TULANE JOURNAL OF TECHNOLOGY AND INTELLECTUAL PROPERTY

VOLUME 19 FALL 2016

Reconsidering Privacy-Promising Technologies

Jasmine McNealy*
Heather Shoenberger†

I. INTRODUCTION

In December 2014, the Federal Trade Commission (FTC) approved its final order settling charges against Snapchat, Inc., a mobile application (app) company that claimed users could send messages that

* Jasmine McNealy, Assistant Professor, University of Florida College of Journalism and Communications; Ph.D., University of Florida, 2008, M.A/J.D., University of Florida, 2006; B.S., University of Wisconsin, 2002.

† Heather Schoenberger, Assistant Professor, University of Oregon School of Journalism and Communication; J.D., University of Missouri, 2006; M.A., University of Missouri, 2006; Ph.D., University of Missouri, 2014.

would "disappear" at a specified time in spite of attempts to save them.[1] The original complaint issued against Snapchat was based on six counts of deceptive acts and practices.[2] These deceptive acts included claims by Snapchat that messages sent from the app would automatically erase after the amount of time set by the user and that users would be notified if the receiver had taken a screenshot of a message.[3] Neither claim by Snapchat proved true. Message-retrieval methods were widely publicized and reported in the technology press circles[4]: computer forensic experts discovered simple ways to find "deleted" messages[5] and users found ways to outwit the screenshot notice feature.[6] Consequently, Snapchat's settlement order forbade the app from continuing to make similar claims related to its messages.[7]

Perhaps more important than the FTC's settlement with Snapchat is the power with which the FTC brought a claim against the company. With the passage of the Federal Trade Commission Act of 1912, Congress granted the FTC broad powers to regulate advertising and trade practices that are false, deceptive, or misleading.[8] When evaluating whether advertisements or practices are deceptive, the FTC thus uses a three-part test that evaluates: (1) whether there was a practice, representation, or omission; (2) whether the deception was misleading "from the perspective of a consumer acting reasonably in the circumstances"; and (3) whether the trade practice or representation was material.[9]

---

1. Decision and Order, Snapchat, Inc., No. C-4501 (F.T.C. Dec. 23, 2014), https://www.ftc.gov/system/files/documents/cases/141231snapchatdo.pdf [hereinafter Snapchat Decision & Order]; *see also* Larry Magid, *Snapchat Settles FTC Charges About Disappearing Posts that Don't Disappear*, FORBES (May 8, 2014, 2:38 PM), http://www.forbes.com/sites/larrymagid/2014/05/08/snapchat-settles-ftc-charges-about-false-disappearing-posts/#6688576919e5.

2. Compl., Snapchat, Inc., No. C-4501 (F.T.C. May 8, 2014), https://www.ftc.gov/system/files/documents/cases/140508snapchatcmpt.pdf [hereinafter Snapchat Compl.].

3. *Id.*

4. *Id.*; *see also* Paul Ducklin, *Snapchat Images that Have "Disappeared Forever" Stay Right on Your Phone . . .*, NAKED SECURITY (May 10, 2013), https://nakedsecurity.sophos.com/2013/05/10/snapchat-images-that-have-disappeared-forever-stay-right-on-your-phone/.

5. Snapchat Compl., *supra* note 2, at *3; *see, e.g.*, Ducklin, *supra* note 4 (providing instructions on how to find "deleted" snapchat photos).

6. Snapchat Compl., *supra* note 2, at *4.

7. *See* Snapchat Decision & Order, *supra* note 1, at *2.

8. *See* Federal Trade Commission Act, 15 U.S.C. §§ 41-56 (2012).

9. Cliffdale Assocs., Inc., 103 F.T.C. 110, 175-76 (1984); *see also* Candace Lance Oxendale, *The FTC and Deceptive Trade Practices: A Reasonable Standard?*, 35 EMORY L.J. 683, 693-95 (1986) (discussing the significance of *Cliffdale's* three-prong test); E. Thomas Sullivan & Brian A. Marks, *The FTC's Deceptive Advertising Policy: A Legal and Economic Analysis*, 64 OR. L. REV. 593, 598-601 (1985) (analyzing the change in FTC deceptive advertising from both legal and economic perspectives); Jack E. Karns, *The Federal Trade*

The first and third criteria for deceptiveness are easily understood in the Snapchat case. Snapchat made statements about its messaging system that were not completely accurate and these statements about the attributes of its system persuaded consumers to use the app.

The second criterion merits closer scrutiny. The FTC examines "reasonableness" in two ways. First, it considers whether consumer expectations for a product or service were reasonable.[10] Second, the FTC evaluates whether a consumer's interpretation of practices, representations, or omissions are reasonable in light of the information surrounding that practice, representation, or omission.[11] As aforementioned, Snapchat's claims that messages would disappear and that users would be informed anytime receivers of the message attempted to copy the message were debunked using methods that did not require superior technical knowledge.[12] Users, nevertheless, still flock to the app based on these promises.[13]

Three key questions thus arise. First, are Snapchat users' expectations "reasonable" in light of how easily others have found ways to circumvent the app's "privacy" features and settings? Second, if understanding how information is stored, retrieved, or manipulated is fundamental to using apps like Snapchat (and other privacy-promising technologies), why do consumers not know of or understand the simple functionalities of pervasive technologies, particularly when their privacy is at risk? Third, if app-users (and the public in general) significantly lack information literacy in the digital context, what, then, does this mean for the FTC's "reasonable person" standard with respect to deceptive practice claims in the digital context?

With these three questions in mind, this Article reconsiders the idea of the "reasonable person" in the digital age. To this end, Part II of this

---

Commission's Evolving Deception Policy, 22 U. RICH. REV. 399 (1987) (examining the changes to the FTC's deceptive trade acts policy).

10. *See* Heinz W. Kirchner, 63 F.T.C. 1282, 1290-93 (1963).

11. *See* Simeon Management Corp. Inc., 87 F.T.C. 1184, 1219 (1976), *aff'd*, 579 F.2d 1137 (9th Cir. 1978) (finding that the Commission interprets advertisements based on the "net general impression" of the consumer).

12. *See* Franziska Roesner, Brian T. Gill & Tadayoshi Kohno, *Sex, Lies, or Kittens? Investigating the Use of Snapchat's Self-Destructing Messages*, *in* FINANCIAL CRYPTOGRAPHY AND DATA SECURITY 66 (Nicolas Christin & Reihaneh Safavi-Naini eds., 2014).

13. *Compare id. with* Alyson Shontell, *Snapchat Is a Lot Bigger than People Realize and It Could Be Nearing 200 Million Active Users*, BUS. INSIDER (Jan. 3, 2015, 9:54 AM), http://www.businessinsider.com/snapchats-monthly-active-users-may-be-nearing-200-million-2014-12 (arguing that Snapchat's user base is growing at an abnormally quick pace) *and* Stuart Dredge, *Ten Things You Need To Know About Snapchat*, GUARDIAN (Nov. 13, 2013, 10:08), http://www.theguardian.com/technology/2013/nov/13/snapchat-app-sexting-lawsuits-valuation (stating that the main appeal of the Snapchat is its ephemeral messaging).

Article first defines privacy-promising technologies in detail and discusses the current regulations covering these technologies. Part III examines the evidence detailing the general public's lack of information and digital literacy, as well as the ramifications for privacy in this digital age. In this discussion, this Article discusses the overall finding that people are not as technologically savvy as, perhaps, the technology requires, particularly with respect to maintaining the privacy of their information. It argues that the literature provides evidence of the necessity for heightened standard for privacy-promising technologies.

