aug. 31, 2009) (exhibit F), *available at* http://www.ftc.gov/os/caselist/0823099/090604sears complaintaf.pdf.

134. *Id.*

135. Complaint, *supra* note 2.

136. *Id.*

137. The application was listed, however, as "My SHC Community" in the "All Programs" menu and the "Add/Remove" utilities; its executable file name was also listed as a running process in the Windows Task Manager. *Id.*

138. In contrast, the FTC ordered Gateway to pay $4,608, Zango to pay $3 million, and DirectRevenue to pay $1.5 million for similar deceptive practices. *See supra* text accompanying notes 87–88.

consumer data collection practices on a separate screen prior to the display of any end user license agreement, privacy policy, or terms of use.[139] This notice must "clearly and prominently" disclose potential uses of the tracked data, whether third parties may use the data, and what types of data may be tracked.[140] It must also disclose any tracking that includes (1) information from consumers' interactions with a specific set of websites or from a broader range of Internet interactions; (2) transactions or information exchanged with third parties in secure sessions; (3) interactions with shopping baskets, application forms, or online accounts; or (4) personal financial or health information.[141]

The order also required that Sears obtain consumers' express consent to download or install the tracking application and have their information collected.[142] Consumers must indicate their assent by clicking on a button that would not be "pre-selected as the default option" and would be "clearly labeled . . . to convey that the action would initiate the [download, installation, or collection] processes . . . ."[143]

III. TOO LITTLE TOO LATE: WHY SEARS'S PRACTICE WAS DECEPTIVE

In its complaint, the FTC acknowledged that Sears's application complied technically with its PSULA. Nevertheless, it concluded that Sears's practices were deceptive because the company's initial communications with consumers failed to disclose adequately the scope of Sears's information-tracking, which included data submitted during secure transactions. Under the Commission's three-factor analysis for deception, an act or practice is deceptive if it involves a representation, omission, or practice that misleads, or is likely to mislead, a consumer acting reasonably under the circumstances,

139. Order, *supra* note 100, § I.A.

140. *Id.*

141. *Id.*

142. *Id.*

143. *Id.*, § I.B. The order also requires Sears (1) to notify affected consumers that they have installed the tracking application and that the application collects and transmits to Sears and others the data described in the PSULA; (2) to notify consumers on how to uninstall the tracking application by (a) posting a clear and prominent notice on www.myshccommunity.com for two years and (b) informing affected consumers who complain or inquire about any tracking application; (3) to provide prompt, toll-free, telephonic, and email support to help affected consumers uninstall any tracking application. *Id.*, § II. Section III of the order also required that Sears (1) stop collecting data from the consumers who downloaded the software and (2) destroy any data it had collected from customers. *Id.*, § III.

and that representation, omission, or practice is material.[144] Because facts about the scope of tracking would be "material to consumers in deciding to install the software," the Commission charged that Sears's "failure to disclose these facts, in light of the representations made, was, and is, a deceptive practice."[145]

Although neither the FTC's complaint nor its order explicitly explains how Sears's actions met each factor of the agency's three-part deception analysis, this Part argues that the agency correctly found Sears's actions to be deceptive. Specifically, it argues that Sears's initial email describing its scope of tracking as "online browsing" was a material omission likely to mislead a reasonable consumer and that the misleading impression created by the email was not undone by Sears's later PSULA. Sections III.A, III.B, and III.C below explain how the FTC likely applied the three factors to reach its charges against Sears.

A. REPRESENTATION OR OMISSION LIKELY TO MISLEAD

The FTC likely found "a representation or omission likely to mislead" in Sears's initial invitation email to consumers. This initial email referred to the application's scope of tracking twice. First, at the end of the fourth paragraph, Sears stated that the customer would be asked to download "research software" that would "confidentially track [the customer's] online browsing."[146] Second, in the middle of a subsequent paragraph, Sears stated, "We'll also collect information on your internet usage."[147]

Given the extensive scope and sensitive nature of Sears's tracking, the use of the term "online browsing," even if supplemented by the second disclosure that Sears would "also collect information on your internet usage," was an inadequate representation or omission. First, Sears used the software to collect information on nearly "all of the [consumers'] Internet behavior," including secure transactions.[148] The application also collected information from the headers of emails.[149] As one public comment to the *Sears* consent agreement noted, a "wide continuum of information collection practices" exists on the Internet, ranging from tracking transactions on a company's own site to improve the site's navigation, to tracking passwords, account

144. *See supra* Section I.C.
145. Complaint, *supra* note 2.
146. Exhibit B, *supra* note 3.
147. *Id.*
148. Exhibit E, *supra* note 4.
149. *Id.*

numbers, and secure transactions from unrelated third-party sites.[150] In using a broad term such as "online browsing," which could describe practices falling on either end of the continuum mentioned in the public comment, this Note agrees with the Commission's finding that Sears failed to describe adequately the extent of its tracking.[151] More specifically, this Note argues that Sears failed to describe up front its most extensive type of tracking. Because the invitation email did not specifically disclose the scope of Sears's tracking, the email allowed consumers to believe that the tracking was on the minimal rather than the extensive end of the invasiveness continuum. As such, this omission or representation was likely to mislead a consumer.

