NOTE

PRIVACY POLICIES, TERMS OF SERVICE, AND FTC ENFORCEMENT: BROADENING UNFAIRNESS REGULATION FOR A NEW ERA

G.S. Hans[*]

Cite as: G.S. Hans, *Privacy Policies, Terms of Service, and FTC Enforcement: Broadening Unfairness Regulation for a New Era*, 19 MICH. TELECOMM. & TECH. L. REV. 163 (2012), *available at* http://www.mttlr.org/volnineteen/hans.pdf

* J.D., University of Michigan Law School, 2012; M.S. in Information, University of Michigan School of Information, 2012; Editor-in-Chief, Vol. 17, *Michigan Telecommunications and Technology Law Review*. With thanks to my thesis advisor, Professor Don Blumenthal, and the other members of my thesis committee, Professor Jessica Litman and Alissa Centivany; Liz Allen, Musetta Durkee, Joseph Lorenzo Hall, Chris Kurpinski, Aaron Melaas, and Brandon Weiner; and Cliff Helm, Alexa Nickow, Liza Roe, Juliana MacPherson, and the *MTTLR* Volume 19 staff.

INTRODUCTION

As Americans continue to embrace the Internet as a tool for communications, business, and social interaction, a host of issues surrounding privacy, data collection, and monetization of content remain both hotly debated and increasingly urgent. In the early years of the commercial Internet, many websites—from Amazon to NYTimes.com to Craigslist—offered their services and content for free. As a result, consumers became accustomed to receiving free content, rather than having to pay individual websites or networks a subscription fee.[1]

Exploiting user data is a lucrative and effective method for websites to earn money and avoid charging consumers. User data consists of information that users provide to websites, information regarding a user's browsing habits on a particular site, or both, and can reveal a great deal about the user herself, from individual preferences to biographical information to browsing history. This data can be sold or shared with third parties, allowing advertisers to create more targeted advertisements for individual users.

In some cases, there are broad social benefits to collecting user data. For example, over the past few years, Google aggregated user search data to track flu outbreaks. The site could even have reported some of these outbreaks before the Center for Disease Control.[2] Yet collecting too much user

1. Indeed, when the *New York Times* announced that it would institute a "pay wall" by restricting content to paid subscribers and allowing non-subscribers a limited number of articles to read per month, reactions were mixed, though the pay wall was ultimately deemed successful. Don Reisinger, *NYTimes: Consumer Pay Wall Response "Positive*," CNET (July 21, 2011, 6:41 AM), http://news.cnet.com/8301-13506_3-20081371-17/nytimes-consumer-pay-wall-response-positive/.

2. Miguel Helft, *Google Uses Searches to Track Flu's Spread*, N.Y. TIMES, Nov. 11, 2008, at A1.

data could be disturbing to website users. When the extent of data collection is revealed, users' emotions have escalated to anger and frustration.[3]

A website's privacy policy should, in theory, make it clear to a website's users if and how their data is being collected, and for what purposes. These privacy policies, however, can be quite long and difficult for an average user to comprehend. Moreover, their claims may not be accurate, and users may have no way of knowing what data is collected and what exactly happens to or with their data. The federal government—specifically the Federal Trade Commission ("FTC"), an independent agency charged with protecting American consumers—has played a crucial role in regulating the collection and use of consumer data online. But in a rapidly changing online ecosystem, government regulation may not be sufficient to protect consumers.

This Note examines website privacy policies in the context of FTC regulation. The relevant portion of Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45(a), uses the following language to define the scope of the agency's regulatory authority: "Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful."[4] Specifically, this Note analyzes the FTC's power to regulate unfair practices (referred to as the FTC's "unfairness power") granted by Section 5, and also discusses the deception prong of Section 5, which allows the agency to regulate and prevent deceptive commercial acts by businesses.

This Note argues that, given the prevalence of confusing and obscure data collection practices, the FTC must aggressively interpret its statutory authority in order to effectively protect consumers. By examining three prominent websites—Google, Facebook, and Twitter—this Note demonstrates how some of their practices might be considered unfair toward consumers, in light of the statements set out in their privacy policies. However, the FTC would need to reformulate its policy choices concerning unfairness and pursue a more aggressive regulatory strategy in order to address those potentially unfair practices.

Part I of this Note examines the recent history of the FTC and its enforcement powers, including a close analysis of the FTC's policy statements on deception and unfairness and their future implications. In Part II, this Note explores the procedures and challenges of applying the legal standards in deception and unfairness cases. In Part III, the focus turns to Google and its recent decision to create a cross-platform privacy policy. Facebook, the subject of Part IV, remains in the news for privacy violations, despite a history of controversies concerning its handling of user data. Finally, Part V

3. *See, e.g.,* Julia Angwin & Jennifer Valentino-DeVries, *Apple, Google Collect User Data*, WALL ST. J. (Apr. 22, 2011), http://online.wsj.com/article/SB10001424052748703983704576277101723453610.html (discussing user "furor" following the revelation that iPhones had been tracking and recording where users went).

4. 15 U.S.C. § 45(a)(1) (2011).

discusses Twitter and the ramifications of the FTC's settlement with the microblogging service—the first case brought against a major social network. In conclusion, this Note examines the likelihood of change in the FTC's approach, the recent attention given toward consumer online privacy by the White House and the FTC, and possible trends in privacy regulation in the near future.

I. The Federal Trade Commission and Its Enforcement Powers

A. *The Background and Structure of the Federal Trade Commission*

The FTC was established in 1914 by the Federal Trade Commission Act.[5] The agency is tasked with preventing unfair methods of competition, as well as unfair or deceptive trade practices.[6] Through the powers granted to it by the FTC Act, the FTC enforces two distinct areas of law: antitrust and consumer protection.[7]

The FTC consists of three Bureaus: the Bureau of Competition ("BC"), which enforces antitrust regulations; the Bureau of Consumer Protection ("BCP"), which enforces consumer protection regulations; and the Bureau of Economics ("BE"), which conducts economic analyses.[8] BCP, the relevant FTC Bureau for this Note, consists of seven subdivisions: Advertising Practices, Marketing Practices, Financial Practices, Privacy and Identity Protection, Planning and Information, Consumer and Business Education, and Enforcement.[9]

The Division of Privacy and Identity Protection ("DPIP")—BCP's newest division—focuses on privacy issues, credit reporting, identity theft, and information security.[10] In addition to enforcing the FTC Act, it also sanctions businesses for violations of the Fair Credit Reporting Act and the Gramm-Leach-Bliley Act.[11] DPIP serves as the federal government's sole regulator for online privacy issues and practices and has brought several

5. *Id.* § 41.

6. *Id.* § 45(a)(2).

7. *About the Federal Trade Commission*, Fed. Trade Comm'n, http://www.ftc.gov/ftc/about.shtm (last visited Oct. 1, 2012).

8. *FTC Bureau of Competition*, Fed. Trade Comm'n, http://www.ftc.gov/bc/index.shtml (last visited Oct. 1, 2012); *FTC Bureau of Consumer Protection*, Fed. Trade Comm'n, http://www.ftc.gov/bcp/index.shtml (last visited Oct. 1, 2012); *FTC Bureau of Economics*, Fed. Trade Comm'n, http://www.ftc.gov/be/index.shtml (last visited Oct. 1, 2012).

9. *About the Bureau of Consumer Protection*, Fed. Trade Comm'n, http://www.ftc.gov/bcp/about.shtm (last visited Oct. 1, 2012).

10. *FTC Bureau of Consumer Protection—Division of Privacy and Identity Protection*, Fed. Trade Comm'n, http://www.ftc.gov/bcp/bcppip.shtm (last visited Oct. 1, 2012).

11. *Id.*

high-profile enforcement actions against websites and online service providers.

In November 2011, DPIP announced a settlement with the popular social network site Facebook concerning its deceptive privacy policies; the settlement was made final in August 2012.[12] The complaint alleged eight counts, including deceptive privacy settings, unfair and deceptive privacy changes, undisclosed dissemination of user information with third-party advertisers, a deceptive "Verified Apps" program, and dissemination of user photos and videos.[13] The settlement with Facebook followed other highly publicized FTC cases brought against online sites such as Google and Twitter.[14]

This Section begins by discussing policy statements dating from the early 1980s, which form the foundation of the FTC's current interpretation of its enforcement powers under Section 5. It will then proceed to analyze the interpretation of the FTC's two main enforcement powers—commonly referred to as "unfairness" and "deception"—since the policy statements were published.

B. *The Policy Statements: Unfairness and Deception*

1. Background

The FTC's enforcement powers derive from Section 5 of the FTC Act, 15 U.S.C. § 45.[15] The relevant language reads:

> (a) Declaration of unlawfulness; power to prohibit unfair practices; inapplicability to foreign trade.
>
> (1) Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful.
>
> (2) The Commission is hereby empowered and directed to prevent persons, partnerships, or corporations . . . from using unfair

12. Press Release, Fed. Trade Comm'n, Facebook Settles FTC Charges (Nov. 29, 2011), *available at* http://www.ftc.gov/opa/2011/11/privacysettlement.shtm; Press Release, Fed. Trade Comm'n, FTC Approves Final Settlement with Facebook (Aug. 10, 2012), *available at* http://www.ftc.gov/opa/2012/08/facebook.shtm.

13. Facebook, Inc., Docket No. C-4365, File No. 092-3184 (Fed. Trade Comm'n July 27, 2012) (complaint), http://www.ftc.gov/os/caselist/0923184/111129facebookcmpt.pdf.

14. Google, Inc., Docket No. C-4336, File No. 102-3136 (Fed. Trade Comm'n Oct. 13, 2011) (agreement containing consent order), http://www.ftc.gov/os/caselist/1023136/110330googlebuzzagreeorder.pdf; Twitter, Inc., Docket No. C-4316, File No. 092-3093 (Fed. Trade Comm'n Mar. 2, 2011) (decision and order), http://www.ftc.gov/os/caselist/0923093/110311twitterdo.pdf.

15. 15 U.S.C. § 45(a) (2011).

> methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce.[16]

For the first fifty years of its existence, the FTC's enforcement of Section 5 varied widely. From the late 1960s through the early 1980s, a very public and contentious debate played out in Washington, with the policy statements serving as the final volley.

In 1969, Ralph Nader spearheaded a project criticizing the work of the FTC. Nader pulled no punches in referring to the FTC as the "little old lady of Pennsylvania Avenue . . . manipulated by the agents of commercial predators, impervious to governmental and citizen monitoring."[17] The American Bar Association also published a report documenting the shortcomings of the FTC and contemplated the dissolution of the agency due to its ineffectiveness.[18] In response to these criticisms, President Richard Nixon appointed Caspar Weinberger as the Chairman of the FTC with the explicit goal of improving the FTC's reputation.[19]

In 1975, Congress passed the Magnuson-Moss Warranty Act, which gave the FTC explicit rulemaking authority.[20] After the election of President Jimmy Carter in 1976, Michael Pertschuk was appointed Chair of the FTC.[21] Under Pertschuk, the FTC created several new rules pursuant to its authority under the Magnuson-Moss Warranty Act.[22] The FTC's unprecedented vigorous enforcement led to a backlash from businesses that did not respond well to increased government oversight and regulation.[23] As a result, Congress cut the FTC's appropriations and nearly shut the agency's doors in 1980.[24] Eventually, in order to combat accusations of ad hoc and unsystematic enforcement, the Commission moved to an economic analysis model, conducted by the Bureau of Economics, to determine how to best enforce the provisions of the FTC Act.[25] Policy statements on unfairness and deception were borne out of this tense political context, explicitly designed by the FTC to limit its own authority in order to combat future accusations that the agency regulated too aggressively and avoid another potential dissolution of the agency itself.

---

16. *Id.*

17. Ralph Nader, *preface* to EDWARD F. COX, ROBERT C. FELLMETH & JOHN E. SCHULZ, THE NADER REPORT ON THE FEDERAL TRADE COMMISSION vii (Richard W. Baron ed.) (1969).

