Vol 25, No. 2
Fall 2016

The Journal of the Antitrust, UCL and Privacy Section of the State Bar of California

FTC PRIVACY AND DATA SECURITY ENFORCEMENT AND GUIDANCE UNDER SECTION 5

By Alexander E. Reicher and Yan Fang[1]

I. INTRODUCTION

Section 5 of the FTC Act does not itself mention privacy or data security, yet it is the legal basis for well over a hundred Federal Trade Commission privacy and data security enforcement actions. The Commission has used the broad language of Section 5—which prohibits "unfair or deceptive acts or practices," among other things—to hold individuals and companies accountable for everything from broken privacy and data security promises to "unfair" collection of personal information. To better understand the contours of the FTC's privacy and data security enforcement under Section 5, this article examines the agency's litigated cases, public settlements, and guidance materials. This article's modest purpose is to serve as an introduction to some of those materials. It proceeds in four sections. The balance of Section I provides an overview of FTC privacy and data security enforcement and guidance. Section II addresses FTC privacy enforcement and guidance under Section 5, including the agency's early privacy actions and those involving social networks, internet tracking, browser toolbars, cookies and behavioral advertising, mobile devices, data brokers, and the misappropriation of consumer data. Section III discusses FTC data security enforcement and guidance under Section 5, including the agency's recent data security litigation and enforcement actions that help define "reasonable" data security. The article concludes in Section IV.

A. Enforcement

In its privacy and data security actions, the Commission has used its Section 5 authority to investigate and file complaints against companies and individuals for privacy and data security violations that are "deceptive," "unfair," or both. Section 5 of the FTC Act states, in relevant part, that the Commission is "empowered and directed to prevent persons, partnerships, or corporations"—excluding certain types of entities, such as banks and credit unions, as well as certain activities such as common carrier activities—"from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce."[2]

A deceptive act or practice under the FTC Act is (1) a representation, omission, or practice (2) that is likely to mislead consumers acting reasonably in the circumstances and

---

1 Alexander E. Reicher is an associate with Latham & Watkins LLP and served as an attorney in the Federal Trade Commission's Western Regional Office in San Francisco from 2015 to 2016. Yan Fang is a Ph.D. student in the Jurisprudence and Social Policy Program at the University of California, Berkeley. She previously served as an attorney in the Federal Trade Commission's Western Regional Office in San Francisco from 2013 to 2016. The authors thank Thomas Dahdouh for his comments on an earlier version of this article. The views expressed in this article are solely those of the authors.

2 15 U.S.C. § 45(a)(2) (2012).

(3) that is material.[3] An unfair act or practice is one that (1) causes or is likely to cause substantial injury to consumers, (2) is not reasonably avoidable by consumers, and (3) is not outweighed by countervailing benefits to consumers or to competition.[4] Though early privacy and data security cases focused on deception, the FTC has increasingly used its unfairness authority to bring cases in the areas of privacy and data security.[5]

In addition to the FTC Act, the FTC also enforces a number of other privacy and data security laws, including the following (among others):

- Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act)[6] and the corresponding CAN-SPAM Rule;[7]
- Fair Credit Reporting Act (FCRA)[8] and a number of corresponding rules;
- Gramm-Leach-Bliley Act (GLBA)[9] and the corresponding Privacy of Consumer Financial Information Rule (Financial Privacy Rule)[10] and Standards for Safeguarding Customer Information (Safeguards Rule);[11] and
- The Children's Online Privacy Protection Act (COPPA)[12] and the corresponding Children's Online Privacy Protection Rule.[13]

The FTC investigates companies and individuals whose conduct may violate Section 5 or a specific statute or rule that the agency enforces. In privacy and data security investigations, the Commission has the authority to issue civil investigative demands (CIDs) for documents, interrogatory responses, and "tangible things," and to compel individuals and companies to attend investigational hearings, which are similar to depositions.[14]

FTC investigations may lead to one of several outcomes: (1) the agency's decision to close the investigation, (2) a settlement between the FTC and the target of the investigation, (3) the agency's filing of an administrative complaint, or (4) the agency's

---

3 Letter from James C. Miller III, Chairman, FTC, to Hon. John D. Dingell, Chairman, House Comm. on Energy & Commerce 1-2 (Oct. 14, 1983), *available at* https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf.

4 15 U.S.C. § 45(n); *see also* Letter from FTC Comm'rs to Sen. Wendell H. Ford & Sen. John C. Danforth (Dec. 17, 1980), *available at* https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness.

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

6 15 U.S.C §§ 7701-7713.

7 16 C.F.R. § 316.

8 15 U.S.C. §§ 1681-1681x.

9 15 U.S.C. §§ 6801-6809 and 6821-6827.

10 16 C.F.R. § 313.

11 16 C.F.R. § 314.

12 15 U.S.C. §§ 6501-6506.

13 16 C.F.R. § 312.

14 15 U.S.C. § 57b-1.

filing of a complaint in federal district court. The Commission has resolved the majority of its publicly announced privacy and data security investigations through consent order settlements, but more recently, has filed three complaints, one in federal court and two before its administrative tribunal.

B. Guidance

In addition to enforcement, the Commission has issued a number of reports and guides for businesses on privacy and data security topics. These guidance documents, written by FTC staff and occasionally approved by the FTC's commissioners, outline how to comply with various privacy laws or present the Commission's view of industry best practices.

The Commission's 2012 report *Protecting Consumer Privacy in an Era of Rapid Change*[15] (hereinafter "*Protecting Consumer Privacy*") is among the more significant FTC guidance on privacy and data security matters. Approved by the FTC's commissioners in a 3-1 vote, *Protecting Consumer Privacy* offers a framework "intended to articulate best practices for companies that collect and use consumer data."[16]

The report's privacy framework centers around three principles. First, "[c]ompanies should promote consumer privacy throughout their organizations and at every stage of the development of their products and services"—so-called "privacy by design."[17] Second, "[c]ompanies should simplify consumer choice" when it comes to choices about a company's collection and use of consumer data.[18] Finally, "[c]ompanies should increase the transparency of their data practice."[19] While the report makes specific recommendations under each of these privacy principles, the Commission clarified that these recommendations may go beyond the existing requirements under the privacy laws.[20]

The report also offers guidance on data security, including the recommendation that companies approach privacy by design by creating substantive and procedural protections. Substantive protections center on reasonableness, including reasonableness in the collection and use of data, in its retention and disposal, and in its security.[21] Procedural protections focus on integrating substantive privacy protections into an organization's everyday practices.[22]

---

15 Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers (2012), *available at* https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

16 *Id.* at 1.

17 *Id.* at 22.

18 *Id.* at 35.

19 *Id.* at 60.

20 *Id.* at iii.

21 *Id.* at 23-30.

22 *Id.* at 30-32.

C. Personally Identifiable Information and Sensitive Personal Information

Though some of the Commission's settlements define personally identifiable information or PII,[23] the agency acknowledged in its 2012 *Protecting Consumer Privacy* report that "the traditional distinction between PII and non-PII has blurred" and suggested that "it is appropriate to more comprehensively examine data to determine the data's privacy implications."[24] In that report, the Commission stated that its privacy framework applies to "consumer data that can be reasonably linked to a specific consumer, computer, or other device" rather than to particular categories of PII.[25]

For both privacy and data security, the FTC has stated that it expects businesses to pay particular attention to protecting "sensitive personal information," which it has defined, "at a minimum," as data about children, financial and health information, Social Security numbers, and precise geolocation data.[26] Some of the privacy and data security statutes and rules enforced by the agency also provide specific definitions of protected information. For example, the Children's Online Privacy Protection Rule applies to online contact information, screen names, certain geolocation information, and "persistent identifiers," which can be used to recognize a user over time and across different online services.[27] In recent reports, the FTC has also highlighted that biometric data[28] and data collected through the "Internet of Things"[29] may pose heightened privacy and physical safety concerns.

* * *

---

23 *See, e.g., In re Geocities*, 127 F.T.C. 94, 122 (1999) (decision and order) (defining "Personal identifying information" as information that includes but is not limited to "first and last name, home or other physical address (e.g., school), e-mail address, telephone number, or any information that identifies a specific individual, or any information which when tied to the above becomes identifiable to a specific individual."); *In re Eli Lilly & Co.*, 133 F.T.C. 763, 783 (2002) (decision and order) (defining "Personally identifiable information" and "personal information" as "individually identifiable information from or about an individual consumer including, but not limited to: (a) a first and last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name that reveals an individual's email address; (d) a telephone number; (e) a social security number; (f) an Internet Protocol (IP) address or host name that identifies an individual consumer; (g) a persistent identifier, such as a customer number held in a "cookie" or processor serial number, that is combined with other available data that identifies an individual consumer; or (h) or any information that is combined with (a) through (g) above" with certain exceptions.).

24 Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers 19 (2012), *available at* https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

25 *Id.* at 22.

26 *Id.* at 47 n.214, 59.

27 16 C.F.R. § 312.2.

28 Fed. Trade Comm'n, Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies iii, 8, 20 (2012), *available at* http://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf.

29 Fed. Trade Comm'n, Internet of Things: Privacy & Security in a Connected World 12-13, 30, 50 (2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

The following sections—"FTC Privacy Enforcement and Guidance Under Section 5" and "FTC Data Security Enforcement and Guidance Under Section 5"—focus on the Commission's actions brought under Section 5 of the FTC Act.

II. FTC PRIVACY ENFORCEMENT AND GUIDANCE UNDER SECTION 5

A. Early FTC Privacy Cases under Section 5

The FTC has been a privacy enforcer for over forty years, beginning with its first case under the FCRA in 1972.[30] As consumer privacy issues moved online, the agency began bringing cases against internet and software companies toward the very end of the 1990s and the early 2000s. This section discusses some of the agency's early privacy cases brought under Section 5 of the FTC Act. Two of these early cases, *In re Geocities* and *In re Microsoft Corporation*, focused on the companies' alleged misrepresentations in privacy policies and elsewhere concerning the purpose or scope of the data collected. The final case in this section, *In re Gateway Learning Corp.*, involved both unfairness and deception counts relating to the company's privacy policy changes.

1. GeoCities

The FTC's 1999 settlement with the web host GeoCities was the agency's first public settlement in the area of internet privacy. GeoCities' members, known as "homesteaders," totaled more than 1.8 million, approximately 200,000 of whom were minors between the ages of three and fifteen.[31] The site was one of the top ten most visited websites at the time.[32] To become a homesteader, all users, including children, were required to complete GeoCities' "New Member Application" form, which required certain information (first and last name, zip code, email address, gender, date of birth, and member name) and solicited, but did not require, other personal information (education level, income, marital status, occupation, and interests).[33]

The Commission alleged that GeoCities deceived consumers, including children, about the purpose of its collection of personal information. Geocities' privacy statements in its New Member Application form and elsewhere indicated that the company would only use the personal information to provide GeoCities members with email ads and product services the members requested.[34] The company also represented that it would only use the optional information it collected "to gain a better understanding of who is visiting GeoCities."[35] The FTC alleged that these privacy representations were false

---

30 Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers A-3 (2012), *available at* https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

31 *In re Geocities*, 127 F.T.C. 94, 95 (1999) (complaint).

32 *Id.*

33 *Id.* at 96-97.

34 *Id.* at 97.

35 *Id.*

or misleading because GeoCities shared with advertisers the personal information it collected, including information the company collected from children.[36]

GeoCities also operated an online community for children called GeoKidz Club.[37] GeoCities collected children's information through a sign-up form for the GeoKidz Club and through contest sign-ups.[38] GeoCities represented, the FTC alleged, that GeoCities—not a third party—was the entity collecting children's personal information submitted.[39] The FTC alleged that this representation was deceptive because third parties operated the GeoKidz Club and collected and maintained the children's personal information submitted through the GeoKidz Club membership form.[40] The order settling the case prohibits Geocities from making any misrepresentation about its collection or use of personally identifying information, or about the identity of the party collecting such information, among other things.[41]

2. Microsoft Passport

The FTC's action against Microsoft represents another early case in which the agency alleged that statements in a company's privacy policy were deceptive in violation of Section 5 of the FTC Act. In 1999, Microsoft launched its Passport and Passport Wallet online authentication and wallet services.[42] Passport's privacy policy contained a detailed description of the information the service purportedly collected from and about its users.[43] The policy further stated that Passport participated in the TRUSTe Privacy Program and, as such, users should "expect to be notified of [w]hat personally identifiable information . . . is collected" from them.[44]

Microsoft also offered a children's version of its Passport service called Kids Passport. Microsoft said that Kids Passport would "help[] [parents] conveniently protect and control [their] children's online privacy."[45] The Commission alleged that Microsoft made other statements to the same effect.[46]

The FTC alleged that Microsoft collected personally identifiable information other than that described in the Passport privacy policy, including information about the sites

---

36 *Id.* at 97-98.

37 *Id.* at 98-99.

38 *Id.*

39 *Id.* at 99.