Second, Sears's initial email failed to disclose that the software would track consumers' offline behavior. The email identified "online browsing" and "internet usage" as the types of information that the tracking application would collect.[152] Neither phrase suggested, however, that the application would also harvest information about computer hardware and software configuration, the speed of the computer processor, the memory capacities, the type of printer or router, or the pace at which consumers clicked links, typed webpage names, and used shortcut keys.[153] The failure of the initial email to state that offline behavior would be tracked was another omission likely to mislead.

B. CONSUMER ACTING REASONABLY UNDER THE CIRCUMSTANCES

Under deception analysis, the second factor that the Commission considers is what a reasonable consumer under the circumstances would have believed about the scope of Sears's tracking. Although the Commission's complaint did not explicitly address this factor, the FTC has previously stated that "to be considered reasonable, the interpretation or reaction does not have to be the only one. When a seller's representation conveys more than one meaning to reasonable consumers, one of which is false, the seller is liable for the misleading interpretation."[154] Correspondingly, "when the first contact between a seller and a buyer occurs through a deceptive practice, the law may be violated even if the truth is subsequently

150. Letter from Angela Gleason, Assoc. Gen. Counsel, Amer. Ins. Ass'n, to the Fed. Trade Comm'n (July 2, 2009), *available at* http://www.ftc.gov/os/comments/searsholdings/542583-00004.html.

151. *See id.*

152. Exhibit B, *supra* note 3.

153. Exhibit E, *supra* note 4.

154. FTC, Deception Policy, *supra* note 46, § III.

made known to the purchaser. Pro forma statements or disclaimers may not cure otherwise deceptive messages or practices."[155]

Applying these standards, this Note argues that a reasonable consumer would not have believed that the scope of Sears's monitoring would be so great as to include information submitted in secure transactions or activities undertaken offline. Sears's initial communications assured consumers that they would have choice and control over their participation. The first pop-up box asked, "Ever wish you could talk directly to a retailer? Tell them about the products, services and offers that would really be right for you?"[156] The subsequent invitation email described the My SHC Community as a "dynamic and highly interactive" online community where "your voice is heard and your opinion matters, and what you want and need counts!"[157] Sears also repeatedly emphasized that participation was "always on your terms and always by your choice."[158]

In contrast to these exuberant claims about user participation being "always on your terms and always by your choice," the initial email used the general term "online browsing" to describe the scope of consumer data tracking.[159] This term allowed reasonable consumers to believe that the scope of tracking would be minimal when it was actually extensive.[160] Because a seller is liable for a misleading representation when the representation conveys more than one meaning to reasonable consumers,[161] this Note concludes that the FTC correctly held Sears responsible for creating the misleading interpretation that its tracking would be minimal.

Sears did eventually disclose the full scope of tracking of online and offline behavior in the PSULA.[162] However, as the complaint pointed out, this disclosure did not appear in the PSULA until the 75th line.[163] In addition, Sears's suggestion in the invitation email that its application tracked "online browsing" or "internet usage" created a misleading impression that the PSULA disclosure could not cure.[164] That Sears is a longstanding brick and

155. *Id.*
156. Exhibit A, *supra* note 104.
157. Exhibit B, *supra* note 3.
158. *Id.*
159. *See* Exhibit B, *supra* note 3.
160. *See supra* Section III.A.
161. *See* FTC, Deception Policy, *supra* note 46, § III.
162. *See* Exhibit E, *supra* note 4.
163. *See* Complaint, *supra* note 2 (observing that the description began on about the 75th line of the PSULA scroll box); Exhibit E, *supra* note 4.
164. *See* FTC, Deception Policy, *supra* note 46, § III (providing that "when the first contact between a seller and a buyer occurs through a deceptive practice, the law may be violated even if the truth is subsequently made known to the purchaser").

mortar company may also have weighed against it; because consumers are more likely to trust a website run by Sears than one run by an unknown vendor, consumers are less likely to expect Sears to track their personal data so pervasively.[165] As such, this Note concludes that a reasonable consumer would not have believed that Sears would monitor information submitted in secure transactions or activities undertaken offline.