18. AM. BAR ASS'N, REPORT OF THE A.B.A. COMMISSION TO STUDY THE FEDERAL TRADE COMMISSION (1969).

19. *See, e.g.*, William J. Baer, *Where to from Here: Reflection on the Recent Saga of the Federal Trade Commission*, 39 OKLA. L. REV. 51, 52 (1986).

20. *See* 15 U.S.C. §§ 2301–12 (2011).

21. *See, e.g.*, *Commissioners and Chairmen of the Federal Trade Commission*, FED. TRADE COMM'N (Oct. 2010), http://ftc.gov/ftc/history/commisionerchartlegal2010.pdf.

22. Baer, *supra* note 19, at 53.

23. *Id.*

24. *Id.* at 54.

25. *Id.* at 55.

2. The Policy Statements

The first policy statement, dated December 17, 1980, addressed the FTC's unfairness power.[26] The Unfairness Policy Statement was sent to Senators Wendell Ford and John Danforth in response to a letter they had written to the FTC requesting its views on how to interpret "consumer unfairness."[27] In the Statement, the FTC relied upon the Supreme Court's holding in *FTC v. Sperry & Hutchinson Co.*,[28] which used three factors to evaluate whether a practice was unfair: (1) whether the practice injures consumers, (2) whether it violates established public policy, and (3) whether it is unethical or unscrupulous.[29]

In evaluating the first factor, the FTC required the injury to meet three requirements: (1) the injury must be substantial, (2) other consumer or competitive benefits must not outweigh it, and (3) it must not be an injury that consumers could have substantially avoided.[30] Regarding the second factor, the FTC looks toward statutes, common law, industry practice, and public policy to evaluate "the validity and strength of the evidence of consumer injury."[31] If the FTC were to rely heavily upon public policy to buttress an unfairness claim, the policy would need to be clearly defined and well established.[32] The FTC determined that because the third factor was largely duplicative of the first two, it would use only the first two factors as a basis for an unfairness finding.[33]

FTC officials created the second policy statement—the Deception Policy Statement—nearly three years later, in October 1983. This policy statement also took the form of a letter to Congress—this time, as a response to Representative John Dingell.[34] In the Deception Policy Statement, the FTC observed that in all deception cases, "there must be a representation, omission, or practice that is likely to mislead the consumer."[35] Such a representation, omission, or practice must be material to a consumer acting reasonably under the circumstances.[36] In establishing whether a representation, omission, or practice

26. Letter from Michael Pertschuk, Chairman, Fed. Trade Comm'n, et al., to Sen. Wendell H. Ford & Sen. John C. Danforth (Dec. 17, 1980), *reprinted in* Int'l Harvester Co., 104 F.T.C. 949 app. (1984), *available at* http://www.ftc.gov/bcp/policystmt/ad-unfair.htm [hereinafter Unfairness Policy Statement].

27. *Id.*

28. Fed. Trade Comm'n v. Sperry & Hutchinson Co., 405 U.S. 233 (1972).

29. *See* Unfairness Policy Statement, *supra* note 26.

30. *Id.*

31. *Id.*

32. *Id.*

33. *Id.*

34. Letter from James C. Miller III, Chairman, Fed. Trade Comm'n, et al., to Rep. John D. Dingell (Oct. 14, 1983), *reprinted in* Cliffdale Assocs., Inc., 103 F.T.C. 110 app. (1984), *available at* http://www.ftc.gov/bcp/policystmt/ad-decept.htm [hereinafter Deception Policy Statement].

35. *Id.*

36. *Id.*

is likely to mislead the consumer, the FTC looks to both express and implied claims.[37] In the case of implied claims, the FTC examines the representation itself and looks to extrinsic evidence to evaluate the implied claim.[38] The FTC also considers cases involving the omission of material information as a deceptive practice.[39]

Concerning the consumer's reasonableness, the FTC examines the entire advertisement, transaction, or course of dealing in order to evaluate a deceptiveness claim.[40] "Puffed" claims, as well as claims that are obviously exaggerated, do not meet this standard.[41] In general, the FTC will consider many factors in determining an "ordinary consumer's" reaction. These include the clarity of the representation, whether qualifying information is conspicuous, the importance of any omitted information (and whether such information is available elsewhere), and the familiarity of the public with the product or service.[42]

Regarding the materiality of the representation, omission, or practice, the FTC first attempts to determine whether the representation in question is likely to affect a consumer's choice or conduct concerning a product.[43] Express claims—claims that the seller explicitly makes to consumers—are presumptively material. Claims that would be important to a reasonable consumer, such as health or safety claims, are also presumptively material.[44] Absent these elements, the FTC may look to other evidence in order to determine whether consumers will consider a claim or omission material.[45]

Both policy statements were appended to FTC cases: the Unfairness Policy Statement to *International Harvester Co.*,[46] and the Deception Policy Statement to *Cliffdale Associates, Inc.*[47] In 1994, Congress codified the Unfairness Policy Statement into law at 15 U.S.C. § 45(n).[48] Although the Deception Policy Statement was not codified into statutory law, it has been adopted by multiple courts, making it persuasive, if not binding, authority in future cases.[49]

37. *Id.*
38. *Id.*
39. *Id.*
40. *Id.*
41. *Id.*
42. *Id.*
43. *Id.*
44. *Id.*
45. *Id.*
46. International Harvester Co., 104 F.T.C. 949 app. (1984)
47. Cliffdale Assocs., Inc., 103 F.T.C. 110 app. (1984).
48. 15 U.S.C. § 45(n) (2011); *see also* Stephen Calkins, *FTC Unfairness: An Essay*, 46 WAYNE L. REV. 1935, 1955–60 (2000).
49. *See, e.g.*, Fed. Trade Comm'n v. Amy Travel Serv., Inc., 1988 U.S. Dist. LEXIS 13371 (N.D. Ill. Feb. 10, 1988).

3. Implications of the Policy Statements

Though the FTC severely circumscribed its ability to litigate at the level it had following passage of the Magnuson-Moss Warranty Act by creating the policy statements, the FTC also arguably saved itself from defunding and irrelevance. Because the policy statements codified the FTC's approach and analysis in unfairness and deception cases, they obviated charges from critics that the agency was inconsistent and unpredictable in bringing cases against businesses. Both statements set out a clear rubric of how the FTC conceives of unfairness and deception and what elements are required for a successful claim.

Courts have consistently relied upon the policy statements for decades, ensuring that they remain a central part of current FTC Act litigation. In the immediate future, political pressure (either from politicians or non-profit organizations) seems to be the sole way of persuading the agency to take a more aggressive role in pursuing commercial organizations that violate the unfairness and deception prongs of the FTC Act. Given the implications that the recent financial crisis has had on government funding, it seems unlikely that the FTC's role will expand drastically. Unless and until consumer frustration reaches the levels documented by Ralph Nader and the ABA in the late 1960s, the FTC's current approach to enforcement via the policy statements will likely remain stable.

II. Applying the Standards in Deception and Unfairness Cases

A. *Deception Cases*

Deception remains the most commonly used prong of the FTC Act.[50] This is likely because of its relative clarity compared to unfairness—it is easier to identify a discrete example of a deceptive practice that misleads consumers than one that is unfair to consumers (and not offset by a consumer benefit). Indeed, in the years since the Deception Policy Statement's publication, the FTC has chosen to use deception rather than unfairness as the basis for its litigation in most cases.[51]

To evaluate the existence of a deceptive trade act or practice, courts generally use the standard articulated in the Deception Policy Statement: "namely, that a practice falls within [the prohibition on deception] (1) if it is likely to mislead consumers acting reasonably under the circumstances

50. *See, e.g.*, Mark E. Budnitz, *The FTC's Consumer Protection During the Miller Years: Lessons for Administrative Agency Structure and Operation*, 46 Cath. U. L. Rev. 371, 396 (1997).

51. *Id.*

(2) in a way that is material."[52] This language is fairly constant throughout recent decisions, suggesting that the deceptiveness doctrine has reached a state of equilibrium. The broad acceptance by courts of what constitutes a colorable deceptiveness claim rebuts the assertions that the FTC's enforcement agenda is inconsistent or unpredictable. That may indicate why litigation under the deception prong remains the agency's weapon of choice.

The appeal of this approach to regulating commercial malfeasance is obvious. The standard has two discrete elements that the agency can evaluate with relative ease. The specific requirements for a deceptiveness case discuss a "reasonable person" and materiality, which are well-established standards throughout the common law. By contrast, the unfairness analysis (as discussed below) uses a more complicated balancing test. Compared to the unfairness test, the deception test serves as a sharper tool to use in evaluating specific cases due to its clearer standards and the larger body of relevant case law.

B. *Unfairness Cases*

In unfairness cases, the standard from Section 5 of the FTC Act controls: "an unfair practice or act is one that 'causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.'"[53] The FTC must therefore demonstrate three criteria, as opposed to only two under the deception standard. Moreover, the unfairness criteria are arguably more difficult to satisfy, since companies can defeat a charge of unfairness by either (1) giving consumers an opportunity to avoid the injury or (2) offsetting it with other benefits.

Stephen Calkins, former General Counsel of the FTC, argues that both the Unfairness Policy Statement and the underlying standards are unhelpful to the FTC and to businesses.[54] During the fourteen years between the publication of the Unfairness Policy Statement and its incorporation into the FTC Act, the FTC stated that it had relied upon the Unfairness Policy Statement in only sixteen cases.[55] Calkins notes that the FTC undercounted and that it also relied upon the test articulated in the Unfairness Policy Statement in several trade regulation rules and ten additional consent orders, but that the number was still small.[56] Given the agency's infrequent use of the unfairness prong to regulate businesses, the FTC was perhaps demon-

52. *See, e.g.*, Fed. Trade Comm'n v. Cyberspace.com, 453 F.3d 1196, 1199–1200 (9th Cir. 2006); Fed. Trade Comm'n v. Med. Billers Network, 543 F. Supp 2d 283, 303 (S.D.N.Y. 2008).

53. Fed. Trade Comm'n v. Neovi, Inc., 2010 U.S. App. LEXIS 12592, *7–8 (9th Cir. Mar. 4, 2010).

54. Calkins, *supra* note 48, at 1937.

55. *Id.* at 1958.

56. *Id.* at 1958–60.

strating its lack of commitment to using unfairness as a regulatory tool. Upon surveying the muddied landscape of unfairness, Calkins argues for increased administrative adjudication to clarify the unfairness standard.[57] He also advocates for increased attention to the cost/benefit analysis (as applied to consumers) prescribed by the Unfairness Policy Statement, and less adherence to consumer injury.[58]

Calkins portrays the unfairness power not as a flexible tool, but as a fuzzy and indistinct doctrine.[59] As he observes, the language of the FTC Act was intentionally vague in order to allow judicial decisions to further clarify and shape the meanings of deception and unfairness.[60] Whether the relevant case law has actually provided such clarity is, of course, debatable. But by examining the recent judicial decisions on unfairness more closely, one may find that possible applications of the unfairness standard in the online space become clearer. In fact, an unfairness claim is demonstrably more useful against websites than a deception claim would be. Websites make material claims to users by using terms of service and privacy policies, and relying upon the deception prong in order to regulate websites would require a "gotcha" moment, in which the website would inadvertently or negligently misrepresent its practices to consumers. By contrast, using the unfairness prong would more proactively regulate the core of website practices, rather than waiting for providers to make a mistake.

C. *Recent Tracking in* Sears Holdings *and Its Implications*

The recent settlement in the *Sears Holdings* case demonstrates the FTC's renewed commitment to increasing consumers' awareness of data collection.[61] The FTC did not use the unfairness prong in *Sears Holdings*; instead, it relied upon the deception prong.[62] Using the deception prong may indicate a more conservative approach to regulating data collection, or it might merely indicate that the deception prong was a better fit in this case. Either way, *Sears Holdings* indicates that the FTC considers data collection to be well within its power to regulate under the FTC Act.