40 *Id.; see also id.* at 122 (defining "Personal identifying information" as information that includes but is not limited to "first and last name, home or other physical address (e.g., school), e-mail address, telephone number, or any information that identifies a specific individual, or any information which when tied to the above becomes identifiable to a specific individual").

41 *Id.* at 123 (1999) (decision and order).

42 *In re Microsoft Corp.*, 134 F.T.C. 709, 710 (2002) (complaint).

43 *Id.* at 714.

44 *Id.*

45 *Id.* at 715.

46 *Id.* at 715-17.

that Passport users signed in to.[47] The Commission also alleged that Microsoft Kids Passport service falsely represented that parents would have control over their children's information.[48] For example, according to the FTC, children could edit their personal information and change account settings set by the parent.[49] Microsoft purportedly also failed to adequately inform parents that some websites outside of the Kids Passport service would have received their children's information.[50] The FTC's complaint also included two counts alleging that Microsoft's representations about Passport's security were false and misleading.[51] In the FTC's settlement with Microsoft, the Commission required the company to, among other things, establish a comprehensive information security program.[52]

3. Gateway

In *In re Gateway Learning Corp.*, another early FTC privacy settlement, the agency focused on a company's changes to its privacy policy. Gateway Learning Corp., the makers of the popular "Hooked on Phonics" learning program, marketed its products through its website, which collected various types of personal information about parents and children in connection with purchases of the company's products.[53]

The company's privacy policy initially stated that Gateway would not "sell, rent or loan" any PII to third parties, and promised to notify consumers online and by email of any "material change" to the policy.[54] Its privacy policy also stated that it would not share information about children under the age of 13 "for any purpose whatsoever."[55] Nevertheless, the FTC alleged, Gateway began renting PII provided by its customers to third party marketers.[56] Gateway subsequently changed its privacy policy to state: "From time to time, we may provide your name, address and phone number (not your e-mail address) to reputable companies whose products or services you may find of interest."[57] The Company did not notify consumers by email of this change.[58]

In its 2004 complaint, the Commission alleged that, contrary to representations in the company's privacy policy, Gateway Learning rented consumers' personal information to third-party marketers without their consent.[59] The company also rented information about children under the age of thirteen, contrary to statements in their privacy policy

---

47 *Id.* at 714-15.

48 *Id.* at 715-17.

49 *Id.* at 717.

50 *Id.*

51 *Id.* at 711-13.

52 *In re Microsoft Corp.*, 134 F.T.C. 709 , 742-43 (2002) (decision and order).

53 *In re Gateway Learning Corp.*, 138 F.T.C. 443, 444 (2004). (complaint).

54 *Id.* at 445.

55 *Id.* at 444-45.

56 *Id.* at 446.

57 *Id.*

58 *Id.* at 447.

59 *Id.* at 449.

that Gateway Learning would not share such information with any third party "for any purpose whatsoever."[60]

The FTC finally alleged an unfairness and a deception count relating to Gateway Learning's change in its privacy policy.[61] The Commission's unfairness count stated that Gateway's "retroactive application of its revised privacy policy caused or is likely to cause substantial injury to consumers that is not outweighed by countervailing benefits to consumers or competition and is not reasonably avoidable by the consumer."[62] The Commission's deception count targeted the same privacy policy change, but was based on the company's representation that it would notify consumers of material changes to its privacy policy—which Gateway failed to do.[63]

As part of the settlement, the FTC ordered Gateway to pay $4,608 in redress, which is approximately the amount Gateway earned from the rental of consumers' information collected during the period when Gateway's privacy policy promised not to sell, rent, or loan PII.[64]

B. Social Networks

The FTC's settlements with Google (relating to its Buzz social network) and Facebook represent significant actions that touched on special issues that accompanied the emergence of social networks. In those cases, and in the agency's settlement with Myspace (another social network), the consent orders require the companies to establish "comprehensive privacy program[s]" which require, among other things, designated employees to coordinate the program, a privacy risk assessment, and controls and procedures to identify the risks identified in the risk assessment.[65] This section discusses the agency's complaints against and settlements with Google and Facebook. Both of these cases involved the allegedly unexpected disclosure of previously private information, which the Commission has characterized as a key type of privacy harm.[66]

1. Google Buzz

In early 2010, Google launched the Google Buzz social network within its Gmail product. Buzz was a social network that allowed users to post updates, comments, photos,

---

60 *Id.*

61 *Id.* at 449-50.

62 *Id.* at 449.

63 *Id.* at 450.

64 *In re Gateway Learning Corp.*, 138 F.T.C. 443, 470 (2004) (decision and order).

65 *In re Google Inc.*, 152 F.T.C. 435, 454-55 (Oct. 13, 2011) (decision and order); *In re Myspace LLC*, 2012 WL 4101790, *18 (Aug. 30, 2012) (decision and order); Decision and Order at 5-6, *In re Facebook, Inc.*, No. C-4365 (Aug. 10, 2012), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf.

66 Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers 8 (2012), *available at* https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

and videos.[67] Buzz users could "follow" and, in turn, be "followed" by other Buzz users.[68] On the day Buzz launched, Gmail users were shown a prompt that purported to allow them to accept or reject enrollment in Buzz.[69] Users who declined to enroll could still be "followed" on Buzz.[70] Users who did enroll were automatically set to follow the Gmail contacts they emailed and chatted with most frequently.[71] Some users complained that these auto-generated lists included "individuals against whom they had obtained restraining orders; abusive ex-husbands; clients of mental health professionals; clients of attorneys; children; and recruiters they had emailed regarding job leads."[72] In some cases, these auto-generated lists were posted on a user's public profile.[73]

Gmail's privacy policy at the time stated that, "Gmail stores, processes and maintains your messages, contact lists and other data related to your account in order to provide the service to you."[74] Google's Privacy Policy, which applied to all Google products including Gmail, also stated that "[w]hen you sign up for a particular service that requires registration, we ask you to provide personal information. If we use this information in a manner different than the purpose for which it was collected, then we will ask for your consent prior to such use."[75]

The FTC's complaint alleged two deception counts based on representations in the privacy policies. The Commission alleged that Google used Gmail users' information for purposes other than providing those users with an email service, contrary to representations in the Gmail privacy policy.[76] Specifically, Buzz used Gmail users' contacts to populate its Buzz social network.[77] The FTC's complaint further alleged that Google's failure to seek Gmail users' consent before using their information in this way also contravened the Gmail privacy policy.[78]

The FTC's complaint also alleged a deception count based on options presented to Gmail users to decline enrollment or turn off Buzz. The Commission alleged that users who clicked on these options were still enrolled in certain Buzz features.[79]

The complaint also alleged that Google's offering certain controls that appeared to indicate user control over what information would be made public in their Google public

---

67 *In re Google Inc.*, 152 F.T.C. 435 , 437 (Oct. 13, 2011) (complaint).

68 *Id.*

69 *Id.* at 437-38.

70 *Id.* at 438.

71 *Id.* at 438-39.

72 *Id.* at 441.

73 *Id.* at 439-40.

74 *Id.* at 437.

75 *Id.*

76 *Id.* at 442.

77 *Id.*

78 *Id.*

79 *Id.* at 442-43.

profile was deceptive because in most instances a Gmail users' frequent contacts were made public by default.[80]

Finally, the complaint alleged that Google's self-certification to the Department of Commerce that the company complied with the U.S.-EU Safe Harbor privacy principles and statements in its privacy policy that it adheres to those principles constitute deceptive acts or practices because Google failed to give Gmail users notice and choice at the launch of Buzz.[81]

The Commission's settlement with Google prohibits the company from, among other things, misrepresenting the extent to which it maintains and protects of the privacy of any information Google collects from or about any individual.[82] The consent decree also requires Google to establish a "comprehensive privacy program" and undergo biennial privacy assessments.[83]

2. Facebook

The same year as the FTC's Buzz settlement, the agency also settled privacy-related claims with Facebook. The Commission's eight-count complaint addressed a number of Facebook's information practices at the time, including those related to Facebook's "platform apps" and changes to its 2009 privacy policy.

a. Facebook Platform Apps

The Commission alleged that, through the "Profile Privacy Settings" page, Facebook falsely represented that users could restrict access to their profile information to certain groups (such as Friends or Friends of Friends).[84] In fact, the Commission alleged, applications that a user's friends used on the Facebook platform could access information a user restricted to Friends or Friends of Friends.[85]

The FTC also alleged that platform apps could access far more information than Facebook claimed they could. The Commission alleged, for example, that "a quiz [app] regarding a television show, in many instances could access a user's Relationship Status, as well as the URL for every photo and video that the user had uploaded to Facebook's web site."[86] This kind of access to user information exceeded Facebook's representation that apps would only access profile information they needed to operate, the Commission's complaint alleged.[87]

---

80 *Id.* at 443.

81 *Id.* at 444-45.

82 *Id.* at 453.

83 *Id.* at 454-55.

84 Complaint ¶¶ 10-13, 17, *In re Facebook, Inc.*, No. C-4365 (July 27, 2012), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookcmpt.pdf.

85 *Id.* ¶¶ 14, 18.

86 *Id.* ¶ 31.

87 *Id.* ¶ 32.

b. 2009 Privacy Policy Changes

The FTC also alleged a deception and an unfairness count relating to Facebook's late 2009 changes to its privacy practices and privacy policy. Specifically, the company made public certain types of information (such as a user's name, profile picture, and friends list) that Facebook users had previously provided the company. The FTC alleged that this change was contrary to Facebook's statements that these changes provided users with "more control" over their information.[88] The FTC also alleged that "Facebook retroactively applied these changes to personal information that it had previously collected from users, without their informed consent, in a manner that has caused or has been likely to cause substantial injury to consumers."[89]

c. Other Counts and Settlement

The Commission alleged a number of other counts in its complaint against Facebook. The agency charged that the company falsely represented that it would not provide advertisers with information about its users,[90] misrepresented that apps it designated "Verified Applications" met a higher standard of security than other apps,[91] misled consumers as to the effect of deleting or deactivating their Facebook accounts,[92] and failed to adhere to the U.S.-EU Safe Harbor notice and choice privacy principles.[93] Facebook's settlement with the Commission requires, among other things, that the company establish a comprehensive privacy program and undergo biennial assessments by a third-party privacy professional.[94]

C. Tracking Internet Activities

The privacy risks associated with the ever-evolving landscape of internet tracking has been a significant focus of the FTC's enforcement efforts. This section discusses the agency's actions against companies that used browser toolbars, cookies, and other technologies to track consumers' activities. In the case of browser toolbars and tracking applications, the Commission targeted misrepresentations or failures to adequately disclose the scope of the data collected by the browser add-on. In the case of browser cookies and similar browsing tracking technologies, the agency focused on practices that make it more difficult for users to opt out of tracking.

1. Browser Toolbars and Tracking Applications

a. Sears

In 2009, the FTC settled with Sears Holdings Management Corporation, a subsidiary that provides marketing operations to the well-known Sears Roebuck and

---

88 *Id.* ¶¶ 27-28.

89 *Id.*¶ 29.

90 *Id.* ¶¶ 34-42.

91 *Id.* ¶ 43-49.

92 *Id.* ¶¶ 50-55.

93 *Id.* ¶¶ 56-63.

94 Decision and Order at 5-7, *In re Facebook, Inc.*, No. C-4365 (F.T.C. July 27, 2012), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf.

Kmart department stores and operates sears.com and kmart.com.[95] Sears rolled out an application as part of its "My SHC Community" market research program that, when installed, allegedly tracked nearly all of a user's internet behavior and certain other activities on a user's computer.[96] Users received $10 to keep the tracking application on their computers for at least a month.[97]

To sign up for the My SHC Community, Sears required users to complete a registration page. At the bottom of the registration page, the company displayed a "Privacy Statement and User License Agreement" in a scroll box that displayed only ten lines of text at a time.[98] On the seventy-fifth line of that document, Sears described the types of information the My SHC Community application would collect, including a user's application usage information, "the pace and style with which [the user] enter[ed] information online" and, possibly a user's username, password, credit card and account numbers.[99]

The FTC alleged that this disclosure was not enough. The sole count in the FTC's complaint against Sears alleged that the company failed to disclose adequately that its application would:

- "monitor nearly all of the Internet behavior that occurs on consumers' computers, including information exchanged between consumers and websites other than those owned, operated, or affiliated with [Sears], information provided in secure sessions when interacting with third-party websites, shopping carts, and online accounts, and headers of web-based email";[100]
- "track certain non-Internet-related activities taking place on those computers";[101] and
- "transmit nearly all the monitored information (excluding selected categories of filtered information) to [Sears'] remote computer servers."[102]

Sears' settlement with the FTC requires, among other things, that the company "[c]learly and prominently" display—on a "separate screen" from any privacy policy or license agreement—the types of data Sears will monitor or collect through its tracking applications, how that data will be used, and whether that data will be transmitted to

---

95 Complaint ¶ 1, *In re Sears Holdings Mgmt. Corp,* No. C-4264 (F.T.C. Aug. 31. 2009), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2009/09/090604searscmpt.pdf.

96 *Id.* ¶¶ 4, 13.