Part IV supplies an overview of the "reasonable person" standard used by the FTC to analyze deceptive practice claims in general. Part IV pays particular attention to the standards the Commission adopted to assess advertising and marketing claims directed to particular groups and to the policy implications of such standards. Ultimately, Part IV argues that the FTC should use a heightened standard of scrutiny, similar to the standard with which the FTC examines complex claims that a reasonable person would not normally completely understand,[14] to evaluate privacy-promising technologies' claims. A heightened standard of review would take into account the nuanced understandings of digital privacy and data disclosure in the digital consumer setting.

This Article ends by reevaluating the meaning of a "reasonable person" in the digital age and proposes guidelines for the FTC to adopt for evaluating the advertising and trade practices of privacy-promising technologies. These guidelines would be reminiscent of the FTC's Endorsement Guides, Weight-loss Supplements Guides, and Green Guides provided to other big-money industries over which the FTC has regulatory power.[15] Companies developing privacy-promising technologies will likely comply with the guidelines issued by the FTC because failure to do so could mean the company has not met regulatory requirements, which would result in the FTC bringing an enforcement action against the developer.

---

14. *See, e.g.*, Simeon Management, 87 F.T.C. 1184, 1230 (1976) (ruling that the advertising of a weight loss drug that claimed it was safe and effective could lead consumers to believe that the claims were based on government approval).

15. *See, e.g.*, Jeremy Rosen, *Requirements for Environmental Marketing Claims Under the Federal Trade Commission's Guides*, 4 ENVTL. LAW. 241, 243 (1997); Edward Correia, *The Federal Trade Commission's Regulation of Weight-Loss Advertising Claims*, 59 FOOD & DRUG L.J. 585, 585 (2004); Jessica Godell, *Consumer-Generated Media and Advertising—Are They One and the Same: An Analysis of the Amended FTC Guides Concerning the Use of Endorsements and Testimonials in Advertising*, 10 J. MARSHALL REV. INTELL. PROP. L. 206, 206 (2010).

Privacy, particularly with respect to data and information in digital technology, has become a buzzword. The recent cases demonstrate that privacy-promising technologies, and the advertising and trade practices related to these technologies, are a special kind of problem for consumers, and ultimately, the FTC.

II. DEFINING PRIVACY-PROMISING TECHNOLOGY

In this Article, the term privacy-promising technology refers to technology, such as apps, software, and online tools, in which the maker or creator uses the promise of privacy, or data control, to induce consumers to use their digital tool. Snapchat, for example, would be a privacy-promising technology because it used the promise of information control to induce consumers to use the app. For example, Snapchat made the specific marketing claim that users could control how long their friends would be able to see their messages.[16] To be sure, Snapchat is not the only organization to use the promise of data control to market its service. Whisper, a message-creation app, billed itself as allowing users to post anonymous messages.[17] The messages, or "whispers," appeared to other users of the app in the form of text superimposed over an image.[18] It was later discovered that users were not completely anonymous as the app tracked their locations and collected and indefinitely stored their data.[19]

Other examples of privacy-promising technologies include Silent Circle and Yik Yak.[20] On its website, Silent Circle claims to offer "privacy in the mobile-first world" and uses the catchphrase "privacy without compromise" to advertise its Blackphone 2 product.[21] It also claims it has created the "world's first enterprise privacy platform."[22] In all of these statements, Silent Circle uses the idea of privacy and the promise of data control to entice users to adopt its service.

---

16. *See* Snapchat Compl., *supra* note 2, at *2.

17. *Community Guidelines*, WHISPER, https://whisper.sh/guidelines (last visited October 27, 2016).

18. *See* WHISPER, https://whisper.sh (last visited October 27, 2016).

19. Paul Lewis & Dominic Rushe, *Revealed: How Whisper App Tracks "Anonymous" Users*, GUARDIAN (Oct. 16, 2014, 11:35), http://www.theguardian.com/world/2014/oct/16/-sp-revealed-whisper-app-tracking-users.

20. Yik Yak is a location-based mobile social media app that allows users to anonymously post discussion threads, which are then available to others within a five-mile radius. YIK YAK, http://www.yikyakapp.com/ (last visited Feb. 13, 2016).

21. Javier Aguera, *Privacy in the Mobile-First World*, SILENT CIRCLE, https://silentcircle.com/blog/privacy-in-the-mobile-first-world/ (last visited Feb. 13, 2016).

22. *Introducing the World's First Enterprise Privacy Platform*, SILENT CIRCLE (Mar. 2, 2015), https://www.silentcircle.com/blog/introducing-the-worlds-first-enterprise-privacy-platform/.

This Article does not highlight these companies' privacy claims to evoke incredulity about whether these assertions are completely truthful. Instead, these examples are meant to illustrate how technology companies use privacy promises to market their technologies. Companies appeal to the public's concerns over the privacy of their networked data by including privacy promises, including privacy policies, in their marketing schemes.[23]

In 2015, both Microsoft and Apple used privacy as a marketing tool.[24] As a part of their marketing schemes, each company updated their websites with a detailed explanation of their respective privacy policies,[25] and an explanation of how each organization used customer data.[26] Apple in its explanation of its privacy policy also made a note of how its privacy policy differed from at least one of its major competitors, without expressly stating the company's name.[27] Although these privacy policy explanations are not exactly like the privacy promises employed by the privacy-promising technologies mentioned above, it illustrates how technology companies use consumers' privacy concerns and the promises of data control as a competitive advantage.[28] Companies also make privacy promises to "garner better publicity, to limit liabilities, and to comply with regulations."[29]

---

23. *When Consumer Privacy Is a Competitive Advantage, Security Can Be a Marketing Tool*, HYTRUST (Mar. 20, 2015), https://www.hytrust.com/blog/when-consumer-privacy-is-a-competitive-advantage-security-can-be-a-marketing-tool/.

24. *See* Peter Sayer, *Apple, Microsoft Wield Privacy as Marketing Tool*, COMPUTERWORLD (Sept. 29, 2015, 9:13 AM), http://www.computerworld.com/article/2987249/data-privacy/apple-microsoft-wield-privacy-as-marketing-tool.html.

25. *Id.*

26. *Id.*

27. *Id.* ("Some companies mine your cloud data or email for personal information to serve you targeted ads. We don't.").

28. *Cf.* Fred Campbell, *Internet Advertisers Seek Competitive Advantages Through Privacy Regulation*, FORBES (Sept. 24, 2015, 4:49 PM), http://www.forbes.com/sites/fredcampbell/2015/09/24/internet-advertisers-seek-competitive-advantages-through-privacy-regulation/; Timothy Morey, *Make Customer Data and Trust a Competitive Advantage*, HARV. BUS. REV. (May 13, 2015, 12:00 PM), https://hbr.org/webinar/2015/05/make-customer-data-and-trust-a-competitive-advantage; Jeff John Roberts, *The Competitive Advantages of Data Privacy*, BLOOMBERG (July 29, 2013, 10:39 AM), http://www.bloomberg.com/bw/articles/2013-07-29/the-competitive-advantages-of-data-privacy; Ken Tysiac, *Use Data Privacy To Gain a Competitive Advantage*, J. ACCT. (Mar. 4, 2014), http://www.journalofaccountancy.com/news/2014/mar/20149721.html.

29. Günter Karjoth et al., *Translating Privacy Practices into Privacy Promises—How To Promise What You Can Keep*, *in* IEEE 4TH INTERNATIONAL WORKSHOP ON POLICIES FOR DISTRIBUTED SYSTEMS AND NETWORKS 135, 135 (2003).