C. MATERIALITY OF REPRESENTATION OR OMISSION

Under the third factor, the Commission considers whether the representation or omission was material. Although the Commission did not describe exactly how Sears's omissions about the scope of its tracking were material,[166] the complaint suggests that the tracking was so extensive that consumers likely would not have joined the community had they been initially informed of the scope.[167] Such a conclusion may be supported by a 2009 study on Americans' attitudes toward behavioral advertising conducted by the University of California, Berkeley, School of Law and the University of Pennsylvania's Annenberg School for Communication.[168] The researchers found that 66% of Americans objected to online tracking by advertisers.[169] When told how advertisers tracked their online information, participants' opposition to behavioral advertising increased: 84% opposed tracking that would monitor their activities on third-party sites, and 86% opposed tracking that would monitor their offline activities.[170] Since Sears collected consumers' data from third-party sites and offline activities, this study seems to support a conclusion that knowledge of Sears's tracking practices would have affected consumers' decisions to participate in the My SHC Community. As such, this Note concludes that Sears's failure to disclose the scope of its tracking in the initial email constitutes a material omission.

---

165. *See* Gindin, *supra* note 9, at 29 (observing that the *Sears* matter is the FTC's first enforcement action for behavioral tracking against a prominent brick and mortar company).

166. The Commission presumes materiality in cases where the seller knew, or should have known, that an ordinary consumer would need the omitted information to evaluate the product or service. *See supra* Section I.C.1; FTC, Deception Policy, *supra* note 46, § IV.

167. A "material" misrepresentation or omission is one that is "likely to affect a consumer's choice of or conduct regarding a product." *See supra* Section I.C.1; FTC, Deception Policy, *supra* note 46, § IV.

168. JOSEPH TUROW ET AL., AMERICANS REJECT TAILORED ADVERTISING AND THREE ACTIVITIES THAT ENABLE IT (Sept. 2009), *available at* http://ssrn.com/abstract=1478214.

169. *Id.*, Table 2, at 15.

170. *Id.*, Tables 2 and 3, at 15.

D. SEARS'S LIABILITY FOR DECEPTIVE PRACTICES

As noted in Section II.B, the Commission did not require Sears to pay monetary equitable relief, as was the case in the matters of *Gateway Learning Corp.*, *Zango, Inc.*, and *DirectRevenue LLC*.[171] This may be because the *Sears* matter is the first in which the Commission charged that a privacy policy disclosing a company's collection and usage practices failed to undo the company's earlier deceptive practice. Moreover, Sears did not violate its privacy policy (as Gateway had) or fail to disclose that software would be installed (as the Zango and DirectRevenue defendants had).[172] As FTC Chairman Jon Leibowitz commented about the *Sears* matter, "Nobody argues that the folks at Sears are bad people who wanted to do bad things with the information they gleaned from these consumers. To the contrary, I don't think they even knew exactly what they expected to learn from the data."[173] Now that the FTC has signaled that detailed privacy policies do not immunize a company from liability for deceptive privacy practices, however, companies may face heavier consequences in the future.

IV. RECOMMENDATIONS FOR PRIVACY DISCLOSURES AFTER *IN RE SEARS*

Given that privacy policies may no longer be adequate in effectively disclosing a company's privacy practices, the *Sears* order provides useful guidelines for companies on how data-tracking practices should be disclosed.[174] In particular, *Sears* provides a concrete example of how the FTC may enforce privacy protection under its behavioral advertising principles. The rest of this Note recommends measures that companies can adopt to comply with *Sears*'s disclosure standards and identifies how these measures fit alongside the FTC's principles for behavioral advertising. These recommendations include pre-privacy policy disclosures, multiple disclosures, disclosures in initial communications, disclosure of the most extensive tracking, and disclosure in system tray icons.

171. *See supra* text accompanying notes 87–88.

172. *See id.*

173. Jon Leibowitz, Chairman of the Fed. Trade Comm'n, Introductory Remarks at FTC Privacy Roundtable 1 (Dec. 7, 2009), *available at* http://www.ftc.gov/speeches/leibowitz/091207privacyremarks.pdf.

174. *See* Gindin, *supra* note 9, at 5–8 (identifying seven lessons to be learned from the *Sears* matter, including clear and prominent presentation of terms that are likely material to consumers, enhanced notice for "sensitive" personal information, and advertising materials that clearly and conspicuously disclose material information).