97 *Id.* ¶ 6.

98 *Id.* ¶ 8.

99 *Id.* ¶ 8.

100 *Id.* ¶ 13.

101 *Id.*

102 *Id.*

a third party.[103] The settlement also requires Sears to obtain express consent to the application's data collection.[104]

More recently, the Commission settled with a medical billing services company and its former CEO that, similar to Sears, made important disclosures that a user would only see after scrolling down in text boxes that only showed six lines of text at a time.[105]

b. Upromise

Like *In re Sears Holdings Management Corp.*, the Commission's 2013 settlement with Upromise, Inc. involved an alleged failure to disclose the extent to which the company's tracking application would collect and transmit data. Upromise runs a membership program that rewards its members for purchasing products and services from partner merchants by depositing money into a college savings account.[106] In 2005, Upromise began offering a browser toolbar with an option to receive "personalized offers," which the company said would collect information about a users' browsing history in order to "provide college savings opportunities."[107]

According to the FTC complaint, Upromise failed to disclose that it would collect and transmit extensive information about users' online activities, including, for a period of time, information such as credit card numbers, security codes, card expiration dates, and Social Security numbers.[108] The FTC complaint also alleged that Upromise falsely represented that information collected by the Toolbar would be encrypted in transit and that reasonable measures were employed to protect consumer data from unauthorized access.[109] The agency also alleged that this failure to employ reasonable security methods to protect consumers' information was unfair.[110] The FTC's settlement with Upromise required the company to, among other things, notify customers whose information Upromise collected through the "personalized offers" feature of the toolbar and to provide those customers with instructions to permanently disable the personalized offer feature and uninstall the toolbar.[111]

---

103 *In re Sears Holdings Mgmt. Corp.*, No. C-4264 (F.T.C. Aug. 31, 2009) (decision and order).

104 *Id.* at *7.

105 Complaint, *In re PaymentsMD, LLC,* No. C-4505 (F.T.C. Jan. 27, 2015), *available at* https://www.ftc.gov/system/files/documents/cases/150206paymentsmdcmpt.pdf (alleging two counts of deception for failing to adequately inform consumers that the medical billing services company would also seek sensitive health information from third parties); *see also* Complaint, *In re Michael C. Hughes,* No. C-4502 (F.T.C. Jan. 9, 2015), *available* at https://www.ftc.gov/system/files/documents/cases/150206michaelhughescmpt.pdf.

106 Complaint ¶ 3, *In re Upromise, Inc*, No. C-4351 (F.T.C. Mar. 27, 2012), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2012/04/120403upromisecmpt.pdf.

107 *Id.*¶¶ 4-6.

108 *Id.* ¶ 15.

109 *Id.* ¶ 16-19.

110 *Id.* ¶ 20.

111 Decision and Order at 5, *In re Upromise, Inc.*, No. C-4351 (F.T.C. Mar. 27, 2012), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2012/04/120403upromisedo.pdf.

c. Compete, Inc.

The Commission also settled with Compete, Inc., a web analytics company, which, in 2006, launched web browser add-ons called the Compete Toolbar and the Compete Consumer Input Panel.[112] The Compete Toolbar offered users information about the websites they visited, such as the website's popularity.[113] The Compete Consumer Input Panel offered users rewards for sharing their opinions about products and services.[114] The company disclosed that when the Compete Toolbar's "Community Share" feature was engaged it would collect the web pages that users visited in an "anonymously pooled" fashion.[115] Similarly, the company indicated that the Consumer Input Panel would "anonymously transmit[]" aspects of users' browsing behavior to Compete.[116]

The FTC alleged that, contrary to these claims of limited collection, the Toolbar and Input Panel collected and transmitted more extensive information about a consumer's internet behavior and financial transactions, including credit card and Social Security number submitted to third-party websites.[117] The agency alleged that this constituted a deceptive act or practice.[118] The Commission also alleged that Compete falsely represented that it removed all personal information collected through its Toolbar and Consumer Input Panel before transmitting that information to Compete.[119] Finally, the FTC alleged counts for deceptive and unfair security practices.[120]

The Company's settlement with the Commission requires Compete to, among other things, establish a comprehensive information security program.[121]

2. Cookies and Behavioral Advertising

a. Chitika

The FTC's 2011 settlement with Chitika represents the agency's first case against an online advertising network.[122] Chitika tracked users by setting a browser cookie on users' computers.[123] Chitika's privacy policy offered users a button to opt-out of receiving

---

112 *In re Compete, Inc.*, 155 F.T.C. 264 , 265 (Feb. 20, 2013).

113 *Id.*

114 *Id.*

115 *Id.* at 266.

116 *Id.*

117 *Id.* at 270-71.

118 *Id.*

119 *Id.*

120 *Id.* at 271-72.

121 *In re Compete, Inc.*, 155 F.T.C. 264, 294-95 (Feb. 20, 2013) (decision and order).

122 Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers A-7 (2012), *available at* https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

123 *In re Chitika, Inc.*, 151 F.T.C. 494, 495-96 (2011) (complaint).

tracking cookies that, when pressed, indicated to the user that "You are currently opted out."[124] Without notice, however, consumers' opt-out preferences expired after ten days, at which point Chitika resumed tracking those users.[125]

The FTC alleged that Chitika's opt-out messaging represented to users that their opt-out preferences would be saved for a "reasonable period of time"—certainly more than ten days.[126] The FTC's complaint alleged that this practice was deceptive in violation of Section 5 of the FTC Act.

b. ScanScout

In re ScanScout, Inc. is another matter that involved an advertising network's tracking technology. ScanScout, Inc. was a video advertising network that employed behavioral advertising technology to select the ads it served users.[127] While many behavioral advertisers use HTTP cookies, which are stored by a users' browser, ScanScout employed Flash cookies, which are stored in a separate location that, at the time, was not managed by a user's browser.[128]

The FTC's 2011 complaint included a single deception count. The agency alleged that ScanScout's privacy policy, which stated that users could change their *browser* settings to "opt out" of receiving a ScanScout cookie, was false and misleading.[129] A browser's cookie settings did nothing to prevent ScanScout from setting a Flash cookie, nor could an operation within a user's browser delete ScanScout's cookies.[130]

c. Epic Marketplace

ScanScout is not the only company to employ other methods of tracking users besides browser cookies. In 2013, the Commission settled with Epic Marketplace Inc. and Epic Media Group, LLC (together, "Epic") based on the agency's complaint that Epic's misleading statements and failure to disclose its "history sniffing" technology violated Section 5 of the FTC Act. Epic served as an internet advertising "intermediary" between website owners and advertisers.[131] It called the network of websites on which it served ads the "Epic Marketplace network."[132] According to the complaint, Epic was able to "history sniff"—that is, determine the websites a consumer had previously visited by accessing a user's browser history.[133] Epic's history sniffing circumvented users' efforts to prevent tracking by deleting cookies, since a browser would retain a user's browsing

---

124 *Id.* at 497.

125 *Id.*

126 *Id.* at 497-98.

127 *In re ScanScout, Inc.*, 152 F.T.C. 1019, 1020 (Dec. 14, 2011) (complaint).

128 *Id.* at 1020-21.

129 *Id.*

130 *Id.* at 1021.

131 *In re Epic Marketplace, Inc.*, 155 F.T.C. 406, 407 (Mar. 13, 2013) (complaint).

132 *Id.*

133 *Id.* at 408.

history even after purging all cookies.[134] History sniffing also allowed Epic to observe users' browsing habits on websites outside of the Epic Marketplace network.[135]

Epic included its history-sniffing code in advertisements displayed on cnn.com, papajohns.com, redcross.com, and orbitz.com, among other websites in the Epic Marketplace network, according to the FTC complaint.[136] The company queried users' browsing histories, which allegedly included some users' visits to webpages relating to "fertility issues, impotence, menopause, incontinence, disability insurance, credit repair, debt relief, and personal bankruptcy."[137]

The FTC alleged that Epic used "history sniffing" to collect information from users about their browsing habits outside of the websites in the Epic Marketplace Network, in conflict with representations that Epic made in its privacy policy.[138] The Commission also alleged that Epic failed to disclose that it was employing history sniffing, which would be material to consumers, and therefore constituted a deceptive act or practice.[139]

d. Google (Safari)

In 2012, the DOJ, on behalf of the FTC, filed a complaint in district court against Google for violating the terms of the 2011 Buzz settlement discussed above.[140] This time the FTC's complaint centered around Google's false representations to Apple Safari browser users that Google would not set tracking cookies or serve targeted ads based on those cookies.[141]

Google uses browser cookies to collect information about users and serve them targeted internet advertisements.[142] The complaint alleged that the company offered users various ways for users to opt-out of targeted advertising, including, for users of Internet Explorer, Firefox, and Chrome browsers, the ability to download a browser plugin to permanently opt-out.[143] Google did not provide a similar plugin for Safari browser users, but stated that Safari's default settings "effectively accomplishes the same thing."[144]

Not so, the Commission alleged. According to the complaint, Google overrode Safari's default settings by first setting a cookie type relating to web form submissions that

---

134 *Id.* at 408-09.

135 *Id.* at 411.

136 *Id.* at 408.

137 *Id.*

138 *Id.* at 411.

139 *Id.*

140 *See supra* Section II(B)(1).

141 Complaint ¶ 12, *United States v. Google Inc.*, No. 5:12-cv-04177-HRL (N.D. Cal. Aug. 8, 2012), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120809googlecmptexhibits.pdf.

142 *Id.* ¶ 23.

143 *Id.* ¶ 35.

144 *Id.* ¶¶ 36, 37.

Safari would accept even under the default settings.[145] Thereafter, Safari would accept other types of cookies from Google, including cookies that allowed the company to serve targeted ads.[146]

The three counts of the complaint alleged violations of the Buzz consent order for misrepresenting the extent to which users could control Google's collection of their information and for misrepresenting Google's compliance with the Network Advertising Initiative's Self-Regulatory Code of Conduct.[147] For violations of the 2011 Buzz consent order, Google was subject to civil penalties of up to $16,000 per individual violation.[148] The company settled with the Commission for $22,500,000.[149]

D. Mobile

Ubiquitous mobile devices pose a number of privacy risks that the FTC has addressed through its enforcement actions and guidance. Some of the agency's enforcement actions have focused on adequate user notice and consent, which are important in the mobile context just as they are elsewhere.[150] Moreover, as the FTC outlined in a 2013 staff report, mobile devices present at least three unique privacy challenges. First, mobile devices are typically associated with a single individual, typically always with that person, and typically always on.[151] Second, mobile devices function at the center of a number of data-collecting entities, including wireless providers, mobile OS providers, app developers, analytics companies, and advertisers.[152] Finally, mobile devices—in contrast to desktop computers—may be used to collect a user's geolocation information to build a record

---

145 *Id.* ¶¶ 42-43.

146 *Id.* ¶¶ 46, 48.

147 *Id.* ¶¶ 49-57.

148 *See* 15 U.S.C. § 45(l), as modified by 28 U.S.C. § 2461; *see also* 16 C.F.R. § 1.98(c).

149 *See* Order Approving Stipulated Order for Permanent Injunction and Civil Penalty Judgment at 3, *United States v. Google Inc.*, No. 5:12-cv-04177-HRL (N.D. Cal. Nov. 16, 2012), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2012/11/121120googleorder.pdf.

150 *See, e.g.,* Complaint, *In re General Workings Inc.*, No. C-4573 (F.T.C. Apr. 26, 2016), *available at* https://www.ftc.gov/system/files/documents/cases/1604vulcuncmpt.pdf (alleging an unfairness count based on respondents' installation, without adequate notice or consent, of a Chrome browser extension on users' PCs that then force-installed apps onto that user's mobile Android device); Complaint, *FTC v. Frostwire LLC*, No. 1:11-cv-23643 (S.D. Fl. Oct. 7, 2011) (alleging unfair design of the company's mobile file-sharing app that caused users to unknowingly share files on their mobile devices).

151 Fed. Trade Comm'n, Mobile Privacy Disclosures: Building Trust Through Transparency 2 (2013), *available at* https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf; *see also, e.g.,* Complaint, *In re Nomi Tech., Inc.*, No. C-4538 (F.T.C. Sept. 3, 2015), *available at* https://www.ftc.gov/system/files/documents/cases/150902nomitechcmpt.pdf (discussed *infra* Section II(D)(3)).

152 Fed. Trade Comm'n, Mobile Privacy Disclosures: Building Trust Through Transparency 2-3 (2013), *available at* https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf; *see also, e.g.,* Complaint, *In re Nomi Tech. , Inc.*, No. C-4538 (F.T.C. Sept. 3, 2015), https://www.ftc.gov/system/files/documents/cases/150902nomitechcmpt.pdf (discussed *infra*)).

of an individual's movements.[153] This section discusses some of the FTC enforcement actions and guidance literature addressing these and other issues.