Studies have concluded that consumers infer privacy promises from publicly available privacy policy statements,[30] or from visible symbols, such as TRUSTe seals indicating that a company has demonstrated compliance with certain privacy practice standards.[31] Visible symbols may trigger privacy-related heuristics that help consumers decide whether to use a service or app.[32] Consumers engage in a privacy calculus to weigh the costs and benefits of disclosing their personal information.[33] Most studies on online privacy assume that consumers make rational information disclosure decisions, as per the Communication Privacy Management (CPM) theory.[34] The CPM theory is based on the intersection of five principles: information ownership, control, self-regulation through privacy rules, stewardship of the information of others, and the regulation of privacy breakdowns.[35] These principles are inherent in the way individuals decide whether to disclose their private information.[36]

While not all consumers read privacy policies every time they decide to use a service or app,[37] the FTC enforces the privacy promises

---

30. *See, e.g.*, George R. Milne & Mary J. Culnan, *Strategies for Reducing Online Privacy Risks: Why Consumers Read (or Don't Read) Online Privacy Notices*, 18 J. INTERACTIVE MARKETING 15 (2004) (finding that consumers who read privacy policies demonstrated higher levels of trust in the policy claims).

31. *Certification Standards*, TRUSTE, https://www.truste.com/privacy-certification-standards/ (last visited Oct. 27, 2016).

32. S. Shyam Sundar et al., *Unlocking the Privacy Paradox: Do Cognitive Heuristics Hold the Key?*, *in* CHI 2013: EXTENDED ABSTRACTS ON HUMAN FACTORS IN COMPUTING SYSTEMS 811, 815-16 (2013), http://doi.acm.org/10.1145/2468356.2468501 (last visited Feb. 13, 2016).

33. *Id.* at 812; *see also* Mary J. Culnan, *Protecting Privacy Online: Is Self-Regulation Working?*, 19 J. PUB. POL'Y & MARKETING 20, 20 (2000); George R. Milne & Mary Ellen Gordon, *Direct Mail Privacy-Efficiency Trade-offs Within an Implied Social Contract Framework*, 12 J. PUB. POL'Y & MARKETING 206, 207-08 (1993).

34. Sundar et al., *supra* note 32, at 812.

35. *See* Sandra Petronio, *Communication Privacy Management Theory: What Do We Know About Family Privacy Regulation?*, 2 J. FAM. THEORY & REV. 175, 178-82 (2010) [hereinafter Petronio, *Family Privacy Regulation*]; *see also* SANDRA PETRONIO, BOUNDARIES OF PRIVACY: DIALECTICS OF DISCLOSURE 1-36 (2002) (describing privacy and disclosure as being in constant dialogue); Sandra Petronio & Wesley T. Durham, *Communication Privacy Management Theory: Significance for Interpersonal Communication*, *in* ENGAGING THEORIES IN INTERPERSONAL COMMUNICATION: MULTIPLE PERSPECTIVES 309-22 (Leslie A. Baxter & Dawn O. Braithwaite eds., 2008) (positioning CPM as a communication theory because of the centrality of the communication process in decision-making about disclosure).

36. Petronio, *Family Privacy Regulation*, *supra* note 35, at 178.

37. *See* Milne & Culnan, *supra* note 30, at 15; Carlos Jensen & Colin Potts, *Privacy Policies as Decision-making Tools: An Evaluation of Online Privacy Notices*, *in* CHI 2004: PROCEEDINGS OF THE SIGCHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS 471 (2004).

companies make in their privacy policies.[38] The FTC began enforcing privacy policies in the late-1990s[39] under its power to regulate unfair and deceptive trade practices.[40] The FTC took a particular interest in actively protecting online privacy after it found that industry self-regulation had been unsuccessful.[41] Of great focus in its enforcement regime was the concern about websites that failed to live up to the representations made in their privacy policies.[42] Importantly, the FTC's mission has shifted from strictly enforcing privacy promises, to enforcing "broken expectations of consumer privacy."[43]

The agency's unfairness and deception enforcement actions amount to guidelines on how the FTC will act in situations in which it deems an organization's data collection and protection schemes seem to run afoul of its privacy promises.[44] Some scholars have even argued that the FTC jurisprudence on this matter has created a de facto common law of privacy.[45] Nonetheless, the FTC is working hard to protect consumer privacy while at the same time staying within the bounds of its Congressional grant of power.

The FTC outlined its enforcement policy with respect to deceptive practices in a letter appended to its ruling in *Cliffdale Associates, Inc.*[46] In the letter, the FTC constructed its perspective on deception based upon a synthesis of its decisions in previous deceptive practice cases.[47] As noted earlier, the FTC's policy statement states that for a statement or practice to be considered deceptive, the statement or practice must both be material and likely to mislead a consumer acting reasonably under the circumstances.[48] Material statements were those that affected, or were likely to influence, the consumer's decision of whether or not to purchase

---

38. *Enforcing Privacy Promises*, FED. TRADE COMMISSION, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/enforcing-privacy-promises (last visited Oct. 27, 2016).

39. *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 599 (2014).

40. Michael D. Scott, *The FTC, the Unfairness Doctrine, and Data Security Breach Litigation: Has the Commission Gone Too Far?*, 60 ADMIN. L. REV. 127, 129 (2008).

41. *Id.* at 130.

42. *Id.* at 130-34. The enforcement of privacy promises within a company's privacy policy itself is not the focus of this Article. Instead, this Article focuses on the claims made in various technologies' marketing and advertising materials because these, too, affect a consumer's reasonable expectation of privacy.

43. *Id.* at 167.

44. Solove & Hartzog, *supra* note 39, at 600.

45. *Id.* at 586; *but see* Justin Hurwitz, *Data Security and the FTC's UnCommon Law*, 101 IOWA L. REV. 955, 955 (2016).

46. *See* Cliffdale Assocs., Inc., 103 F.T.C. 110, 174-84 (1984).

47. *Id.* at 175.

48. *Id.*

the good or service.[49] Practices found to be deceptive included false and misleading claims, failure to perform promised services, and the sale "of hazardous or systematically defective products or services without adequate disclosures."[50] The FTC's conception of the reasonable person illustrates the significance the Commission places on the sophistication of the consumer in examining whether advertising claims could be misleading.

A. The Reasonable Consumer

The FTC summarized that a reasonable consumer is a person who acts reasonably under the circumstances.[51] The FTC will likely not find deception if a claim or practice was misunderstood only by the most sensitive or ignorant consumers.[52] In *Heinz W. Kirchner* the FTC stated:

> Some people, because of ignorance or incomprehension, may be misled by even a scrupulously honest claim. Perhaps a few misguided souls believe, for example, that all "Danish pastry" is made in Denmark. Is it, therefore, an actionable deception to advertise "Danish pastry" when it is made in this country? Of course not. A representation does not become "false and deceptive" merely because it will be unreasonably misunderstood by an insignificant and unrepresentative segment of the class of persons to whom the representation is addressed.[53]

The *Heinz* quotation highlights the two standards that the FTC takes into account when evaluating whether or not the consumer was acting reasonably under the circumstances. First, the quotation illustrates how the FTC takes into account multiple interpretations of a statement (or an omitted a statement) in its analysis. As noted above, the FTC will not hold companies liable for consumers' errant interpretations.[54] Companies are not responsible for consumers who believe baked goods named for their country of origin will have actually been imported from that country. At the same time, the FTC recognizes that more than one message can be conveyed in an advertisement, and that one of those

---

49. *Id.* at 175-76.
50. *Id.* at 175.
51. *Id.*
52. *Id.* at 178.
53. Heinz W. Kirchner, 63 F.T.C. 1282, 1290 (1963).
54. *Cliffdale*, 103 F.T.C. at 178 (citing Jay Norris Corp., 91 F.T.C. 751, 836 (1978), *aff'd*, 598 F.2d 1244 (2d Cir. 1979)) ("A company is not liable for every interpretation or action by a consumer. . . . An interpretation will be presumed reasonable if it is the one the respondent intended to convey.").