---

57. *Id.* at 1989. Of course, any increased agency action would either require an increase in resources or a reduction in other agency actions or practices. Whether the agency is even able to increase its regulatory agenda, given the paucity of government resources in the current political environment, is certainly up for debate.

58. *Id.* at 1990–91.

59. *Id.* at 1989.

60. *Id.* at 1949.

61. Sears Holdings Mgmt. Corp., Docket No. C-4264, File No. 0823099 (Fed. Trade Comm'n Sept. 9, 2009) (decision and order), http://www.ftc.gov/os/caselist/0823099/090604searsdo.pdf.

62. *See* Sears Holdings Mgmt. Corp., Docket No. C-4264, File No. 0823099 (Fed. Trade Comm'n June 4, 2009) (complaint), http://www.ftc.gov/os/caselist/0823099/090604searscmpt.pdf.

In 2009, the FTC settled a complaint with Sears Holdings Management Corporation after alleging that the company disseminated a software program to consumers that tracked nearly all of the consumers' Internet traffic and behavior, presumably to sell the aggregated data to third-party data brokers who sought to monetize online consumer behavior.[63] Consumers received ten dollars for joining the service but lacked awareness of the extent to which Sears Holdings subsequently collected their data.[64] While Sears Holdings stated that its software would track "online browsing," the company did not disclose that the application would track nearly all of a user's Internet behavior.[65]

The FTC alleged that these actions constituted deceptive behavior under Section 5.[66] Sears Holdings' practices were material to consumers' decisions in selecting to install the software, but the company did not disclose the facts to consumers in its Privacy Statement and User License Agreement ("PSULA").[67] The PSULA instead stated that the software would track consumers' "online browsing," but did not state the actual extent of such tracking. The FTC alleged that the statements in the PSULA would not indicate to a reasonable consumer that Sears Holdings tracked nearly all of her online behavior.[68] Moreover, there was no visible indication to consumers that the program was constantly tracking their usage. Given these failures, the FTC alleged that Sears Holdings' practices were deceptive. The final settlement in *Sears Holdings* required the company to disclose to users exactly what data was being collected, how it was being used, and whether it was being turned over to third parties.[69] It also required Sears Holdings to delete *all* user data that it had previously collected.[70]

This case illustrates the primary considerations that the FTC has in mind when investigating Internet data collection cases: disclosure from businesses, the extent of data collection, third-party communication, and data retention. These considerations, as well as the general privacy claims and practices that websites communicate to users, are critical in every FTC investigation and enforcement action.

63. *Id.*

64. *Id.* at 3–4.

65. *Id.* at 5. The complaint alleged that the software tracked almost all Internet behavior, including information transmitted between the computer and websites. *Id.*

66. *Id.*

67. *Id.*

68. *Id.*

69. Press Release, Fed. Trade Comm'n, FTC Approves Final Consent Order Requiring Sears to Disclose the Installation of Tracking Software Placed on Consumers' Computers; FTC Approves Final Consent Order in Matter Concerning Enhanced Vision Systems, Inc. (Sept. 9, 2009), *available at* http://www.ftc.gov/opa/2009/09/sears.shtm.

70. *Id.*

III. GOOGLE: CROSS-PLATFORM PRIVACY POLICIES AND THE ALLURE OF DATA COLLECTION

A. *Traffic, Money, and "Don't Be Evil"*

As the world's most-used search engine and leading digital advertising services company, Google has a great deal of information about consumers and knows how to successfully advertise products and services to them.[71] Moreover, Google's many other products have become an indispensable part of consumer experiences online. Many individuals use Gmail, Google's mail client, as their personal email account; YouTube, the video uploading and streaming site that Google bought in 2006, ranks as the third most visited domain worldwide and in the United States;[72] and various other Google services, such as Blogger, Google Checkout, Google Analytics, and Google Maps, have become vital to Internet users.

Because Google collects, collates, and retains so much raw data—both regarding Internet search queries and its users' behavior within Google's suite of sites—it ranks as one of the most highly valued Internet companies, with a current stock price of over $650 per share.[73] Given that many Internet companies have been unable to put pay walls into place to successfully monetize their content, many Internet companies have chosen to imitate Google's innovative data collection model to make money. User data can be collected, aggregated, and sold to advertisers and other data collectors. Companies can therefore target specific users in order to more accurately and effectively advertise their goods and services. Google is extremely well-positioned to collect and sell vast amounts of user data due to its high traffic volume, ubiquity, and suite of products ranging from search to email to blogging. While the company's unofficial motto is famously "Don't be evil," such absolutist catchphrases are minimally useful in an Internet ecosystem full of shades of gray.[74] As a publicly traded company, Google cannot interpret "Don't be evil" as "don't make money" without betraying its shareholders. With user data remaining a hot commodity, Google has taken steps that, while not necessarily "evil," do not demonstrate a pure commitment to "good." Google's own actions concerning its use of user data, while

71. *See, e.g.*, KEN AULETTA, GOOGLED: THE END OF THE WORLD AS WE KNOW IT xi (2010).

72. *Youtube.com Site Info*, ALEXA, http://www.alexa.com/siteinfo/youtube.com (last visited Oct. 4, 2012). Google is currently ranked number one within the United States. *See Google.com Site Info*, ALEXA, http://www.alexa.com/siteinfo/google.com (last visited Oct. 18, 2012).

73. *GOOG: Summary for Google Inc.*, YAHOO! FINANCE, http://finance.yahoo.com/q?s=GOOG (last visited Oct. 21, 2012).

74. *See, e.g.*, Mat Honan, *Google's Broken Promise: The End of "Don't Be Evil"*, GIZMODO (Jan. 24, 2012, 5:41 PM), http://gizmodo.com/5878987/its-official-google-is-evil-now.

valuable from a business standpoint, are sufficiently opaque to consumers to warrant FTC examination.

B. *Privacy Run-Ins and Government Concerns*

Given its vast suite of products, Google inevitably encounters problems with privacy advocates and American regulators regarding apparent and actual privacy violations. Three products have attracted a large amount of public attention: Google Books, Google Buzz, and Google Maps.

Google Books, which Google uses to sell electronic books (or e-books) directly to consumers, was at one point the great hope for digitizing a large corpus of literary works.[75] Google, seeking to enlarge its database of scanned books, created high-definition electronic scans of books that were under copyright but out of print. American copyright law does not require that artistic works be registered in order to receive protection; therefore, locating the rightsholders of protected, out-of-print materials can be difficult.[76] Google's solution was to scan entire books but to display only a small portion; the company intended to rely upon a fair use defense to forestall any copyright infringement claims.[77] However, objections from authors and the government in a variety of legal areas—from copyright to antitrust to privacy—have greatly altered the project from its initially imagined form.[78]

One of the major concerns surrounding Google Books was reader privacy. Google had not committed to incorporating privacy protections within the project akin to the levels granted to readers who buy books from brick-and-mortar bookstores and libraries. Librarians have traditionally been strong proponents of reader privacy, as have bookstore owners, and courts have upheld an individual's right to privacy in more traditional reading spaces.[79] However, Google's proposed privacy protections—which did not extend beyond its baseline privacy policy—did not rise to the level of traditional reader privacy protections.[80] Google appeared to be more concerned

75. Pamela Samuelson, *Google Book Search and the Future of Books in Cyberspace*, 94 MINN. L. REV. 1308, 1314 (2010).

76. 17 U.S.C. § 408(a) (2011).

77. Samuelson, *supra* note 75, at 1314 n.32. Fair use is a statutory affirmative defense available to alleged infringers. In a copyright infringement case, the trier of fact will look to the purpose and character of the allegedly infringing use, the nature of the copyrighted work, the amount used compared to the original work, and the effect upon the market, in order to determine if the alleged infringer can rely upon fair use as a defense to infringement. 17 U.S.C. § 107 (2011).

78. For an excellent overview of objections to Google Books, see Samuelson, *supra* note 75 at 1326–58.

79. *E.g.*, *In re* Grand Jury Subpoena to Kramerbooks & Afterwords Inc., 26 Media L. Rep. (BNA) 1599 (D.D.C. 1998); Tattered Cover, Inc. v. City of Thornton, 44 P.3d 1044, 1059 (Colo. 2002).

80. Samuelson, *supra* note 75, at 1347. In *Tattered Cover*, the court upheld the bookstore's right to resist subpoenas requiring the store to divulge readers' buying habits as an invasion of privacy. *Tattered Cover*, 44 P.3d at 1047; *see also Kramerbooks*, 26 Media L.

with its commercial bottom line than with allowing users to feel free to browse and purchase books while maintaining their privacy.

While privacy objections surrounding Google Books remain abstract given that the product has not been fully implemented, other privacy issues involving Google products have directly affected consumers. Google Buzz, one of the company's least successful products, created a minor firestorm upon its automatic introduction to all Gmail users in February 2010. When it launched, Google Buzz immediately broadcasted the contacts that each user most frequently communicated with to other users.[81] In one prominent case, a blogger who wrote about violence against women feared for her own safety from antagonistic followers and her abusive ex-husband.[82] Such concerns eventually led to an FTC settlement,[83] which specified that Google had used deceptive practices in its launch of Google Buzz and that it would agree to refrain from future privacy misrepresentations, launch a comprehensive privacy program, and consent to independent privacy audits for twenty years.[84] Google eventually closed Buzz and moved its social networking platforms to Google Plus, a product it launched in 2011 to compete with Facebook.[85]

Later in 2010, German privacy authorities discovered that Google vehicles that had been mapping city streets for its Google Maps project had also been collecting data on personal wireless networks and transfers therein.[86] Dubbed Google "Spyfi" due to Google's apparent surveillance of Wifi networks, the controversy demonstrated to some critics that Google has "a

Rep. (BNA) at 1600. Yet Google was not willing to match that level of privacy. Google Books instead would adopt the general Google privacy policy, allowing Google to track users' purchase history, browsing history, and past and present actions using the service, and cross-reference those actions with other Google products. *See* Samuelson, *supra* note 75, at 1347. This level of tracking is far in excess of the abilities of a traditional bookstore to monitor its customers, and if Google Books had been implemented in the form proposed by Google in the settlement, readers would have been monitored far in excess of the privacy a bookstore browser would normally have. *Id.* at 1346 n.190.

81. Miguel Helft, *Critics Say Google Invades Privacy with New Service*, N.Y. TIMES (Feb. 12, 2010), http://www.nytimes.com/2010/02/13/technology/internet/13google.html.

82. *Id.*

83. Google Inc., Docket No. C-4336, File No. 102-3136 (Fed. Trade Comm'n Oct. 13, 2011) (order), http://www.ftc.gov/os/caselist/1023136/111024googlebuzzdo.pdf.

84. *See id.*; Press Release Fed. Trade Comm'n, FTC Charges Deceptive Privacy Practices in Google's Rollout of its Buzz Social Network (Mar. 30, 2011), *available at* http://www.ftc.gov/opa/2011/03/google.shtm.

85. *See* Claire Cain Miller, *Another Try by Google to Take on Facebook*, N.Y. TIMES (June 28, 2011), http://www.nytimes.com/2011/06/29/technology/29google.html?pagewanted=all.