1. Path

In 2013, the DOJ, on behalf of the FTC, filed a complaint against Path, Inc., a social network, for its false and misleading disclosures relating to its automatic collection of users' mobile device contact information. The Path app for Apple's iOS devices offered users the ability to "Find friends from your contacts."[154] However, even if a user never selected that option, the app automatically collected contacts stored on a mobile device each time the user launched the app and signed in, the complaint alleged.[155] Path's privacy policy also stated that the company automatically collected "certain information . . . such as your Internet Protocol (IP) address, your operating system, the browser type, the address of a referring site and your activity on our site."[156]

The complaint alleged that "Find friends from your contacts" amounted to a representation that Path would collect users' mobile device contacts only if the user selected that option.[157] Because Path automatically collected that information regardless, that representation amounted to a deceptive act or practice.[158] The complaint also alleged that Path's automatic collection of users' mobile device contacts exceeded what the company disclosed in its privacy policy.[159]

Finally, the complaint alleged that Path collected information from children in violation of the COPPA Rule.[160] The company's settlement required Path to pay $800,000 for its violations of the COPPA Rule.[161]

---

153 Fed. Trade Comm'n, Mobile Privacy Disclosures: Building Trust Through Transparency 3 (2013), *available at* https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf; *see also, e.g.,* Complaint, *In re Snapchat, Inc.*, No. C-4501 (F.T.C. Dec. 31, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/141231snapchatcmpt.pdf (discussed *infra*); Complaint, *In re Nomi Tech., Inc.*, No. C-4538 (F.T.C. Sept. 3, 2015), *available at* https://www.ftc.gov/system/files/documents/cases/150902nomitechcmpt.pdf (discussed *infra*); Complaint, *Goldenshores Tech., LLC*, No. C-4446 (F.T.C. Mar. 31, 2014) (alleging that company failed to adequately disclose that Android flashlight app would transmit precise geolocation information third-party advertising networks).

154 Complaint ¶ 12, *United States v. Path, Inc.*, No. 3:13-cv-0448 (N.D. Cal. Jan. 31, 2013), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2013/02/130201pathinccmpt.pdf.

155 *Id.* ¶¶ 13-14.

156 *Id.* ¶ 16.

157 *Id.* ¶¶ 30-31.

158 *Id.* ¶ 31.

159 *Id.* ¶¶ 32-33.

160 *Id.* ¶¶ 34-38.

161 Consent Decree and Order for Civil Penalties, Permanent Injunction and Other Relief ¶ 18, *United States v. Path, Inc.*, No. 3:13-cv-0448 (N.D. Cal. Feb. 8, 2013), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2013/02/130201pathincdo.pdf.

2. Snapchat

In 2014, the FTC settled with Snapchat, Inc., a mobile app that marketed itself as a way to send photo and video "snaps" that "disappear[] forever" after a pre-designated amount of time.[162] Despite this claim, the FTC alleged that there were a number of ways that a snap might not "disappear[] forever": users could access and save video files by connecting a mobile device to a computer, could use third-party apps available on Apple's and Google's app stores to save snaps, or could easily take a screen shot of the snap using a method that was not detected by the Snapchat app.[163] Consequently, the Commission's complaint alleged that Snapchat's representation that messages would "disappear forever" was false and misleading.[164] The Commission's complaint further alleged that Snapchat's representation that Snapchat users would be notified if a "snap" recipient took a screenshot of the message (to preserve it) was false and misleading because users could easily prevent the app from sending this notification.[165]

The Commission's complaint also alleged that a number of other aspects of Snapchat's service violated Section 5 of the FTC Act. In its privacy policy, Snapchat represented that it would "not ask for, track, or access any location-specific information from your device at any time while you are using the Snapchat application."[166] Despite this, the FTC said that Snapchat collected location information from users of the Android version of its application.[167] The FTC alleged that this was false or misleading in violation of Section 5 of the FTC Act.[168]

Snapchat's app offered to assist users in finding other friends on Snapchat. The app prompted users to enter a mobile phone number to search for a Snapchat account associated with that number.[169] When a user entered a phone number, however, the Snapchat app collected the names and phone numbers of *all* contacts on the user's mobile device.[170] The FTC alleged that Snapchat collected more personal information through its "Find Friends" feature than both its user interface and its privacy policy represented.[171]

Finally, the Commission alleged that the company's failure to verify the owner of the phone number that users entered into its application and failure to secure its API did not constitute reasonable security measures to protect personal information that Snapchat represented it offered in its privacy policy.[172]

---

162 Complaint ¶¶ 6-7, *In re Snapchat, Inc.*, No. C-4501 (F.T.C. Dec. 23, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/141231snapchatcmpt.pdf.

163 *Id.* ¶¶ 9-15.

164 *Id.* ¶¶ 16-17.

165 *Id.* ¶¶ 15, 18-19.

166 *Id.* ¶¶ 20-21.

167 *Id.* ¶¶ 23-24.

168 *Id.* ¶ 24.

169 *Id.* ¶ 25.

170 *Id.* ¶ 26.

171 *Id.* ¶¶ 28-33.

172 *Id.* ¶¶ 43-44.

The FTC's settlement requires Snapchat to, among other things, implement a comprehensive privacy program.[173]

3. Nomi

In 2015, the FTC settled with Nomi Technologies, a company that provides retailers with the ability to silently collect and track information about the mobile devices that consumers carry into their stores.[174] Nomi's privacy policy promised to allow consumers to opt out of retailer tracking "on its website as well as at any retailer using Nomi's technology."[175]

The Commission's complaint alleged that Nomi had promised both to give consumers notice when a retailer was using Nomi's technology and to provide a means of opting out of tracking at those retail locations.[176] Nomi's failure to provide users with this notice and opportunity to opt out amounted to deceptive acts or practices, the Commission alleged.[177]

The Commission approved the complaint and settlement by a three to two vote. FTC Chairwoman Ramirez, along with Commissioners Brill and McSweeny, issued a statement in support of the complaint and consent order. They wrote: "This case is simply about ensuring that when companies promise consumers the ability to make choices, they follow through on those promises."[178] Commissioner Ohlhausen issued two dissenting statements emphasizing that Nomi had no obligation to offer an opt-out as a "third party contractor collecting no personally identifiable information,"[179] and was therefore being "punishe[d]" for offering "more transparency and choice than legally required.[180] Commissioner Ohlhausen expressed her concern that this settlement would "undermine the FTC's own established privacy goals" and "diminish companies' incentives to be transparent about their privacy practices."[181] Commissioner Wright also dissented on the basis that penalizing Nomi "sends a dangerous message to firms weighing the costs and

---

173 Decision and Order at 3, *In re Snapchat, Inc.*, No. C-4501 (F.T.C. Dec. 23, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/141231snapchatdo.pdf.

174 Complaint ¶¶ 3-5, *In re Nomi Tech., Inc.*, No. C-4538 (F.T.C. Sept. 3, 2015), *available at* https://www.ftc.gov/system/files/documents/cases/150902nomitechcmpt.pdf.

175 *Id.* ¶ 12.

176 *Id.* ¶¶ 14, 16.

177 *Id.* ¶¶ 14-17.

178 Statement of Chairwoman Ramirez, Comm'r Brill, and Comm'r McSweeny 3-4, *In re Nomi Tech., Inc.*, No. C-4538 (Apr. 23, 2015), *available at* https://www.ftc.gov/public-statements/2015/04/statement-chairwoman-ramirez-commissioner-brill-commissioner-mcsweeny.

179 Dissenting Statement of Comm'r Maureen K. Ohlhausen 1, *In re Nomi Tech., Inc.*, No. C-4538 (Apr. 23, 2015), *available at* https://www.ftc.gov/system/files/documents/public_statements/638361/150423nomiohlhausenstatement.pdf.

180 Dissenting Statement of Comm'r Maureen K. Ohlhausen 1, *In re Nomi Tech., Inc.*, No. C-4538 (Aug. 28, 2015), *available at https://www.ftc.gov/public-statements/2015/08/dissenting-statement-commissioner-maureen-k-ohlhausen-matter-nomi*.

181 *Id.*

benefits of voluntarily providing information and choice to consumers."[182] Moreover, in his view the Commission had not shown that Nomi's representation that consumers could opt out at retail locations was material—a required element of deception.[183] Commissioner Brill also wrote separately in support of the settlement and to address Commissioner Ohlhausen's concern that Nomi's settlement would deter companies from offering privacy choices. In her view, the settlement would incentivize companies "to periodically review statements they make to consumers" and to "make sure their practices line up with those statements."[184]

4. FTC Guidance on Mobile Privacy Issues

The FTC has issued a number of studies and business guidance documents on mobile privacy issues. In the 2013 staff report *Mobile Privacy Disclosures*, FTC staff set forth best practices for privacy disclosures for mobile platforms, app developers, app trade associations, and advertising networks and other third parties that provide app services. The report notes that "platforms, such as Apple, Google, Amazon, Microsoft, and Blackberry are gatekeepers to the app marketplace and possess the greatest ability to effectuate change with respect to improving mobile privacy disclosures."[185] FTC staff suggest that mobile platforms should: (1) offer consistent privacy disclosures across apps; (2) exert more oversight and control over the apps offered in their app stores; (3) make clear the extent to which the platform reviews apps before offering apps for download on their app stores; and (4) develop a do-not-track mechanism to provide users with a means of preventing companies from tracking their behavior across apps.[186]

FTC staff also provide recommendations for app developers in that report. Staff recommend that developers: (1) make their privacy policies available through the app stores in which they offer the app; (2) provide "just-in-time" disclosures and obtain express consent when their apps collect sensitive information outside of the platform's API or when they share such sensitive information with third parties; and (3) better coordinate with the ad networks and other third parties so that developers' privacy-related disclosures to consumers are truthful and accurate.[187] The report also encourages app developers to participate in self-regulatory programs, trade associations, and industry organizations in pursuit of "uniform, short-form privacy disclosures."[188]

---

182 Dissenting Statement of Comm'r Joshua D. Wright 4, *In re Nomi Tech., Inc.*, No. C-4538 (Apr. 23, 2015), *available at* https://www.ftc.gov/public-statements/2015/04/dissenting-statement-commissioner-joshua-d-wright-matter-nomi-technologies.

183 *Id.*

184 Statement of Comm'r Julie Brill 1, *In re Nomi Tech., Inc.*, No. C-4538 (Aug. 28, 2015), *available at* https://www.ftc.gov/public-statements/2015/08/statement-commissioner-julie-brill-matter-nomi-technologies-inc.

185 Fed. Trade Comm'n, Mobile Privacy Disclosures: Building Trust Through Transparency 14 (2013), *available at* https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf.

186 *Id.* at 14-21.

187 *Id. at 22-24.*

188 *Id.* at 24.

For advertising networks and other third parties, the report recommends that these entities make clear the function of the code they are supplying to app developers (to provide advertising services, for example).[189] The report also recommends that these third parties work with platforms to implement a do-not-track system.[190]

Finally, the staff report recommends that app trade associations work to: (1) develop standard icons to depict an app's privacy practices; (2) develop privacy "badges" to standardize privacy disclosures within apps or app advertisements; and (3) standardize within app privacy policies.[191]

In addition, the FTC has published *Marketing Your Mobile App*,[192] which is a short guide for businesses on common advertising, privacy, and data security issues faced by even the smallest mobile app startups. The guide makes the point that "[l]aws that apply to established businesses apply to [small companies], too, and violations can be costly."[193] Finally, two reports—*Paper, Plastic . . . or Mobile?* and *What's the Deal?*—focus on a host of consumer protection issues, including privacy, relating to mobile payments and mobile shopping apps.[194]

E. Data Brokers: Renting or Selling Data

Several FTC enforcement actions and policy initiatives have focused on companies that buy, rent, or sell consumer information. These companies, sometimes called "data brokers," often produce marketing, risk mitigation, or people-searching products, which can help other companies better market their goods, verify identities and detect fraud, or research individuals.[195] The Commission has recognized how consumers benefit from data brokers, but it has also identified some of the risks that such entities pose to consumers. This section discusses some of the agency's enforcement actions, studies, and guidance on data brokers.

---

189 *Id.*

190 *Id.* at 25.

191 *Id.* at 25-27.

192 Fed. Trade Comm'n, Marketing Your Mobile App (2013), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf-0140_marketing-your-mobile-app.pdf.

193 *Id.* at 1.