messages can be considered deceptive even if that message was not the primary message.[55]

Second, although the Commission in *Heinz* identifies a certain kind of consumer, the ignorant consumer, it also must identify the kind of consumer who is the model of reasonableness. According to the FTC, the reasonable consumer is the "average" consumer, or an individual behaving in the manner that most others in the same situation would behave.[56] This "average consumer" standard was employed in a famous case brought against the makers of Listerine.[57] In *Warner-Lambert v. Federal Trade Commission* (a case affirmed by the United States Court of Appeals for the District of Columbia) the FTC brought an action against the company based on its claims that the mouthwash prevented, cured, or alleviated symptoms of the common cold.[58] In evaluating this claim, the FTC considered whether the statements deceived the "average listener" hearing the advertisement,[59] and found that even after Warner-Lambert had stopped using advertisements with the cold-curing claims, a significant portion of the public continued to believe in the efficacy of Listerine as an illness fighter.[60]

B. Special Categories of Audiences

The "reasonableness" inquiry applied to statements directed at special categories of audiences is different from the inquiry when applied to statements directed to general consumers. Although the FTC's deceptiveness analysis usually focuses on whether a consumer (without regard to ignorant consumers) acted reasonably under the circumstances, the FTC may assess "reasonableness" according to what is "reasonable" for a particular group (if those statements are directed at that particular audience).[61] These particular audiences include groups whom the FTC has deemed particularly susceptible to certain deceptive advertising and trade practices or particularly knowledgeable about the advertised or marketed product's subject area.[62]

For instance, when advertisements or trade practices are directed at children, the FTC evaluates "reasonableness" by how a reasonable child

---

55. *Id.*
56. *See* Warner-Lambert Co., 86 F.T.C. 1398, 1415 n.4 (1975), *aff'd*, 562 F.2d 749 (D.C. Cir. 1977), *cert. denied*, 435 U.S. 950 (1978).
57. *See id.*
58. *Id.* at 1398-1401.
59. *Id.* at 1415 n.4. The FTC did not, however, define the "average listener." *See id.*
60. *Id.* at 1415.
61. Cliffdale Assocs., Inc., 103 F.T.C. 110, 177-78 (1984).
62. *Id.* at 179.

would interpret the company's claims.[63] In *Ideal Toy*, the FTC stated that children were a group "unqualified by age or experience to anticipate or appreciate the possibility that the representations may be exaggerated or untrue."[64] In this case, the FTC issued a formal complaint against a toy maker whose television advertisement depicted its products moving automatically when, in fact, the toys required the user to manually adjust its settings.[65] The FTC thought children would be unable to differentiate between the actual capabilities of a product and the exaggerations or outright misrepresentations made by the manufacturer.[66]

Similarly the FTC evaluates advertisements aimed at the elderly and terminally ill with regard to how a reasonable person in that group would interpret the ads.[67] Advertisements aimed at these audiences usually appeal to the survival needs of these groups,[68] and the FTC aggressively prosecutes deceptive claims and practices. In a recent example of its aggressive prosecution, the FTC issued an action against a telemarketing company that preyed on the fears of elderly people in New York.[69] The company in question had been marketing medical alert services to elderly people.[70] The marketer, in some cases, claimed that the individual had already signed up for the service in order to deceive senior citizens into making payments.[71]

Elderly people are particularly susceptible to false or deceptive claims marketing health and wellness products.[72] Many times, elderly people suffer from some form of illness or injury. Likewise, those

---

63. *Id.*

64. Ideal Toy Corp., 64 F.T.C. 297, 299 (1964); *see also* Rainbow Crafts, Inc., 66 F.T.C 655, 657 (1964); Am. Doll & Toy Corp., 66 F.T.C. 658, 661 (1964); Lucky Prods., Inc., 63 F.T.C. 1039, 1043 (1963); Remco Indus., Inc., 61 F.T.C. 310, 313 (1962).

65. *Ideal Toy*, 64 F.T.C. at 299.

66. *See id.*

67. *Cliffdale*, 103 F.T.C. at 179.

68. *See, e.g.*, Carolyn Bonifield & Catherine Cole, *Advertising to Vulnerable Segments*, *in* THE SAGE HANDBOOK OF ADVERTISING 430-44 (Gerard J. Tellis & Tim Ambler eds., 2007) (finding that older adults' feelings of helplessness may increase with physical disabilities, making them less likely to use their persuasion knowledge); *cf.* Suzeanne Benet et al., *The Appropriateness of Fear Appeal Use for Health Care Marketing to the Elderly: Is It OK To Scare Granny?*, 12 J. BUS. ETHICS 45 (1993).

69. Compl. for Permanent Inj. & Other Equitable Relief at *4, Fed. Trade Comm'n v. Instant Response Sys., LLC, No. 13 Civ. 00976(ILG) (VMS), 2015 WL 1650194, *1-3 (E.D.N.Y. Feb. 25, 2013); *see also* Press Release, Fed. Trade Comm'n, FTC Action Halts Brooklyn Company from Using Deception, Threats, and Intimidation to Trick Elderly Consumers in to Paying for Unordered Medical Alert Devices (March 8, 2013) (on file with author).

70. *See* Compl. for Permanent Inj. & Other Equitable Relief, *supra* note 69, at *4.

71. *See* Fed. Trade Comm'n v. Instant Response Sys., LLC, No. 13 Civ. 00976(ILG) (VMS), 2015 WL 1650194, at *4 (E.D.N.Y. Apr. 14, 2015).

72. Bonifield & Cole, *supra* note 68, at 434.

terminally ill may be susceptible to claims about products that may cure or alleviate their symptoms.[73]

Essentially, the FTC requires marketers targeting all three special audience categories mentioned above to be especially conscious of the claims they make in advertisements. In the same vein, the FTC does not, however, require marketers targeting professional groups (groups with a specific kind of training) to be wary of those not in their target groups misinterpreting their statements or practices.[74] For example, a company targeting those in the medical profession (by using terminology with a specific connotation to those in the medical field) would not need to worry about the FTC finding the statements deceptive on the grounds that the general audience might interpret the statements differently than as intended. This is because the FTC would consider who a "reasonable person" is with regard to the specific medical field targeted by the advertisement or practice, and not the general public.

The three special interest categories mentioned above are not the only groups of people of particular interest to the FTC. In fact, in its statement on deceptive practices, the agency noted, "[t]he listed categories are merely examples. Whether children, terminally ill patients, or any other subgroup of the population will be considered a special audience depends on the specific factual context of the claim or the practice."[75] An opportunity exists, then, for the FTC to formally recognize privacy-promising technology users as a special category of audience and to apply a heightened form of scrutiny when assessing the statements directed at them.

C. The Significance of Audience Sophistication

If the FTC recognizes privacy-promising technology users as a special category of audience, the sophistication of that audience is, perhaps, the most important consideration in determining the type of scrutiny afforded to that group. This is because the FTC is more likely to

---

73. *See* Cliffdale Assocs., Inc., 103 F.T.C. 110, 179 n.30 (1984) (quoting Travel King, 86 F.T.C. 715, 719 (1975))

> According to the complaint, the frustrations and hopes of the seriously ill and their families were exploited, and the representation had the tendency and capacity to induce the seriously ill to forego conventional medical treatment worsening their condition and in some cases hastening death, or to cause them to spend large amounts of money and to undergo the inconvenience of traveling for a non-existent "operation."

Id.

74. *See id.* at 179.