86. David Kravets, *An Intentional Mistake: The Anatomy of Google's Wi-Fi Sniffing Debacle*, WIRED (May 02, 2012, 7:18 PM), http://www.wired.com/threatlevel/2012/05/google-wifi-fcc-investigation/; David Sarno, *Lawmakers Grill Google's Eric Schmidt on "Spy-Fi" Privacy Issue*, L.A. TIMES (May 26, 2010), http://latimesblogs.latimes.com/technology/2010/05/legislators-grill-google-eric-schmidt-on-spyfi-privacy-issue.html.

bunch of engineers who push the envelope and gather as much information as they can and don't think about the ramifications of that."[87]

While Google has avoided major privacy controversies in the last year, it still attracts attention when consumers and critics perceive its products as overreaching. In February 2012, various news outlets reported that Google and other advertisers had circumvented settings on Safari—Apple's web browser and the most popular mobile browser—allowing the company to track users' web browsing.[88] The FTC declined to comment on whether it would look into this privacy violation as part of its overall settlement with Google concerning Google Buzz. The terms of that settlement would certainly permit the agency to do so, however, as Google had pledged to enact a comprehensive privacy regime as a condition of the settlement.[89] As many of the agency's proceedings are not disclosed to the public, consumers will almost certainly remain unaware of how much the FTC polices Google's activities and whether the agency's current enforcement strategy responds to each fresh privacy stumble. Increased disclosure from the agency regarding the results of Google's privacy audits would alleviate this concern.

C. *A Change in Privacy—Or Not?*

In January 2012, Google announced an update to its privacy policy on its official blog.[90] Google characterized its new policy as a streamlining of over seventy privacy documents in order to better integrate the vast portfolio of Google products.[91] Some privacy policies would remain independent of the "master policy," but in general, the changes would better accommodate regulatory requests for simplicity while preserving user independence.[92] One of the most notable changes was the removal of the "silo-ing" of user data among Google products. Previously, YouTube user data had been kept separate from Google search data, but under the new terms, Google would analyze all user data together.[93]

87. Maggie Shiels, *Google Admits Wi-Fi Data Collection Blunder*, BBC (May 15, 2010), http://news.bbc.co.uk/2/hi/technology/8684110.stm.

88. Julia Angwin & Jennifer Valentino-DeVries, *Google's iPhone Tracking*, WALL ST. J. (Feb. 17, 2012), http://online.wsj.com/article_email/SB10001424052970204880404577225380456599176-lMyQjAxMTAyMDEwNjExNDYyWj.html.

89. Google Inc., Docket No. C-4336, File No. 102-3136 (Fed. Trade Comm'n Oct. 13, 2011) (order), http://www.ftc.gov/os/caselist/1023136/111024googlebuzzdo.pdf.

90. Alma Whitten, *Updating Our Privacy Policies and Terms of Service*, GOOGLE OFFICIAL BLOG (Jan. 24, 2012), http://googleblog.blogspot.com/2012/01/updating-our-privacy-policies-and-terms.html.

91. *Id.*

92. *Id.*

93. *See* Rainey Reitman, *What Actually Changed in Google's Privacy Policy*, ELEC. FRONTIER FOUND. DEEPLINKS BLOG (Feb. 1, 2012), https://www.eff.org/deeplinks/2012/02/what-actually-changed-google%27s-privacy-policy [hereinafter EFF].

Many privacy advocates and regulators were concerned by Google's new cross-platform privacy policy.[94] In part, this seems due to the company's mixed track record on privacy. Even assuming that Google had expressed a greater willingness to respect user privacy following the Google Buzz consent decree, the recent Safari incident demonstrates that Google has been unable to stay out of the news regarding perceived privacy violations. As a result, Google's changes and assurances have been met with a healthy dose of skepticism.[95]

Following a request from American legislators, Google elaborated on how its privacy policy actually changed as a result of the streamlining.[96] The Electronic Frontier Foundation summarized the changes as allowing Google to use data collected from YouTube and search history in other Google products.[97] Google explained that, for instance, users who searched for recipes on Google would receive cooking videos as suggestions while browsing YouTube.[98] If Google users wanted to preserve the status quo and prevent this commingling of data, however, they would have to create separate accounts for different Google products.[99]

From the perspective of unfairness enforcement under the FTC Act, there are a number of issues that might point to the possibility of an unfairness claim. As discussed in Part II.B, unfairness traditionally invokes the standard codified in 15 U.S.C § 45(n), requiring an act or practice that (1) causes or is likely to cause substantial injury to consumers (2) which is not reasonably avoidable by consumers or (3) outweighed by other benefits.[100] Meeting the three-factor test in this case seems difficult, though not impossible.

Substantial injury would require demonstrating that Google's new privacy policy adversely affected consumers, which is not an obvious finding in the online ecosystem. In this context, meeting this factor would likely require a data breach causing the release of identifiable un-anonymized user data; mere commingling of data across services would probably not qualify

94. *See, e.g.*, *id.*; Rob Waugh, *Unfair and Unwise: Google Brings in New Privacy Policy for Two Billion Users—Despite EU Concerns It May Be Illegal*, DAILY MAIL ONLINE (Mar. 1, 2012, 7:28 PM), http://www.dailymail.co.uk/sciencetech/article-2108564/Google-privacy-policy-changes-Global-outcry-policy-ignored.html.

95. *See, e.g.*, EFF, *supra* note 93.

96. *See* Letter from Pablo Chavez, Dir. of Pub. Policy, Google, Inc., to Members of Congress, Jan. 30, 2012, *available at* https://docs.google.com/viewer?a=v&pid=explorer&chrome=true&srcid=0BwxyRPFduTN2NTZhNDlkZDgtMmM3MC00Yjc0LTg4YTMtYTM3NDkxZTE2OWRi&hl=en_US&pli=1.

97. *See* EFF, *supra* note 93.

98. *See* Letter from Pablo Chavez to Members of Congress, *supra* note 96, at 3.

99. *See* EFF, *supra* note 93.

100. 15 U.S.C. § 45(n) (2011).

as a substantial injury.[101] Thus, absent financial harm or damage to personal property like computers, it seems unlikely that most websites' privacy policies will meet this standard.

By comparison, meeting the other two factors of the unfairness test seems markedly easier. Consumers cannot easily avoid the changes in Google's policy for many reasons. First, the new policy contains no opt-out provisions. Customers were not able to prevent the new policy from going into effect, and they could only work to disassociate their user data before the new policy was implemented.[102] Moreover, users cannot easily switch to other products in order to avoid the changes, given Google's entrenchment within the Internet landscape. The high transaction costs involved in switching from Google products and the premier status of these products means that Google users have a strong degree of loyalty to the company's services.[103]

The final aspect of the unfairness balancing test—whether the benefits of the practice outweigh any substantial injury to consumers—also skews against Google. While Google may claim that its new policies benefit users, this is not readily apparent. Some users may find suggested cooking videos, as in Google's hypothetical, surprising or even unsettling.[104] In addition, Google's track record of taking unilateral action to benefit users received heavy criticism in the Google Buzz case. It is unclear how exactly Google's new practices benefit users; while the new *wording* of the

101. The classic definition of "substantial injury" is an act or practice that either does "small harm to a large number of people, or . . . raises a significant risk of concrete harm." Am. Fin. Servs. Ass'n v. Fed. Trade Comm'n, 767 F.2d 957, 972 (D.C. Cir. 1985).

102. *See, e.g.*, Eva Galperin, *How to Remove Your YouTube Viewing and Search History Before Google's New Privacy Policy Takes Effect*, ELEC. FRONTIER FOUND. DEEPLINKS BLOG (Feb. 23, 2012), https://www.eff.org/deeplinks/2012/02/how-remove-your-youtube-viewing-and-search-history-googles-new-privacy-policy; Eva Galperin, *How to Remove Your Google Search History Before Google's New Privacy Policy Takes Effect*, ELEC. FRONTIER FOUND. DEEPLINKS BLOG (Feb. 21, 2012), https://www.eff.org/deeplinks/2012/02/how-remove-your-google-search-history-googles-new-privacy-policy-takes-effect.

103. *See, e.g.*, Patrick Stafford, *Google Users Show Most Loyalty*, SMART COMPANY (Aug. 18, 2009), http://www.smartcompany.com.au/internet/20090818-google-users-show-most-loyalty.html.

104. *See* discussion *supra* note 96. In a letter to members of Congress, Google suggested that the ability under the new privacy policy to suggest videos on a specific topic to users who had searched for related topics would be beneficial to users. However, some users have complained about Google's ability to assume that a user is looking for a specific result before the user specifically requests that result, most notably in the area of Autocomplete. Autocomplete automatically suggests results to Google users as they begin to type in a query to the search engine, based on the most popular searches related to the first words of a search query. In one notable case, Autocomplete suggested to users in Germany that they were trying to determine if the former First Lady, Bettina Wulf, had been a prostitute or an escort, despite the fact that there was never any plausible evidence that she actually had been either. *See* Nicholas Kulish, *As Google Fills in Blank, a German Cries Foul*, N.Y. TIMES, Sept. 18, 2012, at A4. Because the presumption that Autocomplete suggested was inaccurate, it led to user frustration, demonstrating that Google's predictive algorithms are not always welcome to users.

privacy policy is arguably simpler (though not necessarily clearer to consumers), the actual *content* does not provide any obvious benefits.

Without evidence of actual consumer harm, an unfairness claim against Google concerning its new privacy policy would be difficult to substantiate. Under the terms of the consent decree, the FTC likely has a lower evidentiary burden than under a traditional FTC Act claim. But, given that Google gave clear advance notice to its users and undertook the changes in part to make the landscape easier to understand, it has arguably met the "comprehensive privacy program" standard of the consent decree.[105] Moreover, Google's transparency concerning the changes (even if legislative action proved necessary to obtain clarity) probably forestalls a successful deception claim under the FTC Act.

In August 2012, the FTC announced a proposed settlement with Google for violations of the consent decree.[106] The fine was the largest penalty in history for violating an FTC order,[107] demonstrating the FTC's commitment to protecting consumer privacy and existing consent decrees,[108] as well as its awareness of criticisms that it was lax on privacy protection and enforcement.[109] The fine, however, does not specifically allege that Google committed unfair or deceptive acts or practices, but rather that the company violated the terms of the consent decree by making misrepresentations—a term that points more toward deception than unfairness, given the requirements of the two tests.[110] It remains to be seen

105. Specifically, the Google Buzz consent decree requires Google to "establish and implement, and thereafter maintain, a comprehensive privacy program that is reasonably designed to: (1) address privacy risks related to the development and management of new and existing products and services for consumers, and (2) protect the privacy and confidentiality of covered information." *See* Google Inc., Docket No. C-4336, File No. 102-3136 (Fed. Trade Comm'n Oct. 13, 2011) (order), http://www.ftc.gov/os/caselist/1023136/111024googlebuzzdo.pdf.

106. Press Release, Fed. Trade Comm'n, Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser (Aug. 9, 2012), *available at* http://ftc.gov/opa/2012/08/google.shtm.

107. *Id.*

108. *See, e.g.*, Claire Cain Miller, *F.T.C. Fines Google $22.5 Million for Safari Privacy Violations*, N.Y. TIMES BITS BLOG (Aug. 9, 2012, 1:03 PM), http://bits.blogs.nytimes.com/2012/08/09/f-t-c-fines-google-22-5-million-for-safari-privacy-violations/ (describing BCP Director David Vladeck's comments regarding technology companies and their responsibilities toward users).

109. In June 2012, *Wired* and *ProPublica* published an article criticizing the FTC for its lack of funding and allegedly outdated approach to protecting consumers' privacy. *See* Peter Maass, *Your FTC Privacy Watchdogs: Low-Tech, Defensive, Toothless*, WIRED (June 28, 2012, 6:30 A.M.), http://www.wired.com/threatlevel/2012/06/ftc-fail/all/. The article created a flurry of controversy as the FTC responded to rebut what it saw as unfair implications, creating a "he said, she said" dynamic between the agency and ProPublica. *See Correspondence Between the FTC and ProPublica*, PROPUBLICA (Jul. 6, 2012, 3:55 PM), http://www.propublica.org/article/ftc-emails.

110. *See* Press Release, Fed. Trade Comm'n, *supra* note 106.

what new cases or consent decree violations the FTC will bring against the company, and for which actions.