A. DISCLOSURE PRIOR TO THE PRIVACY POLICY

First, companies should disclose material information about their tracking practices on a separate screen prior to the privacy policy. The *Sears* order requires that a separate disclosure clearly and prominently describing the scope of monitoring be displayed prior to the display of any privacy policy, end user license agreement, or terms of use.[175] This requirement reflects the Commission's finding that a privacy policy may be inadequate if a company's other communications with consumers create a misleading impression.[176] It also reflects the Commission's recognition that consumers often do not read privacy policies and would miss material information about a product or service if that information were only disclosed in the middle of a long privacy policy or agreement, as was the case with Sears's PSULA.[177] By requiring that disclosure about the scope of tracking be made before an end user license agreement or privacy policy, the Commission seeks to increase the chances that consumers will receive such material information.

This requirement also exemplifies the FTC's first principle for behavioral advertising, which provides that disclosures about behavioral advertising be made "*outside* of the privacy policy."[178] Although the Commission recognized that it has become customary for companies to include most privacy disclosures in an online privacy policy and that alternative mechanisms for disclosure may confuse consumers, it also recognized that long and difficult-to-understand privacy policies are not effective in communicating information to consumers.[179]

B. DISCLOSURE IN MULTIPLE PLACES

Second, companies should display pre-privacy policy disclosures in multiple locations on its website. The *Sears* complaint suggests that prior to its PSULA display, Sears could have disclosed the scope of its tracking in several locations, including the pop-up box invitation, the email invitation, and the landing page.[180] The BAPs suggest options such as "just-in-time" notices that are provided when a consumer's action triggers data collection or prominent disclosures that link to relevant areas within a more detailed privacy policy.[181] The BAPs further suggest placing a linked question such as

175. Order, *supra* note 100, § I.A.
176. *See* FTC, Deception Policy, *supra* note 46, § III.
177. *See* Complaint, *supra* note 2.
178. FTC, BAPs, *supra* note 12, at 35 (emphasis added).
179. *Id.*
180. *See supra* Section II.A.
181. FTC, BAPs, *supra* note 12, at 33.

"Why did I get this ad?" near an advertisement. The linked question would bring the user to the pertinent section of a privacy policy explaining how and why data would be collected.[182]

By having multiple short disclosures that link to relevant sections of a comprehensive privacy policy, companies can avoid some of the concerns raised by public commentators in response to the proposed BAPs, which included confusing consumers who have come to rely on a single privacy policy.[183] Multiple pre-policy disclosures need not, however, replace a comprehensive privacy policy. Rather, they can work alongside the longer policy by offering consumers multiple entry points into the policy; at the same time, multiple short disclosures offer the most material information in digestible formats.

Given the limited space available for short disclosures, commentators also expressed concern over which types of information would be important enough to warrant pre-privacy policy disclosure.[184] In *Sears*, the FTC indicated that information warranting pre-privacy policy disclosure included what types of data the application would track, how the tracked data would be used, and whether the data would be used by a third-party. Given that the FTC has not provided an exhaustive list of information warranting pre-privacy policy disclosure, companies seeking to comply with FTC disclosure standards should test proposed disclosures to see which types of additional information help to inform consumers effectively. The BAPs, for example, encourage companies to undertake "empirical research to explore the effects of possible disclosures on consumer understanding."[185] A company that undertakes such research and applies what it learns might not only avoid liability but also enrich the Commission's understanding of effective privacy disclosures.

C. DISCLOSURE IN INITIAL COMMUNICATIONS

In addition to multiple pre-privacy policy disclosures, a company should make sure that its initial contacts with consumers do not create misleading impressions about the company's tracking practices. The *Sears* matter shows that a misleading initial impression is not always reparable by a later complete

182. *Id.* at 35–36.

183. *Id.* at 33.

184. *See* Gindin, *supra* note 9, at 20 (noting that not all disclosures can be presented first and asking how a company should decide which disclosures to provide and in which order); Gleason, *supra* note 150 (observing that "prioritization and separation of consumer disclosures would force companies to decide without additional guidance what type of disclosure should be presented to a consumer first, and what should follow").

185. FTC, BAPs, *supra* note 12, at 37.

disclosure. As such, companies should describe the full scope of tracking in their first relevant communications with consumers. In *Sears*, for example, the first pop-up box inviting consumers to join the My SHC Community could have disclosed the scope of tracking. Alternatively, Sears could have summarized details about the tracking in the initial email and then linked to the complete PSULA. This way, the privacy policy would be comprehensive and centrally located; at the same time, short initial disclosures would highlight material information about tracking up front.