75. *Id.* at 179 n.29.

use a different standard of reasonableness when claims target groups with low levels of audience sophistication.[76]

In general, the United States Supreme Court has supported the use of different standards of scrutiny for certain groups.[77] In *Bates v. State Bar of Arizona*, which held that attorneys had a right under the First Amendment to advertise their services, the Court noted that "[t]he determination whether an advertisement is misleading requires consideration of the legal sophistication of its audience. Thus, different degrees of regulation may be appropriate in different areas."[78] The Court appears to recognize that there may be certain groups that may need a different standard, or level, of protection based upon how ignorant of the subject matter of the marketer's claims those individuals are.

Prior to adopting the current standard it uses to review alleged deceptive practices, the FTC used a different test to gauge audience reaction or sophistication: the "substantial percentage" test.[79] Before 1983, the FTC considered the reactions of a targeted group of the audience pool, and then analyzed whether a "substantial number" of members in that target group would be deceived by the company's representations or omissions.[80] This "substantial percentage" test was vague, as the FTC did not establish a bright-line rule with regard to the number of affected members it would consider "substantial."[81]

For example, the amorphousness of the test resulted in the United States Court of Appeals for the Seventh Circuit ruling in *Aronberg v. Federal Trade Commission* that the advertisements in question were deceptive.[82] *Aronberg* involved the enforcement of a deceptive practice action against a pharmaceutical manufacturer who claimed that its line of medicine would induce menstruation in women whose periods were late.[83] In reality, the medicine contained harmful chemicals that had toxic

---

76. *Id.* at 179.

77. *See* Bates v. State Bar of Ariz., 433 U.S. 350, 384 (1977).

78. *Id.* at 383 n.37 (citation omitted).

79. Karns, *supra* note 9, at 405-06. The test was also referred to as the "substantial portion" test, see Exposition Press, Inc. v. Fed. Trade Comm'n, 295 F.2d 869, 872 (2d Cir. 1961), and the "substantial segment" test, see Statement of Basis and Purpose of Trade Regulation Rule: Unfair or Deceptive Advertising and Labeling of Cigarettes in Relation to the Health Hazards of Smoking, 29 Fed. Reg. 8325, 8350 (1964).

80. Karns, *supra* note 9, at 405 (quoting Bristol-Myers Co., 85 F.T.C. 688, 744 (1975)).

81. *Id.*

82. *Id.* at 406.

83. Aronberg v. Fed. Trade Comm'n, 132 F.2d 165, 166 (7th Cir. 1942). The advertisements asserted, for example, "[d]on't be alarmed over delayed, overdue, unnaturally suppressed periods," "[t]housands of women are needlessly miserable and unhappy because of abnormally delayed periods," and "[f]or countless women such unnatural interruption is often needless." *Id.* at 168.

effects on the blood-circulation, digestive, and reproductive systems.[84] The court held that the statements were "deceiving to a substantial portion of the public . . . the vast multitude which includes the ignorant, the unthinking and the credulous."[85] In its opinion, the court noted that the general public was not well-informed about medical technology[86] and the audience targeted by the pill advertisements was made up of people who were anything but analytical readers.[87] Nevertheless, these were the people that the law was created to protect. The court emphasized that while "the buying public does not ordinarily carefully study or weigh each word in an advertisement,"[88] "[a]dvertisements are intended not 'to be carefully dissected with a dictionary at hand, but rather to produce an impression upon' prospective purchasers."[89] Thus, the court found it necessary for the FTC to act under its regulatory power to protect prospective purchasers from possible injury.[90]

Currently the FTC assesses reasonableness based on the net impression of the entire advertisement or practice.[91] Therefore, the claims within an ad will be evaluated in context. At the same time, the Commission recognizes that consumers may not view the entire ad and all of the disclosures or disclaimers included.[92] The recognition of the importance of the level of sophistication of the target audience, and the fact that the sophistication of the audience can be generally inferred instead of empirically proven, therefore, appears to allow the FTC to apply a heightened standard of scrutiny with respect to claims made by privacy-promising technologies.

Moreover, the FTC's guidelines for endorsements also indicate that the FTC is concerned with audience members' sophistication—or ability to recognize sponsored claims. Advertisers use endorsements to "enhance the distinctiveness and memorability of their messages:"[93] the

84. *Id.* at 169.
85. *Id.* at 167-69.
86. *Id.* at 168.
87. *Id.*
88. *Id.*
89. *Id.* (quoting Newton Tea & Spice Co. v. United States, 288 F. 475, 479 (6th Cir. 1923)).
90. *Id.* at 167.
91. Cliffdale Assocs., Inc., 103 F.T.C. 110, 179 (1984).
92. FED. TRADE COMM'N, .COM DISCLOSURES: HOW TO MAKE EFFECTIVE DISCLOSURES IN DIGITAL ADVERTISING 6 (2013). *See also* Linda J. Demaine, *Seeing Is Deceiving: The Tacit Deregulation of Deceptive Advertising*, 54 ARIZ. L. REV. 719, 744 (2012) (finding that a misplaced regulatory emphasis on advertisers' linguistic claims has resulted in more deceptive ads being subject to less regulation).
93. Consuelo Luada Kertz & Roobina Ohanian, *Source Credibility, Legal Liability, and the Law of Endorsements*, 11 J. PUB. POL'Y & MARKETING 12, 13 (1992).

connection of a product to a well-known personality improves brand recognition[94] and associates a product or service with particular values.[95] At the same time, consumers use endorsements from celebrities, groups, and popular personalities as shortcuts to decide whether to purchase a product or service.[96] Of course, endorsements are not the sole factor in a consumer's decision to purchase a product or service. Generally, consumers make choices related to endorsements based on the strength of ties between a product and the figure offering the endorsement.[97] The strength of the tie is based on "(1) trustworthiness or credibility of the celebrity, (2) likeability of the celebrity, (3) similarity between the celebrity and the target audience, and (4) expertise of the celebrity in the subject matter of the product."[98]

Much the same way consumers rely on celebrity endorsements, consumers appear to use privacy policies as a heuristic when deciding whether or not to use a website or app. Similar to the way consumers subconsciously contemplate the strength of the tie between the celebrity endorsement and the product when making purchasing choices, consumers conduct a privacy calculus (as offered by the CPM theory) in their decisions to purchase or use privacy-promising technologies.

The next Part provides an overview of the literature on digital and information literacy. It also synthesizes the literature on studies relating to consumers and privacy in digital spaces, including social media. It argues that the current literature demonstrates the need for a more exacting standard for the advertising and marketing practices related to digital privacy and privacy-promising technologies.

III. A DEFICIENCY IN CONSUMER INFORMATION LITERACY

In their 1890 *Harvard Law Review* article, Samuel Warren and later-Supreme Court Justice Louis Brandeis observed that new technologies could cause what was once whispered behind closed doors to one day be exposed to the public.[99] Though not originally conceived as a worry focused on governmental regulations on violations of consumer

94. *See id.*
95. *Id.*
96. *See id.* at 12.
97. *See id.*
98. Leah W. Feinman, *Celebrity Endorsements in Non-Traditional Advertising: How the FTC Regulations Fail To Keep Up with the Kardashians*, 22 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 96, 101 (2011).
99. Samuel D. Warren & Louis D. Brandeis, *Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890).

privacy,[100] the jurists' concerns about surveillance foreshadowed consumer advocates' concerns about maintaining privacy in face of the growing number of advertisers, apps, and online retailers who gather consumer data to deliver more relevant messages to their consumers.[101]

Apps such as Snapchat may metaphorically replace Warren and Brandeis' "closed doors" as senders of a "snap" may unwittingly be exposing themselves, quite literally, to "prying ears" other than those of the intended receiver. Privacy concerns are apparent when there is a possibility that snaps can be captured permanently, in direct opposition to the marketed purpose of the app. Yet, app users may be unconcerned about threats to their privacy when marketing promises are unfulfilled.[102] Many apps collecting user data have terms of agreement containing legalese (essentially privacy promises) that pop up just before a consumer downloads or uses an app.[103] Even though the FTC settled with Snapchat over its deceptive messaging one issue remains: current consumer motivation to pay attention to app privacy policies, online behavioral advertising, and other privacy-promising situations in the digital context is very low.