D. *Google at Home and Abroad*

Google's change in its privacy policy, of course, may not be legally or ethically wrong. Just because a company changes a privacy policy in order to benefit its own data-collection practices, it is not necessarily acting unfairly under either an FTC definition or general consumer understanding. Companies constantly enact changes for a variety of reasons. Yet Google's prior conduct makes its recent changes surprising from a public relations perspective. Despite the company's multiple high-profile privacy violations, it is unclear whether it has reformed. Indeed, it is hard to dispel the perhaps cynical suspicion that Google's actions serve a commercial benefit in a way that unfairly harms consumers. The Commission's August 2012 fine demonstrates, however, that government regulators are watching the company closely.

Foreign authorities have also focused their attention on Google, in some cases opening their own inquiries.[111] In Europe, where privacy protections are more stringent, authorities have gone so far as to suggest that Google's new policy appears to violate European Union ("EU") law.[112] The National Commission for Computing and Liberties ("CNIL"), a French privacy agency, stated in a letter to Google CEO Larry Page that the lack of clarity surrounding exactly how Google combined user data pointed to a possible violation of the law.[113]

The FTC does not necessarily need to investigate a company merely because foreign officials are conducting investigations, but the EU's identification of vagueness and obscurity in Google's explanations within the new privacy policy suggests a need for further investigation on our own shores.[114] While the FTC might be able to use its Google Buzz consent

111. Eric Pfanner, *France Says Google Privacy Policy Likely Violates European Law*, N.Y. TIMES, Feb. 28, 2012, at B9. In a letter to Google, France's privacy agency, Commission Nationale de l'Informatique et des Libertés, alleged that Google had violated the European Directive on Data Protection by failing to disclose comprehensively what user data the company processed. *See* Letter from Isabelle Falque-Pierrotin, President, Commission Nationale de l'Informatique et des Libertés, to Larry Page, CEO, Google, Inc. (Feb. 27, 2012), *available at* http://www.cnil.fr/fileadmin/documents/en/Courrier_Google_CE121115_27-02-2012-EN.pdf.

112. Pfanner, *supra* note 111. The EU law in question, commonly referred to as the Data Protection Directive, Council Directive 95/46, 1995 O.J. (L 281) 31 (EC), has generally been seen as more rigorously protecting consumer privacy than the patchwork of American laws. *See, e.g.,* Julia M. Fromholz, *The European Union Data Privacy Directive*, 15 BERKELEY TECH. L.J. 471, 472 (2000).

113. Letter from Isabelle Falque-Pierrotin to Larry Page, *supra* note 111.

114. In October 2012, twenty-seven European data protection agencies wrote to Google asking for a change in the privacy policy in order to make Google's *actual* data protection practices clearer to users. The head of CNIL stated that, should Google fail to make appropri-

decree as the basis for an investigation, other similar cases might lack such justifications. Constraining the agency via the current unfairness test may be shortsighted since foreign consumer protection agencies have no qualms about investigating Google's behavior. Europe's investigation into Google's practices demonstrates that American regulators should also open similar inquiries, especially since it would be unfeasible for the website to operate in drastically different ways in one country versus another.[115] A unified international approach would avoid placing the burden of creating country-specific sites by indicating what terms of service would be generally appropriate to both American and European regulators. Seeking harmonization in an international regulatory approach, preferably via cooperation by international regulators, would ensure clearer expectations for users.

IV. FACEBOOK: CONNECTING "FRIENDS" FROM COLLEGES TO THE WORLD

A. *The Social Network*

In just eight years, Facebook has become the most popular online social network, ranking number one on Alexa's list of the most popular websites globally and number two within the United States.[116] But in that time, the site has become equally infamous for its privacy problems,[117] which remain especially relevant as the site continues its partnerships with other media and technology products such as the *Washington Post*, Spotify, and the *Guardian*.[118] With more partnerships likely on the horizon, Facebook could aggregate a vast amount of data on its users, from "Likes" to articles read to

ate changes, CNIL might file charges against Google. *See* Eric Pfanner & Kevin J. O'Brien, *Europe Presses Google to Change Privacy Policy*, N.Y. TIMES, Oct. 17, 2012, at B1.

115. A classic illustration of this difficulty in tailoring a website for different markets arose in the seminal case of *Yahoo! v. LICRA*. In that case, the International League against Racism and Anti-Semitism filed suit against Yahoo! in France after sending a cease-and-desist letter to Yahoo!'s California headquarters for violating French laws against the sale of Nazi objects. Yahoo! claimed it could not comply with the French court's order requiring Yahoo! to pay a fine of €100,000 per day if French nationals could access auction listings of items that were prohibited for sale under French law. Ultimately, Yahoo! was not fined for any violations of the court orders restricting its listings in France, but neither LICRA nor its partner in the suit, L'Union des Etudiants Juifs de France ("UEJF"), agreed to have the orders eliminated. *See* Yahoo! v. La Ligue Contre Le Racisme, 433 F.3d 1199 (9th Cir. 2006).

116. *Facebook.com Site Info*, ALEXA, http://www.alexa.com/siteinfo/facebook.com (last visited Oct. 21, 2012).

117. *See, e.g.*, Somini Sengupta, *Risk and Riches in User Data for Facebook*, N.Y. TIMES, Feb. 26, 2012, at B1.

118. *See* Margot Kaminski, *Reading Over Your Shoulder: Social Readers and Privacy Law*, 2 WAKE FOREST L. REV. ONLINE 13 (2012).

websites visited.[119] Moreover, Facebook came under criticism in 2011 for tracking users even *after* they had left the social network.[120]

Because of its high level of personalization, Facebook's trove of user data is arguably more valuable than Google's, such that an unexpected data leak would be potentially more damaging. First, Facebook users actively reveal their personal preferences on the site by adding "Likes"; posting links, photos, and videos; identifying locations where they have "Checked In"; and identifying their work and educational history. As a result, most Facebook users create a version of themselves online that reflects their personal history and important aspects of their personality. This "Facebook self" contains the exact kinds of data that marketers find so appealing—age, educational status, family structure, geographic location, product preferences, political leanings, and content curation—while eliding aspects of a personality that are not as commercially valuable (such as moral views, doubts, or emotional patterns).[121]

Due to the high value of its data, Facebook has been able to remain a free service by using advertising as its main source of revenue.[122] As advertising becomes targeted toward individual users, the valuable user data that Facebook retains allows advertisers to determine exactly which ads to send, not only within but possibly outside the site.[123] However, Facebook's policies on how it collects and manages user data have angered users and drawn criticism from advocacy groups.[124]

B. *From Criticism to Litigation: Beacon and the 2011 FTC Settlement*

One of the most prominent incidents concerning Facebook's privacy practices came in November 2007 with the announcement of the ill-fated

119. For further discussion on the "Like" button, *see infra* note 121.

120. *See* Jeff Ward-Bailey, *Facebook Tracking Now Under Federal Investigation*, CHRISTIAN SCI. MONITOR (Nov. 17, 2011), http://www.csmonitor.com/Innovation/Horizons/2011/1117/Facebook-tracking-now-under-federal-investigation.

121. The issue of "Like" buttons—where users can indicate their preference or support for certain businesses, comments, images, and other Facebook content—has been a fraught question. Recently, a district court held that Like buttons are not a form of First Amendment-protected speech. *See* Bland v. Roberts, 857 F. Supp. 2d 599 (E.D. Va. 2012), *appeal docketed*, No. 12-1671 (4th Cir. May 23, 2012). The increased use of Like buttons on Facebook affiliate sites creates interesting questions regarding notice, disclosure, and the privacy practices that apply to such buttons.

122. Emily Steel & Geoffrey A. Fowler, *Big Brands Like Facebook, but They Don't Like to Pay*, WALL ST. J., Nov. 2, 2011, at A1.

123. *See, e.g.*, Sengupta, *supra* note 117.

124. *See, e.g.*, Mark M. Jaycox & Rainey Reitman, *Facebook's (In)Conspicuous Absence from the Do Not Track Discussions*, ELEC. FRONTIER FOUND. DEEPLINKS BLOG (Mar. 15, 2012), https://www.eff.org/deeplinks/2012/03/facebooks-inconspicuous-absence-do-not-track-discussions-when-individual.

Facebook Beacon program.[125] Beacon was designed to send stories about Facebook users' activities *outside* the Facebook site into Facebook newsfeeds. For example, if a user bought a ticket on Fandango's website at www.fandango.com, that user's friends would see a story about her purchase on the main page of their Facebook account (currently known as the News Feed). Users complained when Facebook announced the Beacon program,[126] leading to its eventual shut down two years later, in November 2009.[127] The program also became the subject of a class action lawsuit, *Lane v. Facebook, Inc.*, which eventually settled.[128] In *Lane*, the plaintiffs alleged that Facebook had violated several state and federal laws, including the Electronic Communications Privacy Act, the Computer Fraud and Abuse Act, the Video Privacy Protection Act, California's Computer Crime Law, and the California Consumer Legal Remedies Act.[129] Facebook founder Mark Zuckerberg later admitted that the program was a "mistake."[130]

Like Google, Facebook has been targeted by American regulators for its privacy violations. In November 2011, the FTC announced a proposed settlement with the site.[131] In the final August 2012 settlement, the FTC prohibited Facebook from misrepresenting how it maintained the privacy or security of user data, as it had in the Beacon incident. The FTC settlement sent a clear signal to other online service providers to avoid Facebook's many missteps.[132] Indeed, Zuckerberg admitted the failure of the Beacon program in the settlement in an attempt to reassure Facebook users of the company's commitment to privacy.[133]

125. *See, e.g.*, Louise Story & Brad Stone, *Facebook Retreats on Online Tracking*, N.Y. TIMES, Nov. 30, 2007, at C1.

126. *See id.*

127. Chloe Albanesius, *Facebook Partners with Nielsen, Ditches Beacon*, PCMAG (Sept. 22, 2009, 1:07 PM), http://www.pcmag.com/article2/0,2817,2353156,00.asp.

128. Mark Milian, *What Facebook's Beacon Settlement Means for Those Involved*, L.A. TIMES (Dec. 10 2009, 10:36 AM), http://latimesblogs.latimes.com/technology/2009/12/what-is-facebook-beacon-settlement.html.

129. Complaint at 3–4, Lane v. Facebook, Inc., 2009 WL 3458198 (N.D. Cal Aug. 12, 2008) (No. 08-cv-3845 RS). Because the FTC Act does not allow for private rights of action, the plaintiffs could not file a claim under the FTC Act. *See, e.g.*, Days Inn of Am. Franchising, Inc. v. Windham, 699 F. Supp. 1581 (N.D. Ga. 1988).

130. Mark Zuckerberg, *Our Commitment to the Facebook Community*, THE FACEBOOK BLOG (Nov. 29, 2011, 9:39 AM), https://blog.facebook.com/blog.php?post=10150378701937131.

131. Facebook, Inc., Docket No. C-4365, File No. 092-3184 (Fed. Trade Comm'n 2011) (agreement containing consent order), http://www.ftc.gov/os/caselist/0923184/111129facebookagree.pdf.

132. Facebook, Inc., Docket No. C-4365, File No. 092-3184 (July 9, 2012) (decision and order), http://ftc.gov/os/caselist/0923184/120810facebookdo.pdf.

133. Zuckerberg, *supra* note 130.

The FTC settlement was based primarily on deceptiveness claims under Section 5 of the FTC Act, although the agency also relied in some respects upon the unfairness prong.[134] The settlement cited eight counts:

(1) Even when users restricted their information to a certain audience, third party apps that their friends used could gain access to their information.

(2) Facebook claimed in 2009 that it was giving users more control over their privacy, but information that users attempted to keep private, such as their Friends List, was made public.

(3) Facebook changed some information from private to public, thereby overriding users' choices and retroactively applying the change to previously collected information, which was an unfair act.