194 Fed. Trade Comm'n, What's the Deal? An FTC Study on Mobile Shopping Apps (2014), *available at available at* https://www.ftc.gov/system/files/documents/reports/whats-deal-federal-trade-commission-study-mobile-shopping-apps-august-2014/140801mobileshoppingapps.pdf; Fed. Trade Comm'n, Paper, Plastic . . . or Mobile? (2013), *available at https://www.ftc.gov/sites/default/files/documents/reports/paper-plastic-or-mobile-ftc-workshop-mobile-payments/p0124908_mobile_payments_workshop_report_02-28-13.pdf.*

195 Fed. Trade Comm'n, Data Brokers: A Call for Transparency and Accountability 23-35 (2014), *available at* https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

1. CartManager

In 2005, the FTC settled with Vision I Properties, LLC d/b/a CartManager International ("CartManager"). According to the FTC's complaint, CartManager licensed online shopping cart software to small online merchants who, in turn, incorporated the software into their own websites to look like other pages on the merchant's site.[196] When consumers complete their orders using these shopping carts, CartManager receives the information, including name, billing and shipping addresses, phone number, email, credit card information, and information about the customer's purchase.[197] CartManager would then transmit this information to the merchant to fill the order.[198]

Some merchants using CartManager's shopping cart software published privacy policies stating that they would not rent or sell personal information collected from consumers to third parties, the FTC alleged.[199] Nevertheless, in 2003, CartManager began selling personal information it collected through the check-out process to third-party marketers.[200] The FTC alleged that CartManager did so "knowing that such practices were contrary to merchant privacy policies."[201] The Commission alleged that this constituted an unfair act or practice in violation of Section 5 of the FTC Act.[202]

2. LeapLab

Nine years after the agency's action against CartManager, the FTC filed a complaint in federal district court against another company, SiteSearch Corporation, along with SiteSearch's founder, chairman, and former CEO, LeapLab, LLC, and Leads Company, LLC. The defendants in this case collected and sold payday loan applications, which are applications for short-term loans often used to obtain an advance on an upcoming paycheck.[203] The FTC alleged that the defendants in this case sold these applications, which contain consumers' personal financial information (such as account and Social Security numbers), to non-lenders—entities that were not in the business of offering these consumers a payday loan.[204]

One of defendants' non-lender customers included Ideal Financial. Using data acquired from defendants and other sources, Ideal Financial processed over $47 million in unauthorized charges to consumers' accounts.[205] The FTC's complaint alleged that defendants' sale of consumer payday loan applications to non-lenders that had "no

---

196 *Vision I Properties, LLC*, 139 F.T.C. 296, 297 (2005).

197 *Id.*

198 *Id.*

199 *Id.* at 297-98.

200 *Id.* at 298.

201 *Id.* at 299.

202 *Id.*

203 Complaint ¶¶ 12-13, *FTC v. Sitesearch Corp., dba LeapLab*, No. 2:14-cv-02750-NVW (D. Ariz. Dec. 22, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/141223leaplabcmpt.pdf.

204 *Id.* ¶¶ 13, 15, 19.

205 *Id.* ¶ 36.

legitimate need for this sensitive personal information" constituted an unfair act or practice in violation of Section 5 of the FTC Act.[206] The FTC settled with LeapLab, LLC and John Ayers for $4,124,710 and with Leads Company LLC for $1,651,682.[207] The Court entered a default judgment against SiteSearch Corp. for $4,124,710.[208]

3. Bayview Solutions[209]

In 2014, the same year as the FTC's action against the LeapLab defendants, the FTC filed a complaint in federal district court against Bayview Solutions, LLC and two individuals for publicly disclosing consumers' sensitive financial information on an online debt collection marketplace.[210] Such marketplaces serve as forums for debt sellers to advertise their debt portfolios to buyers.[211] The FTC alleged that the defendants posted partially-redacted debt portfolios in unencrypted Excel format, which included sensitive information such as consumers' first name, date of birth, city, state, email address, employer name, bank, bank account number, bank routing number, and driver's license number.[212]

While defendants partially redacted last names, street addresses, or phone numbers from the portfolios, the FTC alleged that the remaining, unredacted information, such as a user's email address, made it all too easy to re-identify the rest of the consumer's information. For example, since email addresses are commonly a combination of a consumer's first and last names, the partially redacted information could allow someone to figure out a consumer's last name.[213] The agency's complaint alleged that this exposed the personal information of more than 28,000 consumers.[214] Consumers "would be unlikely to know that Defendants possess, and are openly disclosing their information" and could not therefore "protect themselves from the harms and potential harms the disclosures cause, including possible identity theft and concomitant account fraud, invasion of privacy, and job loss."[215] The FTC alleged that defendants' public disclosure of consumer information constituted an unfair act or practice in violation of Section 5

---

206 *Id.* ¶¶ 44-46.

207 Press Release, Fed. Trade Comm'n, Data Broker Defendants Settle FTC Charges They Sold Sensitive Personal Information to Scammers (Feb. 18, 2016) (collecting settlements), *available at* https://www.ftc.gov/news-events/press-releases/2016/02/data-broker-defendants-settle-ftc-charges-they-sold-sensitive.

208 Final Judgment and Order for Injunctive and Other Relief at 6, *FTC v. Sitesearch Corp.*, No. 2:14-cv-02750-NVW (D. Ariz. Dec. 11, 2015), *available at* https://www.ftc.gov/system/files/documents/cases/160218leaplabsitesearch.pdf.

209 The FTC filed another complaint against Cornerstone and Company and its manager for similar conduct. *See* Complaint, *FTC v. Cornerstone and Co.*, No. 1:14-cv-01479-RC (D.D.C. Aug. 27, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/142-3211-x150005/cornerstone-company-llc.

210 Complaint ¶¶ 11-12, 31, *FTC v. Bayview Sols., LLC*, No. 1:24-cv-01830-RC (D.D.C. Oct. 31, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/111014bayviewcmp.pdf.

211 *Id.* ¶ 11.

212 *Id.* ¶ 20.

213 *Id.* ¶ 21.

214 *Id.* ¶ 18.

215 *Id.* ¶ 25.

of the FTC Act.[216] Defendants stipulated to a permanent injunction that requires, among other things, that they establish a comprehensive information security program.[217]

4. FTC Guidance for Data Brokers and Big Data

The FTC has also issued guidance on the privacy issues peculiar to data brokers and so-called "big data." In its 2014 report *Data Brokers: A Call for Transparency and Accountability*, the FTC reported the findings of its study of nine data brokers and offered legislative recommendations to Congress and best practices recommendations to data brokers. The Commission reaffirmed the recommendations it made to data brokers in its *Protecting Consumer Privacy* report,[218] including its recommendation that data brokers consider privacy at every stage of product development—the "privacy by design" principle.[219] The FTC suggested that it is "particularly important" for data brokers to collect only the data they need and dispose of the data they do not.[220] In addition, the agency called on data brokers to improve their efforts to avoid collecting information from children and teens.[221] Finally, the Commission encouraged data brokers to take "reasonable precautions" to make sure that their customers—those who use their data—do not use it for eligibility determinations or unlawful discriminatory purposes.[222]

While the FTC's 2014 data brokers report recommends that companies ensure the appropriate use of consumer data, its focus is primarily on data collection, compilation, and analytics issues. In contrast, the Commission's 2016 report *Big Data: A Tool for Inclusion or Exclusion?* focuses predominantly on how data gets used after it is collected—including the consumer protection and equal employment laws that apply to big data use.[223] Finally, the FTC's business guidance for debt brokers, *Buying or selling debts? Steps for keeping data secure*, offers a collection of common-sense practices for securing debt-related information.[224]

---

216 *Id.* ¶¶ 31-33.

217 Stipulated Final Order for Permanent Injunction at 3, *FTC v. Bayview Sols., LLC*, No. 1:24-cv-01830-RC (D.D.C. Apr. 20, 2015), *available at* https://www.ftc.gov/system/files/documents/cases/150421bayviewstip.pdf.

218 *See supra* Section I(B).

219 Fed. Trade Comm'n, Data Brokers: A Call for Transparency and Accountability 54 (2014), *available at* , https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

220 *Id.* at 55.

221 *Id.*

222 *Id.*

223 Fed. Trade Comm'n, Big Data: A Tool for Inclusion or Exclusion? (2016), *available at* https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf.

224 Fed. Trade Comm'n, Buying or selling debts? Steps for keeping data secure (2015), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf-0202_buying-selling-debt.pdf.

F. Misappropriation of Consumer Data

The FTC has brought several cases against companies that misappropriate consumer data, either through undisclosed monitoring of consumers or unauthorized means. This section discusses three of these cases.

1. DesignerWare and Related Rent-to-Own Cases

In 2013, the FTC settled with several companies and individuals involved with software installed on rented computers that allowed the rental company to take screenshots, log keystrokes, and use the computers' webcams to take pictures—all without the renters' knowledge. DesignerWare, LLC developed the software at issue, called PC Rental Agent, which it licensed to stores that offer rent-to-own computers.[225]

The program had a Detective Mode, which enabled the computer rental companies to silently monitor a computer user's activities and take pictures surreptitiously using the PC's webcam.[226] According to the complaint, one of the owners of DesignerWare stated that Detective Mode works "like many spyware/malware programs" in that it is "not detectable by antivirus programs" and "hooks the screen, keyboard, and mouse so it can 'Spy' on the user and gather information."[227] The agency alleged that Detective Mode had been used to capture pictures of children, naked individuals, and couples engaged in sexual activities.[228]

Using Detective Mode, rental companies could also prompt a renter's computer to display a fake registration window for a software program such as Windows, Internet Explorer, Office, or Yahoo! Messenger.[229] The registration window collected a user's name and contact information, which the software program then transmitted to DesignerWare's servers, which in turn emailed the information to the rent-to-own store.[230]

Finally, the Commission alleged that PC Rental Agent logged, for a period of time, all of the Wi-Fi hotspots the rented computer detected or connected to.[231] The software would then transmit that information to DesignerWare's servers, which would then provide the computer rental companies with a list of the physical locations of the Wi-Fi hotspots the rented computer detected or connected to.[232] This information could be used to pinpoint a rented computer's location and, if aggregated, could track the movements of computer renters.[233]

---

225 *In re DesignerWare, LLC*, 155 F.T.C. 421, 422 (Apr. 11, 2013) (complaint).

226 *Id.* at 424.

227 *Id.*

228 *Id.* at 425.

229 *Id.* at 427.

230 *Id.* at 427.

231 *Id.* at 426.

232 *Id.*

233 *Id.*

The Commission included three counts against DesignerWare in its complaint. First, the Commission alleged that the company's surreptitious monitoring and geophysical location tracking constituted an unfair act or practice in violation of Section 5 of the FTC Act.[234] Second, the Commission alleged that DesignerWare had provided rent-to-own computer stores with the means and instrumentalities to engage in an unfair practice by providing them with PC Rental Agent and by transmitting information improperly acquired from computer rental consumers.[235] Finally, the FTC alleged that DesignerWare's fake registration windows that purported to be from "trusted software providers" were deceptive.[236]

The FTC settled with DesignerWare, two of its principals, and seven rent-to-own companies in April of 2013,[237] and with the national rent-to-own retailer Aaron's, Inc. in March of 2014.[238]

2. Jerk.com

In re Jerk, LLC was one of the agency's few privacy matters to proceed to litigation. In 2014, the Commission filed an administrative complaint against Jerk, LLC and its principal, John Fanning. Respondents operated a social network (www.jerk.com and other URLs) where users could "Post a Jerk" by creating a profile of another person with buttons that allowed users to vote the person a "Jerk" or "not a Jerk."[239] The website contained an estimated 70+ million profiles, which purported to be generated by users, the complaint alleged.[240] By paying a $30 membership fee, users could obtain "additional paid premium features," including, the FTC alleged, the ability to dispute information posted on the website.[241]

The Commission alleged two counts of deception. First, Jerk represented that content on the website was generated by Jerk users and reflected their views when, in fact, the vast majority of Jerk profiles were taken, without users' consent, from Facebook.[242] Second, Jerk represented that consumers who paid the membership fee would receive additional benefits, including the ability to dispute the information posted

---

234 *Id.* at 428-29.

235 *Id.* at 429-30.

236 *Id.* at 430-31.

237 Press Release, Fed. Trade Comm'n, FTC Approves Final Order Settling Charges Against Software and Rent-to-Own Companies Accused of Computer Spying (Apr. 15, 2013) (collecting settlements), *available at* https://www.ftc.gov/news-events/press-releases/2013/04/ftc-approves-final-order-settling-charges-against-software-and.

238 Decision and Order, *In re Aaron's, Inc.*, No. C-4442 (F.T.C. Mar. 10, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140311aaronsdo.pdf.

239 Complaint ¶¶ 4, 6, *In re Jerk, LLC*, No. 9361 (F.T.C. Apr. 2, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140407jerkpart3cmpt.pdf.

240 *Id.* ¶ 4.

241 *Id.* ¶¶ 8, 12.