A. Actual Consumer Privacy Behavior Online

What does the reasonable person pay attention to, as far as privacy policies go, in the online context? The preponderance of the research suggests not much, if anything at all.[104] However, the issue of privacy in the realm of online data collection continues to appear in the media and spark debates among consumer advocates and regulators alike.[105] Studies

---

100. *Id.* Instead, Warren and Brandeis focused on the press and its use of the new technology of the day. *Id.*

101. Heather Shoenberger & Esther Thorson, Prediction of Perceived Online Shopping Benefits and Risks from Trust and Knowledge of Targeting, Presented Before the American Academy of Advertising Conference 155, 155 (2014).

102. *See* Roesner et al., *supra* note 12, at 64-76.

103. *See* Susan E. Gindin, *Nobody Reads Your Privacy Policy or Online Contract? Lessons Learned and Questions Raised by the FTC's Action Against Sears*, 8 NW. J. TECH. & INTELL. PROP. 1 (2009) (examining the FTC's final consent order in its action against Sears for tracking customers without providing proper notice).

104. *See, e.g.*, WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY 108 (2012) [hereinafter CONSUMER DATA PRIVACY]; *see also* Shoenberger & Thorson, *supra* note 101, at 155; Aleecia M. McDonald & Lorrie Faith Cranor, *Americans' Attitudes About Internet Behavioral Advertising Practices*, *in* PROCEEDINGS OF THE 9TH ANNUAL ACM WORKSHOP ON PRIVACY IN THE ELECTRONIC SOCIETY 63 (2010); Joseph Turow et al., Americans Reject Tailored Advertising and Three Activities that Enable It, 20-21 (Sept. 29, 2009) (on file with the University of Pennsylvania Scholarly Commons).

105. David E. Sanger & Steve Lohr, *Call for Limits on Web Data of Customers*, N.Y. TIMES, May 1, 2014, at A1.

have even noted that media may have influenced consumer behavior in this respect.[106] However, news coverage on its own—including a series entitled "What They Know" run by the *Wall Street Journal* from 2010 to 2012[107]—has not motivated consumers to pay attention to privacy policies, let alone motivated consumers to opt-out of websites tracking of clickstream.[108]

In fact, while research suggests that consumers want more privacy protections online,[109] according to a recent White House report, consumers may not always make the best initial decision about their privacy when creating a relationship with social media sites.[110] Additionally, consumers rarely take actions to control their data.[111] This research calls into question whether the current opt-out system and privacy settings and policies offered by companies are effective at ensuring consumers have adequate control over their data.[112] As such the FTC proposed that "[e]very Web site where data is collected for behavioral advertising should provide a clear, consumer-friendly, and prominent statement that data is being collected to provide ads targeted to the consumer and give consumers the ability to choose whether or not to have their information collected for such purpose."[113]

One such mechanism adopted by websites is the privacy seal. Websites that generate advertisements through consumer online behavior data or collect consumer data for advertising purposes may include privacy seal logos on such advertisements.[114] These regulatory logos are based off FTC's requirement that consumers should be given notice of the site's data practices and position that consumer control over data is a

---

106. *See* Amit Poddar, Jill Mosteller & Pam Scholder Ellen, *Consumers' Rules of Engagement in Online Information Exchanges*, 43 J. CONSUMER AFF. 419, 419-48 (2009).

107. *See, e.g.*, Julia Angwin, *The Web's New Gold Mine: Your Secrets*, WALL ST. J. (June 30, 2010), http://www.wsj.com/news/articles/SB10001424052748703940904575395073512989404.

108. See Poddar et al., *supra* note 106 (finding that although media coverage of privacy issues would be thought to create awareness among consumers, it was not found to be most influential for behavioral responses).

109. McDonald & Cranor, *supra* note 104, at 71 (finding in a survey of Internet users that more privacy protections would entice more online purchases); *see* Turow et al., *supra* note 104, at 20-21 (finding most consumers surveyed would not want tailored advertising).

110. *See* CONSUMER DATA PRIVACY, *supra* note 104, at 107-08.

111. *See* Adam N. Joinson et al., *Privacy, Trust, and Self-Disclosure Online*, 25 HUM.-COMPUTER INTERACTION 1, 3 (2010); *but see* Miriam J. Metzger, *Communication Privacy Management in Electronic Commerce*, 12 J. COMPUTER-MEDIATED COMM. 335 (2007).

112. *See* CONSUMER DATA PRIVACY, *supra* note 104, at 106.

113. Press Release, Fed. Trade Comm'n, FTC Staff Proposes Online Behavioral Advertising Privacy Principles (Dec. 20, 2007) (on file with author).

114. Kim Bartel Sheehan & Mariea Grubbs Hoy, *Dimensions of Privacy Concern Among Online Consumers*, 19 J. PUB. POL'Y MARKETING 62, 70-73 (2000).

feature of privacy.[115] As such, the icons and the terms of use offered by apps in the digital context when clicked, typically offer information about how to opt-out of targeted advertising services, how the advertisements are generated or how the data will be used within an app.[116] Warning labels have also been used to offer consumers the chance to make informed decisions about purchase and usage of products, an activity considered inseparable from a free-market system.[117]

One pitfall of privacy seals, however, is that they have often been used by consumers, not as a gateway to more information, but as a heuristic for safety.[118] The mere presence of a readily visible privacy policy on a website may be enough to increase consumer trust in the site regardless of the content of the policy.[119] The Digital Advertising Alliance's (DAA's) use of the AdChoices icon—which allows Internet users to opt out of receiving a specific targeted ad—has been shown to cause an increase in the number of people who actually click on the ad.[120] The reason behind this click-thru rate increase is not likely due to comprehension of or agreement with the website's privacy policy and data use promises. The survey results do not mention the number of people who actually read and understood the privacy policy offered by the DAA;[121] however, previous research has noted that few consumers read privacy policies or choose to opt-out.[122] Indeed, in one survey conducted by DAA, over half of the respondents said they would be more likely to click on an ad displaying the icon.[123] At the same time, approximately 73% said they would be more comfortable with the

115. *Id.* at 70. *See, e.g.*, Financial Privacy Rule, 16 C.F.R. § 313 (2000).

116. Alan R. Peslak, *Internet Privacy Policies of the Largest International Companies*, 4 J. ELECTRONIC COM. ORGS. 46 (2006) (reviewing the privacy policies of companies listed on the Forbs International 100).

117. *See* Eli P. Cox III et al., *Do Product Warnings Increase Safe Behavior? A Meta-Analysis*, 16 J. PUB. POL'Y MARKETING 195, 195 (1997). Studies on the effectiveness of warning labels have, however, been inconsistent. *Id.*

118. Robert Larose & Nora J. Rifon, *Promoting i-Safety: Effects of Privacy Warnings and Privacy Seals on Risk Assessment and Online Privacy Behavior*, 41 J. CONSUMER AFF. 127, 130 (2007).

119. *See* Yue Pan & George M. Zinkhan, *Exploring the Impact of Online Privacy Disclosures on Consumer Trust*, 82 J. RETAILING 331, 336-37 (2006).