(4) Facebook apps could collect more information beyond what the app "needed to work," despite Facebook's statement that apps would only collect enough information to work properly.

(5) Facebook claimed that it would not share information with advertisers, but in some instances, when a user clicked on ads, that user's UserID was shared with advertisers.

(6) Despite creating a "Verified Apps" program designed to provide certain apps and developers with a certification of good practices, Facebook did not take additional steps when reviewing apps for the program—even though developers paid between $175 and $375 for the stamp of approval.

(7) Facebook said that when users deactivated accounts, all the content they had uploaded to Facebook would be deleted; however, the content that former users had uploaded could still be accessed by entering the URL into a web browser.

(8) Facebook did not accurately represent its compliance with the U.S.-EU Safe Harbor Framework.[135]

134. Press Release, Fed. Trade Comm'n, Facebook Settles FTC Charges that it Deceived Consumers by Failing to Keep Privacy Promises (Nov. 29, 2011), *available at* http://www.ftc.gov/opa/2011/11/privacysettlement.shtm [hereinafter Facebook Settlement].

135. *Id.*; Lesley Fair, *The FTC's Settlement with Facebook: Where Facebook Went Wrong*, On Guard Online (Nov. 29, 2011), http://onguardonline.gov/blog/ftc's-settlement-facebook-where-facebook-went-wrong. The U.S.-EU Safe Harbor Framework is an international effort to coordinate privacy protection standards. For more information, see

Several elements of the settlement agreement warrant examination. First, the number of claims that the FTC felt comfortable pursuing against Facebook demonstrates the volume of problematic practices in which the company engaged. One can only guess at how many practices Facebook engages in that would trouble consumers but that do not rise to the level of unfairness or deception. Moreover, the number of claims and their scope—covering user deactivation, application privacy, and overrides of user privacy preferences—indicates that the FTC takes its enforcement mission seriously vis-à-vis Facebook. As discussed above, the FTC has been frequently criticized for not pursuing as robust of an enforcement program as it might have.[136] Yet by evincing its willingness to examine different aspects of Facebook's architecture and privacy design, the FTC has sent a signal to private industry, consumer advocates, and the general public that it is serious about looking into Facebook's practices, and presumably into other companies' practices as well.

Most of the FTC's claims in the Facebook settlement were based on the deception prong under Section 5. The one claim based on unfairness, Claim 3, states that retroactively changing the privacy settings on user data *that users had actively selected* and overriding those preferences constituted an unfair act.[137] Of course, just because the FTC argues that the action was unfair does not mean that it meets the legal standard of unfairness under Section 5; a judge or jury would need to make that determination at trial. Yet the FTC would almost certainly not allege a claim in a complaint that it was not confident of winning.

As discussed above, under the three elements of unfairness as articulated in Section 5(n) of the FTC Act, the FTC must demonstrate that the act or practice causes or is likely to cause substantial injury to consumers, which is not reasonably avoidable by consumers or outweighed by other benefits.[138] Facebook's allegedly unfair practice is certainly likely to cause substantial injury to consumers, given that data they previously designated as private could be gathered by anyone with an Internet connection.[139] Such data, if not properly anonymized, could be used for any number of ends (including fraudulent financial transactions or identity theft) that could damage a consumer's reputation, credit score, or privacy.

U.S.-EU Safe Harbor Overview, EXPORT.GOV, http://export.gov/safeharbor/eu/eg_main_018476.asp (last visited Oct. 20, 2012).

136. *See, e.g.*, Claire Cain Miller, *F.T.C. Said to Be Near Facebook Privacy Deal*, N.Y. TIMES, Nov. 10, 2011, at B3.

137. Fair, *supra* note 135.

138. 15 U.S.C. § 45(n) (2011).

139. These types of data breaches are typically found to qualify as a substantial injury, given that financial fraud or identity theft is likely to result. *See, e.g.*, Thomas B. Leary, Comm'r, Fed. Trade Comm'n, Speech at the Wayne State University Law Review Symposium: Unfair Practices and the Internet (June 25, 2007), *available at* http://www.ftc.gov/speeches/leary/unfairness.shtm.

Applying the other prongs of the unfairness test, Facebook's retroactive change was certainly not reasonably avoidable by consumers, considering the lack of proper communication to users. Nor does there seem to be any benefit to changing data privacy settings that would outweigh the injury to consumers, especially absent consumer notice. Arguably, if Facebook had announced the change to users, it could more easily rebut the unfairness claim, but Facebook's direct contravention of user intent—without notice—creates an air of unfairness around the entire action.

C. *Post-Settlement Reactions and Future FTC Enforcement*

The FTC settlement with Facebook provoked a great deal of public debate. Most reactions were positive, pointing to a restatement of the FTC's commitment to protecting consumer privacy online.[140] Others were more measured, expressing optimism at the settlement and at the possibility of future government enforcement, but calling for stronger privacy regulation and consumer protection.[141] A few critics—perhaps most surprisingly Gawker—lambasted the FTC, labeling the settlement as insufficient and a kowtow to industry.[142] Although Gawker is more known as a gossip website than a consumer privacy advocacy organization, not all of its criticisms can be easily dismissed. It is obvious that Facebook could do more to protect user privacy. It could require users to actively opt in to make data publicly available or usable by Facebook in advertising. It could adopt "privacy by design," a principle that argues for including user privacy at the design stage of web and mobile product development, rather than as an afterthought once the products have been designed, tested, and implemented.[143] At the least, Facebook could clearly communicate to users how it utilizes their data, what its privacy policy actually means, and what changes it is making and why.

Yet all of these fairly obvious changes must be made by Facebook voluntarily, or perhaps under consumer or regulatory pressure. The FTC cannot unilaterally enforce them upon the company; nor can the agency, as discussed above, act as freely as other agencies in regulating industry.[144] But

140. *See, e.g.*, Somini Sengupta, *F.T.C. Settles Privacy Issue at Facebook*, N.Y. TIMES, Nov. 30, 2011, at B1.

141. *See, e.g.*, Kurt Opsahl & Rainey Reitman, *With FTC Settlement, Facebook Moves Closer to EFF Bill of Rights for Social Network Users*, ELEC. FRONTIER FOUND. DEEPLINKS BLOG (Nov. 29, 2011), https://www.eff.org/deeplinks/2011/11/ftc-settlement-facebook-moves-closer-eff-bill-rights-social-network-users.

142. *See, e.g.*, Ryan Tate, *Facebook Just Played the Government*, GAWKER (Nov. 29, 2011, 3:10 PM), http://gawker.com/5863493/facebook-just-played-the-government; *Fix FB Privacy Fail*, ELEC. PRIVACY INFO. CTR., http://epic.org/privacy/fixprivacyfail/noauth.php (last visited Mar. 18, 2012).

143. *See, e.g.*, *The Role of Privacy by Design in Protecting Consumer Privacy*, CTR. FOR DEMOCRACY & TECH. (Jan. 28, 2010), https://www.cdt.org/policy/role-privacy-design-protecting-consumer-privacy (last visited Mar. 18, 2012).

144. *See* discussion *supra* Part I.B.

unless (and until) the FTC receives greater enforcement authority from a grant by Congress, its abilities remain limited.

The question of whether the FTC *should* enforce with a heavier hand (assuming greater regulatory freedom) is an issue on which reasonable minds will differ. Examining Facebook's current privacy policy, following the settlement and the rollout of Facebook's Timeline feature (which displays all of a user's content on one page),[145] will illuminate whether or not Facebook has learned any valuable lessons regarding its policies toward users and the use of FTC authority to regulate Facebook practices.

Facebook's current privacy policy can be found at the bottom of its homepage, referred to as a "Data Use Policy."[146] It contains multiple components, including sharing procedures, information retrieval and use policies, third-party sharing, advertising practices, policies relating to minors, and others.[147] Interestingly, the main Data Use Policy page was not modified between September 2011—two months before the FTC settlement was announced—and June 2012.[148] Given the changes that Facebook was required to make as a result of the settlement, it is surprising that they would not inform users of the changes for over half a year.

One critical element of Facebook's privacy policy is the explanation of how the site uses the information it obtains from users. In its Data Use Policy, Facebook claims:

> We don't share information we receive about you with others unless we have:
>
> - received your permission;
> - given you notice, such as by telling you about it in this policy; or

145. *See, e.g.*, Jill Duffy, *12 Things You Should Know About Facebook Timeline*, PCMAG (Jan. 25, 2012), http://www.pcmag.com/article2/0,2817,2393464,00.asp. One relevant consideration might be the way in which Facebook implemented its Timeline feature. Originally, users could opt in to Timeline, and once they did they would have seven days to review their old data and delete old posts and content that they might not want to be visible to all users. *Id.* By late 2012, Facebook had moved most users to Timeline, but still allowed the seven-day curation period. *See* Samantha Murphy, *Facebook Timeline Coming to Most Users by the Fall*, MASHABLE (July 31, 2012), http://mashable.com/2012/07/31/facebook-timeline-coming-fall/.

146. *Data Use Policy*, FACEBOOK, https://www.facebook.com/about/privacy/ (last visited Mar. 18, 2012).

147. *Id.*

148. *Id.*

- removed your name or any other personally identifying information from it.[149]

These statements lead a reasonable consumer to believe that user data will be shared with other parties only if a user opts in or receives notice, or if the data being shared has been anonymized to remove sensitive information. This is exactly the sort of statement that might lead to an unfairness claim if demonstrably inaccurate, as it is similar to the unfairness claim from the FTC settlement, which concerned the modification of user expectations and choices without notice.[150] Presumably, a similar modification to these "sharing standards" without notice would point toward a successful unfairness claim.

Facebook also claims that when users click on advertisements, those clicks are recorded anonymously. Advertisers do not know to whom their advertisements are delivered, nor who saw or clicked on those ads.[151] As with how user data is used, a violation of user expectations on these statements—especially a retroactive violation, by which Facebook revealed older user data concerning advertisements—could support an unfairness claim.

D. *Privacy Audits and Public Disclosure*

Examining Facebook's privacy policies for evidence of unfair acts requires a certain amount of supposition. In part, this is because of the difficult standards of unfairness; it also stems from Facebook's opacity concerning how it uses the data it collects from users. Put simply, Facebook's history of obfuscation and misleading statements suggests that one cannot take the company at its word—especially when that word is expressed in a privacy policy or a press release concerning Facebook's privacy practices. The record of controversies, campaigns, and cases have so tarnished Facebook's public image on privacy that a reasonable consumer will likely be skeptical of Facebook's privacy promises.[152]

Whether one is confident that the FTC will be keeping a close eye on Facebook in the near future depends on one's opinion on the efficacy of pri-

149. *Data Use Policy*, FACEBOOK, https://www.facebook.com/about/privacy/your-info#howweuse (last visited Mar. 18, 2012).

150. Facebook Settlement, *supra* note 134.

151. *Data Use Policy*, *supra* note 149.

152. In some instances, user skepticism about Facebook's privacy settings may in fact lead to "false alarms" about privacy violations. *See, e.g.*, Colleen Taylor, *Update: Facebook Confirms No Private Messages Appearing on Timeline. They're Old Wall Posts*, TECHCRUNCH (Sept. 24, 2012), http://techcrunch.com/2012/09/24/reports-facebook-users-seeing-private-messages-pre-2009-showing-up-on-timelines-as-posted-by-friends/ (describing how some users thought that private messages were being posted on user profiles, but in actuality they were merely old public posts). *See also* danah boyd, Keynote Speech at World Wide Web Conference 2010: Privacy and Publicity in the Context of Big Data (Apr. 29, 2010), *available at* http://www.danah.org/papers/talks/2010/WWW2010.html (discussing Facebook's privacy hiccups).

vacy audits. A third-party examiner will conduct the audits for the next twenty years. This long time period points to both the serious nature of the violations and the FTC's commitment to holding Facebook accountable. But the results of the audits will probably not be made public,[153] and it will be difficult to know whether Facebook is actually serious about its commitment to privacy—despite Zuckerberg's reassuring statements.