D. DISCLOSURE OF THE MOST EXTENSIVE TRACKING

In their pre-privacy policy disclosures, companies should specify their most extensive form of tracking rather than use general terms that could span the continuum of tracking invasiveness. Sears's initial email was problematic because it used the term "online browsing" to describe tracking, and that phrase could signify either minimal or extensive tracking.[186] Had Sears initially disclosed that it would track information submitted by consumers in secure sessions, consumers would have known more clearly that Sears's tracking was extensive. Accordingly, the *Sears* order requires pre-privacy policy disclosures related to the tracking of consumers' (1) interactions with a specific set of websites or broader Internet interactions; (2) transactions or information exchanged with third parties in secure sessions; (3) interactions with shopping baskets, application forms, or online accounts; and (4) personal financial or health information.[187]

E. DISCLOSURE IN THE SYSTEM TRAY

The *Sears* complaint also suggests that a company should design a tracking application so that it displays an icon in a computer's system tray area when the tracking program is running. The complaint notes that although Sears's tracking software ran at all times on consumers' computers,[188] the application did not indicate its presence on the desktop or the system tray icon area.[189] Thus, though the application's executable file name would be listed as a running process in any task manager program that provided information about the processes and programs running on a computer, Sears's failure to indicate visibly the ongoing running of the application heightened the inadequacy of the company's disclosures.

186. *See supra* III.A–B.
187. Order, *supra* note 100, § I.A.
188. Complaint, *supra* note 2.
189. *Id.*

F. EXPRESS CONSENT MAY NOT BE ENOUGH

Lastly, the Commission's order requires that Sears obtain express consent from consumers regarding the download and installation of any tracking applications.[190] The BAPs similarly recommend that companies should only collect sensitive data after obtaining affirmative, express consent from the consumer targeted to receive the behavioral advertising.[191] The *Sears* case shows that even obtaining express consent is not always enough to ensure that a practice is not deceptive. Although the consumers in *Sears* were required to click that they "ha[d] read, agree[d] to, and ha[d] obtained the agreement of all computer users to the terms and conditions of the [PSULA],"[192] the FTC still found Sears's practice to be deceptive because the full scope of tracking was not disclosed until approximately the 75th line of the scroll box PSULA.[193] Thus, even if companies obtain consumers' express consent, they should consider the measures recommended in Sections IV.A–E so that they disclose adequately the scope of their tracking.

V. CONCLUSION

Although privacy lawyers were surprised by the FTC's complaint and Sears's settlement, this Note has argued that the Commission properly analyzed Sears's conduct as a deceptive practice under Section 5 of the FTCA. Sears failed to disclose the scope of personal information that the My SHC Community tracking application would monitor, and this failure was a material omission likely to create a misleading impression in reasonable consumers. Although Sears did ultimately describe the scope of its tracking in the PSULA, that disclosure was inadequate, particularly given Sears's emphasis on user choice and control in its initial contacts with consumers. To comply with the disclosure standards identified in *Sears* and the FTC's principles for behavioral advertising, companies should adopt privacy disclosure practices that include multiple pre-privacy policy disclosures linked to corresponding sections of a comprehensive privacy policy, disclosure of the most extensive form of tracking in initial communications with consumers, and system tray icons that indicate when an application is running.

Although this Note has focused on the implications of *In re Sears* for behavioral advertising, the disclosure standards set forth in the case will likely

190. Order, *supra* note 100, § I.B.
191. FTC, BAPs, *supra* note 12, at 42.
192. Exhibit D, *supra* note 119.
193. *See* Complaint, *supra* note 2.

apply beyond that context. In December 2009, the FTC held the first of three public roundtables focused on privacy challenges created by technology and business practices that collect and use consumer data, such as social networking, cloud computing, and mobile marketing. At the opening of the first roundtable, FTC Chairman Jon Leibowitz described *Sears* as an example of how companies are grappling with protecting privacy while collecting and using consumer data:

> [W]hile the extent of tracking was described in [Sears's PSULA], that disclosure wasn't sufficiently clear or prominent given the extent of the information tracked, which included online bank statements, drug prescription records, video rental records, library borrowing histories, and the sender, recipient, subject, and size for web-based e-mails.
>
> So consumers didn't consent with an adequate understanding of the deal they were making.[194]

As the collection and use of consumer data develops across a variety of contexts, the privacy disclosure requirements outlined in *Sears* provide a useful starting point for companies seeking to comply with FTC standards. Yet because the technologies, business practices, and consumer expectations in each context inevitably differ, *Sears*'s privacy disclosure requirements should be applied with nuance and reconsidered as needed.

194. Leibowitz, Privacy Remarks, *supra* note 173, at 1.