242 *Id.* ¶¶ 15-16.

on the website, when, in fact, consumers often received nothing in return for paying the membership fee.[243]

In March 2015, the Commission granted summary judgment for FTC complaint counsel. The Commission found for the FTC on both deception counts and found John Fanning individually liable.[244] Fanning, but not Jerk, LLC, appealed the Commission's decision to the First Circuit, which upheld the Commission's finding of liability.[245]

3. Craig Brittain

In 2016, the FTC settled with an individual, Craig Brittain, who owned and ran the so-called "revenge porn" websites www.isanybodydown.com and www.obamanudes.com. According to the complaint, Brittain posted nude photographs along with the subject's full name, date of birth, town and state, phone number, and a link to the subject's Facebook profile.[246] Brittain compiled the photos and information through anonymous submissions, by asking for others to send him nude photographs and through a "bounty" system on the website where users could ask others to post nude photos of a specific person in exchange for a reward.[247] In many instances, Brittain did not remove the photos in response to requests.[248] According to the complaint, Brittain, posing as an independent entity called "Takedown Hammer" and "Takedown Lawyer," advertised content removal services on the website and charged users $200-500 to remove photos that he himself had posted.[249]

The FTC alleged that Brittain's posting of nude photographs, along with the personal information of the subjects, constituted an unfair act or practice in violation of Section 5 of the FTC Act. The agency also alleged that Brittain had represented that the photos submitted to him would be used solely for his private use.[250] The Commission said that posting those photos and their personal information therefore constituted a deceptive act or practice.[251]

The FTC privacy enforcement actions and guidance discussed above help define the boundaries of Section 5 liability for companies and individuals. While technological developments—particularly those that involve the collection or use of consumer data—will always create uncertainty, these past FTC privacy actions should help individuals, companies, and the attorneys that advise them to predict whether particular data practices amount to deceptive or unfair acts or practices under Section 5.

---

243 *Id.* ¶¶ 17-18.

244 Opinion of the Commission at 2, *In re Jerk, LLC*, No. 9361 (F.T.C. Mar. 13, 2015), *available at* https://www.ftc.gov/system/files/documents/cases/150325jerkopinion_0.pdf.

245 *Fanning v. FTC*, 821 F.3d 164, 168 (1st Cir. 2016).

246 Complaint ¶ 5, *In re Craig Brittain*, No. C-4564 (F.T.C. Dec. 28, 2015), *available at* https://www.ftc.gov/system/files/documents/cases/160108craigbrittaincmpt.pdf.

247 *Id.* ¶¶ 5-7.

248 *Id.* ¶ 9.

249 *Id.* ¶ 10.

250 *Id.* ¶ 15.

251 *Id.* ¶ 16.

III. FTC DATA SECURITY ENFORCEMENT AND GUIDANCE UNDER SECTION 5

The FTC's data security enforcement actions and guidance play a similar role in outlining the contours of Section 5 liability for particular data security practices. This section discusses some of those cases and materials.

A. FTC's Data Security Enforcement Authority under Section 5

Since 2002, the agency has brought dozens of data security actions under Section 5 theories of deception and unfairness.[252] Like its privacy cases, the FTC's early data security actions focused on companies' violations of their express or implied promises about their data security practices. Later ones alleged unfairness and deception or unfairness alone.[253]

The vast majority of FTC data security actions have concluded in settlements. Two cases, however, have proceeded to litigation: *FTC v. Wyndham Worldwide Corp.* in federal court and *In re LabMD, Inc.* before the FTC's administrative tribunal.[254] Both the *Wyndham* and *LabMD* actions addressed the FTC's unfairness authority under Section 5 to bring data security enforcement actions. In these cases, the defendants argued that the FTC lacks authority to bring such actions under an unfairness theory and that the agency failed to provide fair notice of the data security standards that the companies must follow under Section 5. This section addresses the FTC's two litigated cases, its settlements, and its guidance.

1. Wyndham

In *Wyndham*, the FTC alleged that the hospitality chain engaged in both deceptive and unfair practices under Section 5 by "fail[ing] to maintain reasonable and appropriate data security for consumers' sensitive personal information,"[255] including failing to remedy known security vulnerabilities, allowing software to be configured inappropriately, and failing to employ reasonable measures to detect and prevent unauthorized access to the company's network.[256] Wyndham moved to dismiss the complaint, challenging on two grounds the FTC's authority to bring data security under an unfairness theory. First, Wyndham argued that the passage by Congress of specific laws relating to data security, such as the FCRA, GLBA, COPPA, and the Health Insurance and Portability and

---

252 *In re Eli Lilly & Co.*, 133 F.T.C. 763 (2002) (complaint) was the agency's first data security action. *See* Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers A-3 (2012), *available at* https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

253 *See supra* Section I(A) (citing Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 Colum. L. Rev. 583 (2014)).

254 *F.T.C v. Wyndham Worldwide Corp.*, No. 2:12-cv-01365-PGR (D. Ariz.); *In re LabMD, Inc.*, No. 9357 (F.T.C.).

255 First Amended Complaint for Injunctive and Other Equitable Relief ¶¶ 1, 44-49, *FTC v. Wyndham Worldwide Corp.*, No. 2:12-cv-01365-PGR (D. Ariz. Aug. 9, 2012), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2012/08/120809wyndhamcmpt.pdf.

256 *Id.* at 24.

Accountability Act of 1996 (HIPAA), implies that Section 5, alone, does not authorize the agency to regulate data security under an unfairness theory.[257] Second, Wyndham argued that due process and fair notice principles require the agency to issue rules or regulations on data security before bringing enforcement actions.[258] The court rejected both arguments. It held that "the FTC's unfairness authority over data security can coexist with the existing data-security regulatory scheme,"[259] and that the FTC Act's statutory three-part test for unfairness, as well as the agency's public complaints and consent orders, provide sufficient notice of what is prohibited under Section 5.[260]

On appeal, the Third Circuit affirmed the district court's decision. First, it upheld the FTC's data security authority under the unfairness prong, reasoning that Congress's passage of topic-specific statutes, such as the FCRA, GLBA, and COPPA, are consistent with the FTC already having "some authority" to regulate data security through Section 5.[261] Second, it held that Wyndham had fair notice that the company's data security practices could constitute an unfair practice.[262] "While far from precise," Section 5 still informs parties that the relevant inquiry is a "cost-benefit, analysis" that considers "the probability and expected size of reasonably unavoidable harms . . . given a certain level of cybersecurity and the costs to consumers that would arise from investment in stronger cybersecurity."[263] The court also found that the FTC's 2007 business guidance, *Protecting Personal Business Information: A Guide For Business*, counseled against many of the practices alleged against Wyndham, and that the agency's published complaints can help companies to "apprehend the possibility that their cybersecurity could fail as well."[264] In December of 2015, Wyndham agreed to settle the FTC's charges.[265]

2. LabMD

LabMD involved similar challenges to the FTC's Section 5 unfairness authority to bring data security cases. In this administrative litigation, the FTC alleged that a medical testing laboratory failed to reasonably protect the security of consumers' personal data, including medical information, by failing to use appropriate measures to prevent employees from installing on company computers applications and files that employees did not need to perform their jobs.[266] LabMD filed a motion to dismiss—and subsequently, a motion for summary judgment—arguing (1) that Section 5 does not

---

257 *F.T.C v. Wyndham Worldwide Corp.,* 10 F. Supp. 3d 602, 610-11 (D.N.J. Apr. 7, 2014).

258 *Id.* at 616.

259 *Id.* at 613.

260 *Id.* at 620-21.

261 *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 248 (3d Cir. 2015) (explaining that the topic-specific statutes require, rather than merely authorize, the FTC to issue regulations).

262 *Id.* at 255.

263 *Id.*

264 *Id.* at 256-57.

265 Stipulated Order for Injunction, *FTC v. Wyndham Worldwide Corp.*, 2:13-cv-01887-ES-JAD (D.N.J. Dec. 11, 2015), *available at* https://www.ftc.gov/system/files/documents/cases/151211wyndhamstip.pdf.

266 Complaint ¶ 10, *In re LabMD, Inc.*, No. 9357 (F.T.C. Aug. 29, 2013), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2013/08/130829labmdpart3.pdf.

expressly authorize the FTC to regulate data security practices; (2) that HIPAA removes the agency's ability to apply Section 5 to unfair practices involving health information; and (3) that the agency cannot regulate data security under Section 5 on a case-by-case basis. The Commission rejected all three arguments. First, the Commission held that Congress delegated broad authority to determine what practices were unfair, citing the three-part test unfairness set in Section 5, the legislative history of the FTC Act, as well as federal case law deeming as "unfair" a wide range of acts and practices that were never expressly authorized under Section 5.[267] Next, the Commission held that neither HIPAA, nor any other "targeted" statute, such as the HITECH provision of the American Recovery and Reinvestment Act of 2009, forecloses the Commission from challenging data security measures that it has reason to believe are unfair acts or practices.[268] Finally, the Commission held that conducting an administrative adjudication without first conducting a rulemaking comports with due process—emphasizing that "complex questions relating to data security practices in an online environment are particularly well-suited to case-by-case development," rather than general regulations.[269]

After an administrative trial, the Chief Administrative Law Judge of the FTC issued an initial decision dismissing the FTC's complaint for failing to prove that Wyndham's conduct caused, or was likely to cause, substantial consumer injury.[270] FTC complaint counsel appealed the ALJ's decision to the Commission, which reversed and found LabMD's data security practices unfair under Section 5.[271] LabMD has appealed the Commission's order to the Eleventh Circuit.[272]

B. Enforcement Actions and Guidance

While *Wyndham* and *LabMD* focused on unfairness, the FTC has brought data security actions under both the deception and unfairness prongs of the FTC Act. The majority of FTC enforcement actions are settlements leading to consent orders that require the settling company, among other things, to establish and maintain a "comprehensive security program" or "information security program" that requires designated employees

---

267 Order Denying Respondent LabMD's Motion to Dismiss at 4, *In re LabMD, Inc.*, No. 9357 (F.T.C. Jan. 16, 2014), *available at https://www.ftc.gov/sites/default/files/documents/cases/140117labmdorder.pdf*; *see also* Order Denying Respondent LabMD, Inc.'s Motion for Summary Decision at 9, *In re LabMD, Inc.*, No. 9357 (F.T.C. May 19, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140520labmdmotion.pdf.

268 Order Denying Respondent LabMD's Motion to Dismiss at 11, *In re LabMD, Inc.*, No. 9357 (F.T.C. Jan. 16, 2014), *available at https://www.ftc.gov/sites/default/files/documents/cases/140117labmdorder.pdf*; *see also* Order Denying Respondent LabMD, Inc.'s Motion for Summary Decision at 9, *In re LabMD, Inc.*, No. 9357 (F.T.C. May 19, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140520labmdmotion.pdf.

269 Order Denying Respondent LabMD's Motion to Dismiss at 16, *In re LabMD, Inc.*, No. 9357 (F.T.C. Jan. 16, 2014); *see also* Order Denying Respondent LabMD, Inc.'s Motion for Summary Decision at 9, *In re LabMD, Inc.*, No. 9357 (F.T.C. May 19, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140520labmdmotion.pdf.

270 Initial Decision, *In re LabMD, Inc.*, No. 9357 (F.T.C. Nov. 13, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/151113labmd_decision.pdf.

271 Opinion of the Commission at 1, *In re LabMD, Inc.*, No. 9357 (F.T.C. July 29, 2016), *available at* https://www.ftc.gov/system/files/documents/cases/160729labmd-opinion.pdf.

272 Petition for Review, *LabMD, Inc. v. FTC, No. 16-16270 (11th Cir. Oct. 7, 2016).*

to coordinate the program, a privacy risk assessment, and safeguards to control the identified risks.[273] Such security programs also generally require the company to obtain biennial independent assessments of the appropriateness and effectiveness of the program.[274] Most orders also prohibit the settling company from mispresenting the extent to which it, or its products and services, protect(s) the "privacy, security, confidentiality, or integrity" of consumer personal information.[275]

---

273 *See, e.g.,* Stipulated Final Order for Permanent Injunction at 3-4, *FTC v. Cornerstone and Co.*, No. 1:14-cv-01479-RC (D.D.C. Apr. 21, 2015), *available at* https://www.ftc.gov/system/files/documents/cases/150421cornerstonestip.pdf (comprehensive information security program); Decision and Order at 3-4, *In re GMR Transcription Servs., Inc.*, No. C-4482 (F.T.C. Aug. 14. 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140821gmrdo.pdf (comprehensive information security program); Decision and Order at 3-4, *In re Fandango, LLC,* No. C-4481 (F.T.C. Aug. 13, 2014), available at https://www.ftc.gov/system/files/documents/cases/140819fandangodo.pdf (comprehensive security program); *In re HTC America Inc.,* 155 F.T.C. 1617, 1631-33 (2013) (decision and order) (comprehensive security program); Decision and Order at 2-3, *In re EPN, Inc.,* No. C-4370 (F.T.C. Oct. 3, 2012), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2012/10/121026epndo.pdf (comprehensive information security program); Consent Decree and Order for Civil Penalties, Injunction and Other Relief at 8-9, *United States v. RockYou, Inc.,* No. CV-12-1487 (N.D. Cal. Mar. 28, 2012), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2012/03/120327rockyouorder.pdf (comprehensive information security program); *In re CardSystems Sols, Inc.,* 142 F.T.C. 1019, 1025-26 (2006) (decision and order) (comprehensive information security program).