Privacy audits are an important way to enforce a settlement and encourage "good behavior" from a company; they serve as a sort of long-term probationary period. But the audits—like the investigations—are not public, and thus their deterrent effect is not as large as it could be. The FTC could increase the awareness of the audits and their effectiveness by describing the general audit process via a publicly posted, electronically available press release.[154] This would give the audits more force and would signal to consumers that their privacy is being protected, and a press release could be written to preserve the confidentiality of any private information or trade secrets that an audited company needs to protect. The current audit system, in which audits seem to be less important in deterring bad consumer practices than the actual complaints and settlements, does not adequately demonstrate the FTC's commitment to privacy protection.[155] Because audits are not made public or even discussed beyond the initial announcement in a consent decree, they seem obscure to the general public.

There is something unsatisfying about the result in the latest skirmish between the FTC and Facebook. Since the settlement mainly provides for increased future oversight, it is hard to proclaim it a regulatory victory. Much will depend on the vigor and effectiveness of the privacy audits and the FTC's response. Certainly, public disclosure on the results of those audits would pressure Facebook into following both the letter and the spirit of privacy law. There are strong reasons for keeping audit results confidential—most

153. In October 2012, the Electronic Privacy Information Center ("EPIC") obtained the initial privacy assessment submitted to the FTC by Google under the terms of the consent degree via a Freedom of Information Act ("FOIA") request. *See* Letter from Dione J. Stearns, Assistant Gen. Counsel, Fed. Trade Comm'n, to Ginger McCall, Elec. Privacy Info. Ctr. (Sept. 25, 2012), *available at* http://epic.org/privacy/ftc/googlebuzz/FTC-Initial-Assessment-09-26-12.pdf. However, the FTC invoked several FOIA exceptions in release of the letter, which EPIC planned to challenge. *See Federal Trade Commission*, ELEC. PRIVACY INFO. CTR., http://epic.org/privacy/internet/ftc/ (last visited Nov. 16, 2012). Relying upon FOIA requests in order to obtain the results of privacy audits is an inefficient method of raising public awareness, as citizens, journalists, and non-profit organizations would need to actively seek the audits from the FTC, rather than relying upon the agency itself to release them.

154. The Commission already makes most of its consent decrees and settlements publicly available via its online Newsroom. *Newsroom*, FED. TRADE COMM'N, http://www.ftc.gov/opa/index.shtml (last visited Nov. 16, 2012).

155. For example, there is the suggestion that Google violated its own settlement agreement when privacy setting circumventions in Apple's Safari browser were discovered. *See, e.g.*, James Temple, *FTC Chief Weighs in on Online Privacy Report*, S.F. CHRON., Apr. 27, 2012, at D1. If so, the privacy audits did not preclude the agency from engaging in practices prohibited by the FTC settlement.

obviously, to respect the privacy rights of Facebook itself. But in order to convince consumers that it is serious about preventing Facebook from once again acting unfairly, the FTC needs to show that it has taken tangible action in regulating the social network.

V. TWITTER: MICROBLOGGING AND INTERACTION ON AN UNPRECEDENTED SCALE

A. *140 Characters or Fewer*

Twitter, the microblogging social network service, has not achieved the high traffic or pervasiveness of Facebook and Google for most Internet users, in part due to its relative youth compared to the older companies. Currently, the site is ranked number eight on the Alexa global ranking.[156] Unlike Facebook and Google, Twitter provides one service: the ability to microblog by posting updates to one's feed with a maximum length of 140 characters. Another key difference lies in the ways in which individuals can access and interact via the service; Twitter users can post updates and read others' Tweets by using the website interface, or use third-party clients (both official and unofficial). Google and Facebook, by contrast, get much of their traffic through their main websites.

Twitter's main source of data comes from its users, who update their Twitter feeds with a vast amount of information. Twitter feeds can contain geolocation, user-created photos and videos, and information on an individual's preferences and brand loyalties. Twitter users also select other users to follow on the service, thereby providing Twitter with information about which celebrities and public figures they find interesting, and which users are within their personal social networks.

Because Twitter is a younger service than Facebook and Google, it has had fewer years to experience and rebound from privacy setbacks and controversies. Twitter's privacy problems have not been as prominent as the Google Buzz or Facebook Beacon episodes, but the FTC announced its Twitter settlement prior to announcing the Google and Facebook settlements.[157] The Twitter settlement was finalized in March 2011.[158] This Section investigates the settlement and examines Twitter's recent privacy lapses to determine the necessity of current and future enforcement.

156. *Twitter.com Site Info*, ALEXA, http://www.alexa.com/siteinfo/twitter.com (last visited Oct. 21, 2012).

157. The FTC announced its proposed settlement with Twitter in June 2010. *See* Press Release, Fed. Trade Comm'n, Twitter Settles Charges that it Failed to Protect Consumers' Personal Information; Company Will Establish Independently Audited Information Security Program (June 24, 2010), *available at* http://www.ftc.gov/opa/2010/06/twitter.shtm.

158. Press Release, Fed. Trade Comm'n, FTC Accepts Final Settlement with Twitter for Failure to Safeguard Personal Information (Mar. 11, 2011), *available at* http://www.ftc.gov/opa/2011/03/twitter.shtm.

B. *The FTC's Complaint and Final Settlement*

1. The Initial Complaint

The FTC alleged two counts of deceptive practices against Twitter in its complaint:[159] (1) that Twitter did not use reasonable and appropriate security measures to prevent unauthorized access to nonpublic information, despite its security claims; and (2) that Twitter did not use reasonable and appropriate security measures to honor the privacy choices made by users, again in contrast to its assertions.[160] The complaint included evidence of unauthorized account use by intruders in order to demonstrate how Twitter falsely made claims about its security practices.[161] On multiple occasions between January and May 2009, intruders were allegedly able to reset user passwords based on access to Twitter employee accounts. As a result, intruders were able to modify accounts and gain access to nonpublic information.[162] The FTC used its deception power to seek an enforcement action, claiming that Twitter's security was far less robust than asserted. If Twitter had taken security steps akin to what it stated on its website, the FTC argued, the intruders would not have been able to so easily gain access to user accounts.[163]

While the Twitter settlement is commendable for its censure of inadequate security practices, it also illustrates the limitations of relying upon the deception prong of Section 5 to regulate website practices. Though the violations described in the complaint specifically concern security rather than privacy, they hold implications for user privacy since the security breach resulted in easy access to user data. The FTC had to rely upon security breaches caused by third parties that exposed vulnerabilities, rather than Twitter's own actions. It did not regulate typical Twitter practices, but instead reacted to a shortcoming demonstrated by unauthorized access.

Alternatively, the FTC could have brought an unfairness claim against Twitter for its business practices in this case. As discussed *supra* in Part II, a three-factor test applies in determining whether a business practice or act is unfair: the act or practice must cause or be likely to cause (1) substantial injury to consumers which is (2) not reasonably avoidable by consumers or (3) outweighed by other benefits.[164] In this case, the practice—Twitter's internally inadequate security measures—is certainly likely to cause substantial injury to consumers, if identifiable private information was disclosed to third parties without user consent. Since Twitter users can exchange direct private messages with other users and post nonpublic

159. Twitter, Inc., Docket No. C-4316, File No. 0923093, at 5 (Fed. Trade Comm'n June 24, 2010) (complaint), http://www.ftc.gov/os/caselist/0923093/100624twittercmpt.pdf.
160. *Id.*
161. *Id.* at 3–5.
162. *Id.*
163. *Id.*
164. 15 U.S.C. § 45(n) (2011).

tweets, some sensitive user information must have been disclosed as a result of Twitter's inadequate practices.

Twitter's practices also meet the second and third prongs of the unfairness test. Consumers could not have avoided the inadequate security practices that Twitter employed, because it would have been impossible for any consumer to know the exact contours of Twitter's internal security. There also was no clear benefit to consumers based on Twitter's practices, much less a benefit that outweighed Twitter's practices; the lack of rigorous security could only prove detrimental to users. Therefore, all three elements of the current unfairness test seem to be met.

It is unclear why the FTC did not allege an unfairness claim against Twitter. As discussed *supra*, the agency seems to prefer to litigate under the deception prong of Section 5 rather than the unfairness prong, in part because of the clearer standards of deception and the more robust legal precedent. Of course, to some extent this is a vicious cycle: if the agency prefers to use deception rather than unfairness in cases, the standards of unfairness will remain fuzzier than those of deception, and there will be less unfairness case law to rely upon. While *Sears Holdings* and the more recent case *FTC v. Neovi, Inc.* point to a renewed commitment to unfairness litigation by the agency, in the online privacy realm there are distressingly few recent examples of successful unfairness cases.[165]

2. The Final Settlement

The final FTC settlement with Twitter did not materially alter any of the pleadings from the initial complaint.[166] Under the terms of the settlement, Twitter cannot mislead consumers regarding its security practices for twenty years, and must establish a comprehensive information security program, to be audited every other year for ten years.[167]

The effectiveness of privacy audits notwithstanding, this particular case in large part mirrors the Facebook analysis.[168] The Twitter complaint and order are narrower in scope than the Facebook order, perhaps because this complaint was the first to be brought against a social network and paved the way for future, broader enforcement actions against Facebook and

165. *See* Fed. Trade Comm'n v. Neovi, Inc., 604 F.3d 1150 (9th Cir. 2010). In *Neovi*, the FTC used its unfairness authority to bring a case against Qchex, a service that allowed for automated creation and mailing of checks. Qchex was governed by Neovi, Inc. The FTC alleged that Qchex's unsecured systems led to widespread fraud and were unfair as defined by Section 5. The use of the unfairness prong in a case that concerned over $400 million in fraudulent checks illustrates that the FTC was willing to use its lesser-exercised unfairness authority in a high-profile case. *See id.*

166. Twitter, Inc., Docket No. C-4316, File No. 0923093 (Fed. Trade Comm'n Mar. 2, 2011) (decision and order), http://www.ftc.gov/os/caselist/0923093/110311twitterdo.pdf.

167. *See id.*; Press Release, Fed. Trade Comm'n, *supra* note 158.

168. *See supra* Part IV.

Google.[169] Since in recent decades the agency has taken a conservative approach to its mission, the order's narrowness compared to subsequent actions makes sense; to some extent, the Twitter action "opened the door" to later cases.[170] The final settlement did not provide for monetary damages,[171] which could have been helpful in deterring future conduct by Twitter that might violate Section 5. Nonetheless, the public nature of the settlement sent a clear message to other web service operators.[172]

C. *Twitter Post-Settlement: Mobile Privacy and Current Policies*

1. We Know Who Your Friends Are

In the wake of the settlement, Twitter has reformed its practices concerning internal security,[173] but the company has remained in the spotlight for privacy issues. In February 2012, several news outlets reported that Twitter's smartphone app retained user data without explicitly informing users about this practice.[174] When users tapped on the "Find Friends" button within the app, Twitter would download the entire address book from the phone, storing the data for eighteen months.[175]

Crucially, Twitter did not blatantly violate its terms of service by retaining its users' address book data.[176] The terms apparently indicated that certain types of data would be retained for eighteen months, but did not state explicitly *which* data would be stored, or that Twitter would download users' address books in this way.[177] Twitter also provided users the ability to remove their personal address book data from Twitter's servers.[178]

Because Twitter *did* disclose that some data would be retained for eighteen months, but used vague language about how it decided what data would be stored for that length of time, the FTC would likely be unable to pursue a claim under the deception prong of Section 5. Strictly speaking, Twitter did not *deceive* its users; it merely did not explain its practices as clearly as it could have. Yet the company's actions—and its lack of clarity surrounding its practices until an issue publicly materialized—demonstrate

169. *See* discussion *supra* Parts II–III.
170. *See* discussion *supra* Part IV.B–C.
171. Twitter, Inc., Docket No. C-4316, File No. 0923093 (Fed. Trade Comm'n Mar. 2, 2011) (decision and order), http://www.ftc.gov/os/caselist/0923093/110311twitterdo.pdf.
172. *See, e.g.*, Caroline McCarthy, *Twitter, FTC Reach Agreement on Security*, CNET (June 24, 2010, 11:31 AM), http://news.cnet.com/8301-13577_3-20008743-36.html.
173. *See, e.g., id.*
174. *See, e.g.*, David Sarno, *Twitter Stores Full iPhone Contact List for 18 Months, After Scan*, L.A. TIMES (Feb. 14, 2012), http://articles.latimes.com/2012/feb/14/business/la-fi-tn-twitter-contacts-20120214.
175. *Id.*
176. *Id.*
177. *Id.*
178. *Id.*

at best carelessness, and at worst a derogation of responsibilities under the March 2011 settlement.