120. Katy Bachman, *Users More Likely To Click on Ads with AdChoices Icon*, ADWEEK (Nov. 5, 2013, 10:27 AM), http://www.adweek.com/news/technology/users-more-likely-click-ads-adchoices-icon-153617.

121. *Id.*

122. *See* Jeff Langenderfer & Anthony D. Miyazaki, *Privacy in the Information Economy*, 43 J. CONSUMER AFF. 380, 382 (2009).

123. *Id.*

targeted ads if they knew the privacy policies behind the DAA's self-regulatory program.[124]

B. Consumer Digital Literacy

The consumer's active role in the protection of his or her data in the online context is a key consideration weighing in favor of the FTC adopting a heightened form of scrutiny for the claims involving privacy-promising technology. Control of where and how an individual's data are used is an essential concept to online consumer privacy. Consumer advocates have pushed for increased consumer knowledge or literacy in this area.[125] Consumer advocates believe that if a consumer knows more about how his or her data are used online, he or she will be more apt to exercise control over that data.[126] While this assumption seems intuitive, actual knowledge is, at best, a weak predictor of whether or not a consumer has privacy concerns.[127] In fact, even in other instances of rapid technological advancement, knowledge of the intricacies of a new technology is typically a weak predictor of concern about or support for the new technology.[128]

Different types of information may be considered more important to keep private than others. For example, consumers may be more likely to be worried about financial or medical information being collected.[129] Also, it is likely that the idea of other people looking at information collected would be considered more of an invasion of privacy than an algorithm putting together information using unidentified online behavioral data—but again, knowledge of this data aggregation seems to

---

124. *Id.*

125. Dustin D. Berger, *Balancing Consumer Privacy with Behavior Targeting*, 27 SANTA CLARA COMP. & HIGH TECH. L.J. 3, 6 (2010) (arguing for an increase in mandatory regulation and audit requirements to address privacy issues in behavioral advertising).

126. *See* Ellen R. Foxman & Paula Kilcoyne, *Information Technology, Marketing Practice, and Consumer Privacy: Ethical Issues*, 12 J. PUB. POL'Y & MARKETING 106, 117-18 (1993).

127. *See* Edith G. Smit, Guda Van Noort & Hilde A.M. Voorveld, *Understanding Online Behavioural Advertising: User Knowledge, Privacy Concerns and Online Coping Behaviour in Europe*, 32 COMPUTERS HUM. BEHAV. 15, 21 (2014); Shoenberger & Thorson, *supra* note 101, at 158-59; McDonald and Cranor, *supra* note 104, at 71.

128. *See, e.g.*, Dominique Brossard et al., *Religiosity as a Perceptual Filter: Examining Processes of Opinion Formation About Nanotechnology*, 18 PUB. UNDERSTANDING SCI. 546, 555-56 (2009) (finding that knowledge about new technology was mediated by religious beliefs).

129. Glen J. Nowak & Joseph Phelps, *Understanding Privacy Concerns: An Assessment of Consumers' Information-Related Knowledge and Beliefs*, 6 J. DIRECT MARKETING 28, 36 (1992).

have no effect on behavior.[130] A survey conducted about Snapchat illustrates this argument: approximately 79% of people asked about the app knew or thought it was possible for snaps to be captured, slightly more than 52% of those surveyed noted that they did not care.[131]

IV. SOLUTIONS FOR THE FUTURE

A. Heightened Standard of Review

In light of the seemingly naïve or lackadaisical attitude that consumers display toward their online privacy, what should the FTC do, if anything, in an attempt to offer protection? This Part argues that the FTC should create a heightened standard of review for claims promising consumer privacy or data control. This heightened standard of review would take into account who is a "reasonable person" specifically within the digital context. The majority of consumers occupying the digital space are not, as aforementioned research indicates, ignorant consumers. This begs the question as to what type of behavior in the digital context is reasonable.

An average consumer in the digital context is bombarded with all kinds of media.[132] The average consumer is unlikely to click on privacy information or pay attention to privacy promises, even when they know there may be consequences (e.g., Snapchat pictures being saved).[133] They might rely on the presence of a policy or a safety seal as a heuristic denoting safety.[134] They may also want so much to be included in activities of their peers that they download, join, or click on apps and websites merely to belong.[135] The average person in the digital context is not, however, one who exercises control over his or her data or is

---

130. *See* George R. Milne & Andrew J. Rohm, *Consumer Privacy and Name Removal Across Direct Marketing Channels: Exploring Opt-In and Opt-Out Alternatives*, 19 J. PUB. POL'Y & MARKETING 345 (2002) (finding that of survey respondents indicating knowledge of name removal capabilities, only a small proportion would want their personal information removed all from advertiser lists).

131. *See* Roesner et al., *supra* note 12, at 64.

132. *See* ROBERT HASSAN, THE INFORMATION SOCIETY: CYBER DREAMS AND DIGITAL NIGHTMARES xii (2008) (describing the volume of information produced each day); Peter J. Denning, *Infoglut*, COMM. ACM, July 2006, at 15 (describing the exponential growth in information individuals receive).

133. *See* Joinson et al., *supra* note 111.

134. *See* Sundar et al., *supra* note 32.

135. *See, e.g.*, Xia Wang, Chunling Yu, & Yujie Wei, *Social Media Peer Communication and Impacts on Purchase Intentions: A Consumer Socialization Framework*, 26 J. INTERACTIVE MARKETING 198 (2012) (finding that online peer communication influenced purchasing decisions).

motivated to so.[136] While this Article does not address, with empirical evidence, the peer-driven social norms that appear to more strongly encourage the trust of the Internet than offline social norms do,[137] it suggests that the reasonable person in the digital context is quite different than the reasonable person in the offline context.

It is tempting to generalize online and offline behaviors and it is tempting to assume that they are mirrors of each other when in reality they are not. Consumers in the offline world interact with other human beings and physically put pen to paper (a motion that requires a more conscious attention than that of clicking through privacy policies to get to an app of interest). In the digital context, consumers often feel not only anonymous, but also compelled to abide a different set of social norms.[138] Legal scholars have noted that consumers confronted with online click wrap agreements behave differently than those offered contracts in the brick and mortar world.[139] Scholars have also noted that consumers have less bargaining power in the digital context.[140]

This line of reasoning notes the importance of signals that indicate to consumers that a piece of information is important, such as large and bold printed warnings.[141] As noted with the use of signals studied in the social sciences, warning labels and signals tend to merely serve as heuristics denoting safety or the assumption of safety and do little to further inform or empower a consumer in the digital context.[142]

Thus, both in terms of consenting to data collection and actual data collection, it appears that consumers in the digital context operate differently; consumers are likely to use heuristics such as safety seals to guide their navigation habits and unlikely to participate in conscious risk/benefit analyses about their privacy concerns over privacy-promising technologies.[143]

---

136. *See* CONSUMER DATA PRIVACY, *supra* note 104, at 107-08.

137. *See, e.g.*, Sebastián Valenzuela, Namsu Park & Kerk F. Kee, *Is There Social Capital in a Social Network Site?: Facebook Use and College Students' Life Satisfaction, Trust, and Participation*, 14 J. COMPUTER-MEDIATED COMM. 875 (2009) (finding relationships between the social media site and various aspects of students' lives).

138. *See, e.g.*, Charla Mathwick, *Understanding the Online Consumer: A Typology of Online Relational Norms and Behavior*, 16 J. INTERACTIVE MARKETING 40 (2002) (identifying four different types of online consumers).

139. Juliet M. Moringiello, *Signals, Assent and Internet Contracting*, 57 RUTGERS L. REV. 1307, 1309, 1340-46 (2005).

140. *Id.* at 1343.

141. *See id.* at 1315.