274 *See, e.g.*, Stipulated Final Order for Permanent Injunction at 5-6, *FTC v. Cornerstone and Co*., No. 1:14-cv-01479-RC (D.D.C. Apr. 21, 2015), *available at* https://www.ftc.gov/system/files/documents/cases/150421cornerstonestip.pdf; Decision and Order at 4-5, *In re GMR Transcription Servs., Inc.*, No. C-4482 (F.T.C. Aug. 14. 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140821gmrdo.pdf; Decision and Order at 4-5, *In re Fandango, LLC*, No. C-4481 (F.T.C. Aug. 13, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140819fandangodo.pdf; *In re HTC America Inc.*, 155 F.T.C. 1617, 1631-35 (2013) (decision and order); Decision and Order at 4, *In re EPN, Inc.*, No. C-4370 (F.T.C. Oct. 3, 2012), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2012/10/121026epndo.pdf; Consent Decree and Order for Civil Penalties, Injunction and Other Relief at 9-11, *United States v. RockYou, Inc.*, No. CV-12-1487 (N.D. Cal. Mar. 28, 2012), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2012/03/120327rockyouorder.pdf; *In re CardSystems Sols., Inc.*, 142 F.T.C. 1019, 1026-28 (2006) (decision and order).

275 *See, e.g.,* Decision and Order at 3, *In re GMR Transcription Servs., Inc.*, No. C-4482 (F.T.C. Aug. 14. 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140821gmrdo.pdf (prohibiting misrepresentations of "the extent to which respondents use, maintain, and protect the privacy, confidentiality, security, or integrity of personal information collected from or about consumers."); Decision and Order at 2, *In re Fandango, LLC*, No. C-4481 (Aug. 13, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140819fandangodo.pdf (prohibiting misrepresentations of "the extent to which respondent or its products or services maintain and protect the privacy, security, confidentiality, or integrity of any covered information.)"; *In re HTC America Inc.*, 155 F.T.C. 1617, 1631 (2013) (decision and order) (prohibiting misrepresentations of "the extent to which respondent or its products or services, including any covered devices, use, maintain and protect the security of covered device functionality or the security, privacy, confidentiality, or integrity of any covered information from or about consumers."); Decision and Order at 2, *In re EPN, Inc.*, No. C-4370 (F.T.C. Oct. 3, 2012), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2012/10/121026epndo.pdf (prohibiting misrepresentations of "the extent to which respondent maintains and protects the privacy, confidentiality, or security of any personal information collected from or about consumers."); Consent Decree and Order for Civil Penalties, Injunction and Other Relief at 7, *United States v. RockYou, Inc.*, No. CV-12-1487 (N.D. Cal. Mar. 28, 2012), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2012/03/120327rockyouorder.pdf (prohibiting misrepresentations of the "the extent to which [Defendant and its officers, agents, representatives, and employees] maintain and protect the privacy, confidentiality, security, or integrity of consumer personal information collected from or about consumers.").

Although the requirements in the consent orders apply only to the companies under order, the inadequacies and failures alleged in the FTC's public complaints associated with these settlements provide insight into the agency's approach to data security enforcement, as do the various reports, business guides, and blogs that the agency has issued.

For data security, one of the agency's key pieces of guidance is *Start with Security*, which identifies ten important lessons culled from the FTC's dozens of data security enforcement actions.[276] Another informative guide is *Protecting Personal Information*, which provides a practical checklist of actions for creating and implementing a sound data security plan.[277] Although FTC reports and business guides generally do not distinguish between practices required under Section 5 and best practices that go beyond existing legal requirements, the materials nevertheless provide concrete advice on many of the practices that the FTC has alleged to be unfair or deceptive in its public complaints. Indeed, in *FTC v. Wyndham*, the Third Circuit cited *Protecting Personal Information* as a helpful source of notice about companies' data security obligations under Section 5.[278]

The next sections discuss the FTC enforcement actions as well as its guidance, synthesizing key principles and practices from both areas of agency activity.

C. Reasonable Data Collection, Use, Retention, and Disposal

The Commission has stated that "reasonableness" is the "touchstone" of the agency's approach to data security: "'[A] company's data security measures must be reasonable in light of the sensitivity and volume of consumer information it holds, the size and complexity of its data operations, and the cost of available tools to improve security and reduce vulnerabilities.'"[279] In its guidance, the agency calls on companies to "limit data collection to that which is consistent with the context of a particular transaction or the consumer's relationship with the business, or as required or specifically authorized by

---

276 Fed. Trade Comm'n, Start with Security (2015), *available at* , https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

277 Fed. Trade Comm'n, Protecting Personal Information (2011), *available at* https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf.

278 According to the court, guidance materials "that are neither regulations nor 'adjudications on the merit'" can satisfy fair notice principles. *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 257-59 (3d Cir. 2015). The court also noted that "consent orders, which admit no liability and which focus on prospective requirements on the defendant, were of little use to [Wyndham] in trying to understand the specific requirements imposed by [Section 5]." *Id.* at 257 n.22.

279 Fed. Trade Comm'n, Commission Statement Marking the FTC's 50th Data Security Settlement 1 (Jan. 31, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf; *see also* Fed. Trade Comm'n, Big Data: A Tool for Inclusion or Exclusion? 22-23 (2016), *available at* https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf; Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers 24 n.108 (2012), *available at* https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf; Fed. Trade Comm'n, Prepared Statement of the Fed. Trade Comm'n on Opportunities and Challenges in Advancing Health Info. Tech. Before the Subcomm. on Info. Tech. and the Subcomm. on Health, Benefits, and Admin. Rules of the Oversight and Gov't Reform Comm., United States House of Representatives (Mar. 22, 2016), *available at* https://www.ftc.gov/system/files/documents/public_statements/941063/160322commtestimonyhealthinfo.pdf; Fed. Trade Comm'n, Data Security, https://www.ftc.gov/datasecurity (last visited March 13, 2016).

law."[280] The agency also recommends a closely related principle of data minimization—the idea that companies should limit the data they collect, use, and retain to that which is needed to serve a legitimate business purpose.[281] Consistent with its guidance, the FTC has brought numerous actions against companies for failing to establish reasonable policies or procedures regarding the collection, use, retention, and disposal of consumer information.

1. Reasonable Collection

In *United States v. RockYou*, the FTC alleged that the online game operator collected users' email passwords as part of the website registration process, even though the passwords were not needed by the business.[282] The company's unnecessary collection of consumers' email passwords, among several other alleged failures in its storage and protection of consumer information, led the FTC to charge that RockYou broke its promises to "use[] commercially reasonable physical, managerial, and technical safeguards" and to "make[] commercially reasonable efforts to ensure the security of our systems."[283]

The lesson from *RockYou* comports with the FTC's guidance that companies avoid the use and collection of sensitive personal information that does not serve a legitimate business need.[284] For example, the agency counsels against using social security numbers as employee or customer identification numbers.[285] It also recommends adjusting settings on credit card-reading software so that credit card information is not retained permanently.[286] If a company must keep information for business reasons, the agency

---

280 Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers 27 (2012), *available at* https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

281 *See, e.g.*, Fed. Trade Comm'n, Internet of Things: Privacy & Security in a Connected World iv, 21, 34 (2015), *available at* https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

282 Complaint for Civil Penalties, Permanent Injunction, and Other Relief ¶¶ 14, 16, *United States v. RockYou, Inc.*, No. CV-12-1487 (N.D. Cal. Mar. 26, 2012), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2012/03/120327rockyoucmpt.pdf.

283 *Id.* ¶¶ 15-16.

284 *See, e.g.*, Fed. Trade Comm'n, Start with Security 2 (2015), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf; Fed. Trade Comm'n, Mobile App Developers: Start with Security (2013), *available at* http://business.ftc.gov/documents/bus83-mobile-app-developers-start-security; Fed. Trade Comm'n, Internet of Things: Privacy & Security in a Connected World iv, 21, 34 (2015), *available at* https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf; Fed. Trade Comm'n, Protecting Personal Information 6-7 (2011), *available at* https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf.

285 Fed. Trade Comm'n, Protecting Personal Information 6 (2011), *available at* https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf.

286 *Id.* at 7.

recommends developing a written records retention policy to identify what information must be kept, how it long it is to be kept, and how it is to be secured and disposed.[287]

2. Reasonable Use

The agency has also taken actions against companies for unreasonable use of consumer data, including unnecessary use of real consumer information. In *In re Accretive Health*, the FTC alleged that the medical billing company used real people's personal information in employee training sessions and then failed to remove that information from employees' computers once the training ended.[288] Similarly, in *In re GeneLink*, the Commission alleged that a nutritional supplements and skincare products company gave sensitive consumer data to outside service providers that were developing software for the company, even though the service providers had no need for such sensitive data to develop the software.[289] In both cases, the FTC alleged that the practices were unfair, and, in *In re GeneLink*, alleged that the practices were also a violation of the company's promises.[290]

To avoid the unnecessary risk of exposing consumers' sensitive personal information, the agency advises that companies use fictitious information for training or application development purposes.[291]

3. Reasonable Retention

The FTC has also brought actions against companies for retaining consumer information beyond the time necessary to serve a legitimate business purpose. In *In re Life is Good*, the FTC alleged that the retailer violated its privacy policies by indefinitely storing consumer information, including credit card numbers, expiration dates, and security codes, without a business need.[292] Likewise, in *In re BJ's Wholesale Club*, the FTC alleged as unfair the retailer's practice of retaining customers' credit and debit card information used to process transactions for up to 30 days, which was long after the transactions were complete.[293] The *BJ*'s case shows that even a relatively short retention period in absolute terms may be considered unreasonable if a company retains information for longer than the time needed to serve business reasons.

The agency has stated that the reasonableness of a retention period depends, in part, on the type of relationship a company has with a consumer, as well as how the

---

287 *Id.* at 7.

288 Complaint ¶ 6(d), *In re Accretive Health, Inc.*, No C-4432 (F.T.C. Feb. 5, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140224accretivehealthcmpt.pdf.

289 Complaint ¶¶ 29(D), 30, *In re Genelink, Inc.*, Nos. C-4456, C-4457 (F.T.C. May 8, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140512genelinkcmpt.pdf.

290 Complaint ¶ 9, *In re Accretive Health, Inc.*, No C-4432 (F.T.C. Feb. 5, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140224accretivehealthcmpt.pdf; Complaint ¶¶ 31-33, *In re Genelink, Inc.*, Nos. C-4456, C-4457 (F.T.C. May 8, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140512genelinkcmpt.pdf.

291 Fed. Trade Comm'n, Start with Security 3 (2015), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

292 *In re Life Is Good, Inc.* 145 F.T.C. 192, 194 (2008) (complaint).

293 *In re BJ's Wholesale Club, Inc.*, 140 F.T.C. 465, 467-68 (2005).

company uses the information.[294] Companies that have a direct relationship with consumers, for example, may be justified in retaining data for an extended period, while companies engaged in a one-time transaction with consumers may not have a basis to hold information beyond the time needed to process the transaction.[295] In its guidance on this issue, the agency has offered several examples of contexts in which appropriate lengths of data retention will vary. A consumer's mortgage company, for example, may need to maintain data for the life of the mortgage to ensure accurate payment tracking.[296] Likewise, a consumer's auto dealer may need to retain customer data for longer periods of time in order to manage service records.[297] By contrast, however, the agency has stated that "online behavioral advertising data often becomes stale quickly and need not be retained long."[298]

The reasonableness of a retention period also depends on the type of information at issue. The FTC advises that companies consider the nature of the data they collect when they decide how long to retain data.[299] Companies that collect data on children and teens, on consumers' real-time locations, or on consumers' biometrics may want to dispose of such data more quickly.[300]

---

294 Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers 28 (2012), *available at* https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

295 *See id*.

296 *Id*.

297 *Id*.

298 *Id.; see also*, Fed. Trade Comm'n, Mobile App Developers: Start with Security (2013), *available at* http://business.ftc.gov/documents/bus83-mobile-app-developers-start-security ("[I]f you offer a location-based mobile game, get rid of the location data when it's no longer relevant."); Fed. Trade Comm'n, Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies ii (2012), *available at* http://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf ("[I]f a consumer creates an account on a website that allows her to virtually 'try on' eyeglasses, uploads photos to that website, and then later deletes her account on the website, the photos are no longer necessary and should be discarded.").

299 Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers 27 (2012), *available at* https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

300 *Id*. at 29; Fed. Trade Comm'n, Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies ii, 11-12, 18 (2012), *available at* http://www.ftc gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf.