Because the company's privacy policy statements appear to forestall any potential deception claim, unfairness would seem to be the sole method of FTC regulation and enforcement of this particular Twitter practice. Under a traditional unfairness analysis, the FTC would need to demonstrate that Twitter's practices harmed or were likely to harm consumers. Without further investigation into how Twitter collected address book data and whether it transmitted that data to third parties, it is impossible to determine if the first prong of the unfairness test has been met. Under the terms of the consent agreement, however, one could argue that Twitter violated its preexisting obligations to the FTC. For example, the FTC consent decree prevents Twitter from misrepresenting "in any manner, expressly or by implication, the extent to which respondent maintains and protects the security, privacy, confidentiality, or integrity of any nonpublic consumer information."[179]

The second and third elements of the unfairness test are more easily met. Consumers had no way to avoid Twitter's collection of data, and the company itself admitted that the policy was not clear.[180] It is theoretically true that consumers could have avoided using Twitter's smartphone mobile app, thereby preventing Twitter from retaining address book data. Yet it was not evident to Twitter users that the app retained any data at all. Thus, there would be no apparent reason for consumers to avoid using the app, given that the behavior they would be attempting to avoid was not obvious.[181]

Finally, there does not seem to be any benefit to consumers as a result of Twitter's address book retention policy. Users already have the data that Twitter retains on their phones, and, should they choose to rerun the Find Friends tool, Twitter would not need to retain any data in order to allow the Find Friends tool to operate. Overall, the mobile privacy controversy would at least seem to warrant further FTC investigation. Yet the current understanding of the unfairness standard might cramp the agency's ability to investigate, even under the broad terms of the consent decree.

2. Twitter's Current Privacy Policy

In the aftermath of the address book controversy, Twitter pledged to modify its privacy policy to more clearly establish what data was being col-

179. Twitter, Inc., Docket No. C-4316, File No. 0923093, at 2 (Fed. Trade Comm'n Mar. 2, 2011) (decision and order), http://www.ftc.gov/os/caselist/0923093/110311twitterdo.pdf.

180. *See, e.g.*, Sarno, *supra* note 174.

181. The differences between mobile and desktop applications may also demonstrate that consumer expectations vary depending on the type of device used. *See* Angelique Carson, *At FTC Event, Experts Agree There's Work to Be Done on Mobile Privacy Disclosures*, INT'L ASS'N OF PRIVACY PROFESSIONALS (June 18, 2012), https://www.privacyassociation.org/publications/2012_06_14_at_ftc_event_experts_agree_theres_work_to_be_done_on_mobile.

lected from users, how such data was being collected, and for how long.[182] At present, Twitter does not claim to store any personal data as part of the "Log Data" that it retains for eighteen months; rather, Log Data consists of information regarding the devices and services used to access the site, rather than personal information about the user.[183]

Twitter also states in its privacy policy that it dictates how third parties use personal data.[184] As a result, a user could reasonably assume that any data transferred to a third party would be treated in largely the same way that Twitter would treat such data. If that assumption turned out to be incorrect, a case could certainly be made for unfairness enforcement against Twitter and any third parties that received Twitter user data.

D. *Openness and Certainty in the Twittersphere*

Much of the analysis of Twitter's practices and the possibility of claims remain suppositional. As with Facebook and Google, it can be frustratingly difficult to parse what Twitter says it does and reconcile those claims with the scandal du jour. Twitter's attempt to express its privacy policy in concise, plain English deserves credit for avoiding lengthy legalese. Yet by stripping down its privacy policy, Twitter has made it difficult to determine exactly what it does with user data—obfuscating the transparency that the clear language was designed to effect.

Because the FTC does not publicize the results of privacy audits or its investigations, consumer advocates can only hope that the agency has been addressing its troubling practices vigorously. The Twitter settlement agreement—although not as broad as Facebook's—certainly provides the FTC with the tools to ensure that inappropriate practices, like the address book data retention issue, receive full attention from the agency. Whether the agency actually uses the tools at its disposal to investigate Twitter—or other technology companies, for that matter—will be difficult to determine in the immediate future.

CONCLUSION: BROADER UNFAIRNESS AUTHORITY ON THE HORIZON?

The three examples of Google, Facebook, and Twitter demonstrate the information asymmetries in the user/website relationship pertaining to online privacy. Much of the analysis requires assumptions about site practices and close readings of privacy policy language that may or may not accurately describe the actual practices of websites.

Years of self-regulation have failed to create an industry standard of privacy by design, opt-in sharing provisions, or other principles that would

182. *See, e.g.*, Sarno, *supra* note 174.

183. *Twitter Privacy Policy*, TWITTER, https://twitter.com/privacy (last visited Mar. 31, 2012).

184. *Id.*

more effectively protect consumers. Web service providers consistently remain in the news for breaches involving user data.[185] The status quo has been plainly insufficient in protecting user privacy, just as the current regulatory tools available to the FTC have been inadequate to ensure that companies are deterred from violating reasonable user privacy expectations.

In early 2012, President Obama announced a renewed government interest in protecting consumer privacy.[186] The President argued "American consumers can't wait any longer for clear rules of the road that ensure their personal information is safe online."[187] He also claimed that "[b]y following [the proposed] blueprint, companies, consumer advocates and policy makers can help protect consumers and ensure the Internet remains a platform for innovation and economic growth."[188]

The President's statement prioritizes the use of clear rules, but does not place those rules in opposition to innovation or the growth of an important economic sector. By arguing that government and industry can work cooperatively, rather than in adversarial debate, the President has signaled that further regulation need not take the form of litigation. The FTC has historically employed policy levers to achieve its regulatory goals, and the White House report on its proposed Consumer Privacy Bill of Rights relies upon and encourages Congress to expand the FTC's regulatory authority.[189] As contemplated by the White House, Congress would expand that authority in

185. In October 2012, for example, Bogomil Shopov, a Bulgarian blogger and activist announced that he had purchased a database of Facebook users' names, user IDs, and email addresses for five dollars. While some or most of that data was publicly available, Shopov claimed that his ability to buy so much valuable user data demonstrated Facebook's failure to securely protect its users' data. *See* Andy Greenberg, *Facebook Investigating How Bulgarian Man Bought 1.1 Million Users' Email Addresses for Five Dollars*, FORBES (Oct. 25, 2012, 4:39 PM), http://www.forbes.com/sites/andygreenberg/2012/10/25/facebook-investigating-how-bulgarian-man-bought-1-1-million-users-email-addresses-for-five-dollars/.

186. Edward Wyatt, *White House, Consumers in Mind, Offers Online Privacy Guidelines*, N.Y. TIMES, Feb. 23, 2012, at B1.

187. Press Release, White House, We Can't Wait: Obama Administration Unveils Blueprint for a "Privacy Bill of Rights" to Protect Consumers Online (Feb. 23, 2012), *available at* http://www.whitehouse.gov/the-press-office/2012/02/23/we-can-t-wait-obama-administration-unveils-blueprint-privacy-bill-rights.

188. *Id.*

189. WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY 36 (2012), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf [hereinafter CONSUMER DATA PRIVACY]. In the report, the White House emphasized the importance of transparency, respect for context, security, access and accuracy, focused collection, and accountability as companies continue to collect information from consumers. *See* Press Release, White House, *supra* note 187. The White House also specifically contemplated strong FTC enforcement in order to further these consumer goals, either through existing statutory grants or through expansion of the FTC's regulatory power. *See* CONSUMER DATA PRIVACY, *supra*, at 36.

order to uphold the Consumer Privacy Bill of Rights, using both its deception and unfairness regulatory powers.[190]

The White House's express identification of unfairness as appropriate in this space provides an acknowledgement from the government that unfairness enforcement can and should be used to regulate websites' privacy practices. By using the unfairness doctrine as a regulatory strategy, the FTC can extend its reach and create a more specific understanding of what unfairness means. In its March 2012 final report on protecting consumer privacy, the FTC expressly acknowledged that increased regulation of personal privacy rights would require use of the unfairness prong.[191] It remains to be seen exactly how the FTC will create and define a new or revised approach to unfairness regulation for online privacy, but its commitment is a promising sign.[192] The September 2012 announcement that the FTC has used its unfairness authority to file complaints against a software company and seven rent-to-own franchises for privacy invasions demonstrates that the agency is ready to use its unfairness authority more actively to pursue violations of personal privacy.[193]

In his dissenting statement to the report, FTC Commissioner J. Thomas Rosch argued that the Commission's report would require a vastly expanded understanding of the unfairness prong.[194] He disagreed with the proposal to expand the unfairness authority, claiming " 'Unfairness' is an elastic and elusive concept. What is 'unfair' is in the eye of the beholder."[195] Rosch identified this supposed lack of specificity as contrary to the motivation behind the 1980s policy statements.[196]

---

190. *Id.* at 27 n.32.

191. FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS 73 (2012).

192. In the report, the FTC called for Do No Track Legislation, indicating that it understood the importance of consumer choice with regard to tracking. *See* Tanzina Vega & Edward Wyatt, *U.S. Agency Seeks Tougher Consumer Privacy Rules*, N.Y. TIMES, Mar. 27, 2012, at A1.

193. *See* Press Release, Fed. Trade Comm'n, FTC Halts Computer Spying (Sept. 25, 2012), *available at* http://www.ftc.gov/opa/2012/09/designware.shtm. In the case, a software firm, DesignerWare, created software that allowed the rent-to-own companies to spy on their customers without disclosure or consent after renting laptops. The software allowed the companies to track consumers via webcams, geolocation, and keystroke monitoring. In the complaint, the Commission asserted that DesignerWare's conduct was unfair because it caused or was likely to cause substantial injury to consumers without the possibility of avoidance or a countervailing benefit. DesignerWare, LLC, File No. 1123151, at 5, 7 (Fed. Trade Comm'n 2012) (complaint), http://www.ftc.gov/os/caselist/1123151/designerware/120925designerwarecmpt.pdf. The traditional definition of unfairness was not expanded in this case, but merely applied to a data privacy case, demonstrating the FTC's ability and willingness to use its unfairness authority against privacy invasions.

194. FED. TRADE COMM'N, *supra* note 191, at C-3.

195. *Id.*

196. *Id.* at C-4.

Rosch's argument that the FTC claimed it would not rely upon intangible harm in an unfairness case is accurate,[197] but his reliance upon a policy statement that was crafted as a response to political pressure is surprising and somewhat misguided. It is certainly true that the FTC report contemplates a shift—perhaps even a radical shift—in the agency's position on its own unfairness authority. Yet the policy statements were arguably an equally radical shift at the time they were written, created out of political necessity. Similarly, the new approach contemplated by the report comes in response to a new technological reality. While the policy statements may have been expedient for their era, they provide an inadequate regulatory tool for current business practices. The FTC's willingness to acknowledge that times have changed proves the agency's awareness that the current digital environment requires a modern approach to consumer protection. As a result, consumers may still have hope that their data may one day soon be used fairly.

197. *Id.*