142. *Id.*

143. *See* Pan & Zinkhan, *supra* note 119, at 336-37; Bachman, *supra* note 120 (reporting that transparency and choice influenced consumer response to targeted ads).

These mental short-cuts are created from assumptions based on past experience;[144] thus, a person may gravitate toward apps his or her peers already have downloaded assuming it is safe or gravitate to a website with a privacy policy link under the assumption that the site is safe. This shift in perspective, then, reflects the value of taking the consumer as he or she is, which according to the ruling in *Aronberg*, is an individual that does not partake in a critical analysis of the statements made in marketing campaigns.[145]

When businesses make statements specifically promising privacy related to the use of its technology, whether apps, social media, email, etc., the FTC should take a more aggressive approach to protecting consumer privacy by heightening the standard of review for privacy protection claims. Such measures would recognize that consumer online decision-making is mediated by many things which may influence a user's assumptions about privacy-promising claims. To be sure, this standard should only apply to those technologies, like Snapchat, that use privacy or data control to encourage the use of their product or service. This does not include the claims in privacy policies, or other terms of service that are already subject to FTC regulation—although those claims should not be considered insignificant.[146]

B. Industry Guides for Privacy-Promising Technology

If the FTC were to consider the social science literature and theories, like those noted above, "it could increasingly demand that companies engage in practices that will correct mistaken consumer assumptions, or at the very least not exploit such assumptions."[147] However, the FTC has not yet completely taken this step.[148] The FTC could use its regulatory tools to protect consumers from deceptive privacy claims and to make the promises offered by technologies in this context more transparent by creating guidelines for companies creating and advertising privacy-promising technologies. The FTC's industry guides are one of two ways the FTC uses public participation to assist with the promulgation of rules.[149] The power to create guides is derived from 16 C.F.R. § 1.5, which states:

---

144. *See* Sundar et al., *supra* note 32.
145. *See* Aronberg v. Fed. Trade Comm'n, 132 F.2d 165, 168 (7th Cir. 1942).
146. *See id.* at 667-76.
147. Solove & Hartzog, *supra* note 39, at 667.
148. *See id.*
149. Charles H. Koch Jr. & Beth Martin, *FTC Rulemaking Through Negotiation*, 61 U.N.C. L. REV. 275, 280 (1982).

> Industry guides are administrative interpretations of laws administered by the Commission for the guidance of the public in conducting its affairs in conformity with legal requirements. They provide the basis for voluntary and simultaneous abandonment of unlawful practices by members of industry. Failure to comply with the guides may result in corrective action by the FTC under applicable statutory provisions. Guides may relate to a practice common to many industries or to specific practices of a particular industry.[150]

The FTC has, for example, created industry guides for industries that market alcohol, funerals, and jewelry.[151] The FTC also offers guidance for organizations on consumer privacy.[152]

In fact in 2013, the FTC published a guide for creators of apps.[153] This guide offered suggestions to app makers on how to insure that their practices comply with basic FTC consumer regulations on privacy and truthful advertising.[154] Three of the important suggestions were that businesses "[t]ell the truth about what your app can do," "[b]uild privacy considerations in from the start," and "[h]onor your privacy promises."[155]

In explaining these three suggestions, the FTC appears to recognize that the onus is on the business organization to make clear to consumers what they can actually expect from their apps. Two of these three suggestions provide an adequate jumping off point from which the FTC can craft an industry guide for the creators of privacy-promising technologies.

First the FTC advises app makers to "tell the truth."[156] In this suggestion, the FTC details its expectation that developers follow a "truth in advertising approach" when making claims about the capabilities of the technology. Of note is its specific suggestion that organizations look at the marketing of their apps from the perspective of the "average user" and not of experts.[157] Also important is that the FTC specifically mentions those apps that claim to provide "health, safety, or

---

150. Industry Guides, 16 C.F.R. § 1.5 (2015).

151. *See Selected Industries*, FED. TRADE COMMISSION, https://www.ftc.gov/tips-advice/business-center/selected-industries (last visited Feb. 13, 2016).

152. *See, e.g.*, *The Children's Online Privacy Protection Rule: A Six-step Compliance Plan for Your Business*, FED. TRADE COMMISSION, https://www.ftc.gov/system/files/documents/plain-language/BUS84-coppa-6-steps.pdf (last visited Nov. 6, 2016).

153. *See generally Marketing Your Mobile App: Get It Right from the Start*, FED. TRADE COMMISSION (2013), https://www.ftc.gov/system/files/documents/plain-language/pdf-0140_marketing-your-mobile-app.pdf (highlighting how to truthfully and honestly advertise your new app) [hereinafter *Marketing Your Mobile App*].

154. *See id.*

155. *Id.*

156. *Id.*

157. *Id.*

performance" benefits.[158] According to the guide, when businesses make claims, whether express or implied, that the technology provides such benefits it must be able to support those claims with scientific evidence.[159]

Businesses that make claims of enhanced privacy or, as in the case of Snapchat, control over information, should also be required to provide supporting evidence. Two of the important claims that Snapchat made were that it offered the user the ability to control how long the "snap" would appear to the receiver, and that there was no way that the receiver could save the snap without the app knowing and alerting the sender.[160] Individuals and members of the media later debunked both of these claims.[161] Had the company been required to substantiate its claims, it may have revised how it advertised its product, and considered the implications of the wording of its claims.

Second, the FTC advises app makers to "[h]onor your privacy promises"[162] In this suggestion, the FTC focuses on the claims that organizations make not only in their privacy policies, but also claims about privacy practices.[163] Although this suggestion is not specifically directed at privacy-promising technologies, the implication is clear: if a company promises privacy or user control over data, it must honor that promise. Failure to do so should result in an action by the FTC. Snapchat's failure, for instance, to ensure its claim of information control and anti-circumvention technology resulted in the FTC's action against the organization.

V. CONCLUSION

There is a dire need for the FTC to move with specific regulatory authority over privacy-promising technologies; to do so would be well within its powers. The FTC is as an agency designed to prevent and rectify the harm brought upon consumers by the statements, omissions, or practices of those in industry.[164] Maintaining information privacy in the digital age is an area of increasing concern for consumers.[165]

---

158. *Id.*
159. *Id.*
160. Snapchat Compl., *supra* note 2, at *2, *4.
161. Ducklin, *supra* note 4.
162. *Marketing Your Mobile App*, *supra* note 153.
163. *Id.*
164. *See* Federal Trade Commission Act, 15 U.S.C. §§ 41-56.
165. *See, e.g.*, Jochen Wirtz, May O. Lwin & Jerome D. Williams, *Causes and Consequences of Consumer Online Privacy Concern*, 18 INT'L J. SERV. INDUSTRY MGMT. 326 (2007) (finding many factors contributing to growing awareness and concern for online privacy).

Technology developers have increasingly capitalized on such concerns.[166] Regulators like the FTC must remain vigilant of the overlapping interests of these two groups. Such vigilance will allow regulators to prevent the loss of privacy resulting from a fundamental misunderstanding of how privacy-promising technologies actually work. These brief suggestions would only be the beginning of an industry guide related to privacy-promising technologies that the FTC could create. These suggestions recognize two important issues with new privacy-promising technologies. First, the viewpoint of the audience is important. That is, the average person will not be digitally literate and may not be able to critically evaluate claims of enhanced privacy protection. Second, the suggestions place the onus on the corporation to live up to its privacy claims.

No expectation exists for an industry guide or a heightened standard to completely end privacy issues with new technologies. However, the goal of this Article was to provide a discussion of tools the FTC could use when evaluating the privacy promises that developers and organizations are making to induce consumers to use their technology and services.

166. *Id.* at 341-43.