4. Reasonable Disposal

The agency has pursued several actions against companies for claims that they failed to securely dispose of consumers' personal information.[301] For example, in *In re Rite Aid*, the FTC alleged that the use of open dumpsters by some pharmacies to discard consumers' and employees' personal information, including pharmacy labels and job applications, was unfair and contrary to the company's data security claims.[302] Similarly, in *In re CVS Caremark Corp.*, the agency alleged that the pharmacy engaged in unfair practices when it failed to obscure or redact consumers' and employees' personal information before disposing that information in publicly accessible dumpsters.[303]

The agency has also settled with companies for failing to properly dispose of consumer information when selling computer equipment containing such information. In *In re Goal Financial*, the FTC alleged that the student loan originator and servicer failed to live up to its data security promises when, among other things, its employee sold surplus hard drives that contained the sensitive personal information of approximately 34,000 customers in clear text.[304]

The FTC has offered a significant amount of guidance on secure disposal practices.[305] When disposing of old computers and portable storage devices, for example, the FTC recommends using available technology to wipe the devices.[306] For paper records, the agency recommends shredding, burning, or pulverizing.[307]

---

301 *See, e.g.*, Complaint for Civil Penalties, Permanent Injunction, and Other Equitable Relief ¶¶ 16-18, *United States v. PLS Fin. Servs., Inc.*, No. 1:12-cv-08334 (N.D. Ill. Oct. 17, 2012), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2012/11/121107plspaydaycmpt.pdf (payday loan and check cashing store's inadequate disposal procedures alleged to be contrary to company's claims); Complaint for Civil Penalties, Injunction, and Other Equitable Relief ¶¶ 11-14, *FTC v. Navone*, No. 2:08-cv-01842 (D. Nev. Dec. 30, 2008), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2009/01/090121navonecmpt.pdf (mortgage broker's disposal of consumers' personal financial records in a publicly-accessible dumpster alleged to be contrary to company's claims); *In re Nations Title Agency, Inc.* 141 F.T.C. 323, 325, 327 (2006) (complaint) (failure to implement reasonable policies and procedures in key areas, such as the collection, handling, and disposal of personal information, contradicted company's claims).

302 *In re Rite Aid Corp.*, 150 F.T.C. 694, 697 (2010) (complaint).

303 Complaint ¶¶ 7, 8, *In re CVS Caremark Corp.*, No. C-4259 (F.T.C. June 18, 2009), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2009/06/090623cvscmpt.pdf.

304 *In re Goal Fin., LLC*, 145 F.T.C. 142, 144 (2008) (complaint).

305 *See, e.g.*, Fed. Trade Comm'n, Protecting Personal Information 16, 20-21 (2011), *available at* https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf.

306 Fed. Trade Comm'n, Start with Security 14 (2015), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf; Fed. Trade Comm'n, Protecting Personal Information 21 (2011), *available at* https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf.

307 Fed. Trade Comm'n, Protecting Personal Information 21 (2011), *available at* https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf.

D. Reasonable Security Measures

The FTC has stated that it assesses the reasonableness of a company's data security practices based on the sensitivity and volume of consumer information the company holds, the size and complexity of its business, and the cost of available tools to improve security and reduce vulnerabilities, among other things.[308]

1. Assessments of Information Sensitivity and Risks

The FTC has stated that it expects companies to assess their security vulnerabilities, including inventorying what consumer information they have, which employees or third parties have access to that information, and the life cycle of that information as it "moves into, through, and out of a business."[309] To protect sensitive and other consumer information, the agency advises that companies inventory all computers, mobile devices, flash drives, and other equipment to determine where data is stored.[310] It also advises talking to staff throughout the company, as well as to outside service providers, to understand how the personal information flows.[311] Depending on particular circumstances, "appropriate assessments may range from having a knowledgeable employee run off-the-shelf security software to having an independent professional conduct a full-scale security audit."[312]

---

308 Fed. Trade Comm'n, Commission Statement Marking the FTC's 50th Data Security Settlement 1 (Jan. 31, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf; Fed. Trade Comm'n, Big Data: A Tool for Inclusion or Exclusion? 22-23 (Jan. 2016), *available at* https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf; Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers 24 n.108 (2012), *available at* https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf; Fed. Trade Comm'n, Prepared Statement of the Fed. Trade Comm'n on Opportunities and Challenges in Advancing Health Info. Tech. Before the Subcomm. on Info. Tech. and the Subcomm. on Health, Benefits, and Admin. Rules of the Oversight and Gov't Reform Comm., United States House of Representatives (Mar. 22, 2016), *available at* https://www.ftc.gov/system/files/documents/public_statements/941063/160322commtestimonyhealthinfo.pdf; Fed. Trade Comm'n, Data Security, https://www.ftc.gov/datasecurity (last visited March 13, 2016).

309 Fed. Trade Comm'n, Commission Statement Marking the FTC's 50th Data Security Settlement 1 (Jan. 31, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf; *see also* Fed. Trade Comm'n, Protecting Personal Information 4-5 (2011), *available at* https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf; Fed. Trade Comm'n, Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies ii, 10 (2012), *available at* http://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf.

310 Fed. Trade Comm'n, Protecting Personal Information 5-6 (2011), *available at* https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf.

311 *Id.*

312 *Id.* at 10.

a. Information Sensitivity

The FTC considers the sensitivity of the collected information when evaluating whether a company has implemented reasonable data security measures. Dozens of FTC data security actions have involved personal information relating to finances,[313] health,[314] and minors.[315] The FTC has also provided guidance for companies that collect or use sensitive personal information, including blogs for businesses that use health data.[316]

b. Risk Scope and Control

Failure to identify potential security risks to consumer information or to implement measures to control for such risks has been a significant focus in FTC enforcement actions.[317] The agency has pursued several cases alleging that companies compromised consumers' personal information by failing to assess the risks posed by peer-to-peer (P2P) file-sharing software that employees install on their networks. In *In re EPN, Inc.*, the FTC charged as unfair the debt collector's failure to "[a]ssess risks to the consumer

---

313 *See, e.g.*, *FTC v. Wyndham Worldwide Corp.*, No. 2:12-cv-01365-PGR, 2013 WL 1222491 (D. Ariz. Mar. 25, 2013); *In re Goal Fin., LLC*, 145 F.T.C. 142 (2008); *FTC v. Cornerstone and Co.*, No. 1:14-cv-01479-RC (D.D.C. Aug. 27, 2014), *available at* http:// www.ftc.gov/system/files/documents/cases/141001cornerstonecmpt.pdf; *FTC v. Bayview Sols.,* Case 1:14-cv-01830-RC (D.D.C. Aug. 27, 2014), *available at* http:// www.ftc.gov/system/files/documents/cases/111014bayviewcmp.pdf; *In re Credit Karma, Inc.*, No. C-4480, 2014 WL 4252397 (F.T.C. Aug. 13, 2014); *In re Fandango, LLC*, No. C-4481, 2014 WL 4252396 (F.T.C. Aug. 13, 2014); *United States v. PLS Fin. Servs., Inc.*, No. 1:12-cv-08334 (N.D. Ill. 2012); *In re EPN, Inc.*, No. C-4370, 2012 WL 2150217 (F.T.C. June 7, 2012); *In re Upromise, Inc.*, No. C-4351 (F.T.C. Mar. 27, 2012); *In re Dave & Buster's, Inc.*, 149 F.T.C. 1450 (2010); *FTC v. Navone*, No. 2:08-cv-01842 (D. Nev. filed Dec. 30, 2008); *In re Premier Capital Lending, Inc.*, No. C-4241, 2008 WL 4892987 (F.T.C. Nov. 6, 2008); *In re Life Is Good, Inc.* 145 F.T.C. 192 (2008); *In re CardSystems Sols., Inc.*, 142 F.T.C. 1019 (2006); *In re DSW, Inc.*, 141 F.T.C. 117 (2006); *United States v. ChoicePoint Inc.*, No. 06-CV-0198 (N.D. Ga.) (settlement entered Feb. 15, 2006), *available at* http:// www.ftc.gov/sites/default/files/documents/cases/2006/01/stipfinaljudgement.pdf; *In re Nations Title Agency, Inc.*, 141 F.T.C. 323 (2006); *In re Superior Mortgage Corp.*, 140 F.T.C. 926 (2005); *In re BJ's Wholesale Club, Inc.*, 140 F.T.C. 465 (2005).

314 *See, e.g.*, *In re GMR Transcription Servs., Inc.*, No. C-4482 (F.T.C.); *In re Genelink, Inc.*, Nos. C-4456, C-4457 (F.T.C.); *In re Accretive Health, Inc.*, No C-4432 (F.T.C.); *In re Henry Schein Practice Solutions, Inc.*, No. C-4575 (F.T.C.); *In re LabMD, Inc.*, No. 9357 (F.T.C.); *In re CBR Systems, Inc.*, 155 F.T.C. 841 (2013); *In re EPN, Inc*, No. C-4370 (F.T.C.); *In re Rite Aid Corp.*, 150 F.T.C. 694 (2010); *In re CVS Caremark Corp.*, No. C-4259 (F.T.C.); *In re Eli Lilly & Co.*, 133 F.T.C. 763 (2002).

315 *In re GMR Transcription Services, Inc.*, No. C-4482 (F.T.C.); *In re TrendNET*, No. C-4426 (F.T.C.); *In re CBR Systems, Inc.*, 155 F.T.C. 841 (2013); *United States v. RockYou, Inc.*, No. CV-12-1487 (N.D. Cal.); *In re Upromise, Inc.*, No. C-4351 (F.T.C.); *In re Microsoft Corp.*, 134 F.T.C. 709 (2002).

316 *See, e.g., Cora Han, Using Consumer Health Data?,* FTC Bus. Blog (Apr. 27, 2015 9:32 AM), https:// www.ftc.gov/news-events/blogs/business-blog/2015/04/using-consumer-health-data; Cora Han, *Using Consumer Health Data: Some Considerations for Companies,* FTC Bus. Blog (Apr. 28, 2015 9:52 AM), https://www.ftc.gov/news-events/blogs/business-blog/2015/04/using-consumer-health-data-some-considerations-companies.

317 *See, e.g.*, *In re Goal Fin., LLC*, 145 F.T.C. 142, 144, 146 (2008) (complaint) (failure to adequately assess risks to information collected and stored in paper files and on computer network alleged to be contrary to company's claims); Complaint ¶¶ 7, 9-10, *In re CVS Caremark Corp.*, No. C-4259 (F.T.C. June 18, 2009), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2009/06/090623cvscmpt.pdf (failure to employ a reasonable process for discovering and remedying risks in disposal of personal information alleged to be unfair and contrary to company's claims); Complaint at 325, *In re Nations Title Agency, Inc.* 141 F.T.C. 323 (2006) (failure to assess risks to consumer information collected and stored online and offline alleged to be contrary to company's claims).

personal information it collected" and to "[a]dopt an information security plan that was appropriate for its networks and the personal information processed and stored on them."[318] The complaint alleged that EPN failed to use "reasonable measures to assess and enforce compliance with its security policies and procedures, such as scanning networks to identify unauthorized [P2P] file sharing applications" or to use "reasonable methods to prevent, detect, and investigate unauthorized access to personal information on its networks, such as by adequately logging network activity and inspecting outgoing transmissions to the Internet."[319] These and other failures allegedly led to the disclosure of company files containing personal financial and health information about thousands of debtors, including social security numbers, employer addresses, and in the case of healthcare clients, physician name, insurance number, and diagnosis code, on a P2P network.[320] Similarly, in *In re Franklin's Budget Car Sales, Inc.,* the FTC charged that the auto dealer's failure to assess risks to consumer information it collected and failure to adopt an appropriate security plan led to the exposure of personal information about thousands of consumers on a P2P network.[321]

c. Secure Design

The agency has also brought actions against companies for failing to design their products securely. In *In re Snapchat,* discussed in Section II(D)(2), the FTC alleged that the mobile messaging company failed to securely design its application, which would allow an individual to create an account using another consumer's phone number and to enable that individual to send and receive messages with the consumer's phone number.[322] According to the FTC's complaint, numerous consumers complained that their numbers had been misappropriated to create unauthorized Snapchat accounts.[323]

The agency has also taken action against companies that failed to verify the performance of advertised privacy and security features. In *In re TRENDnet*, the FTC charged that the electronics company failed to test the efficacy of its password protection option on the live internet feed of the company's IP cameras.[324] The FTC charged that the setting did not reasonably prevent unauthorized access to the live feeds and was therefore unfair.[325] The agency further alleged that the company's failure to "perform security review and testing" of the software through measures such as a security architecture review or software vulnerability and penetration testing was contrary to the company's

---

318 Complaint ¶ 6, *In re EPN, Inc.*, No. C-4370 (F.T.C. Oct. 3, 2012), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2012/10/121026epncmpt.pdf.

319 *Id.*

320 *Id.* ¶¶ 4, 8.

321 Complaint ¶¶ 8-10, *In re Franklin's Budget Car Sales, Inc.*, No. C-4371 (F.T.C. Oct. 3, 2012), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2012/10/121026franklinautomallcmpt.pdf.

322 Complaint ¶¶ 34-36, *In re Snapchat, Inc.*, No. C-4501 (F.T.C. Dec. 23, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/141231snapchatcmpt.pdf (discussed *supra* Section II(D)(2)).

323 *Id.* ¶ 36.

324 Complaint ¶¶ 7, 8, *In re TRENDnet, Inc.*, No. C-4426 (F.T.C. Jan. 16, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140207trendnetcmpt.pdf.

325 *Id.* ¶ 18.

promises that it took reasonable steps to ensure security.[326] The agency has brought actions alleging comparable failures in *In re Snapchat*,[327] *In re ASUSTeK Computer*,[328] *In re Oracle*,[329] and *In re Upromise*.[330]

As the agency has stated in its guidance, reviewing and testing the functionality of security features is especially important because such practices help companies—and their service providers—to identify if there are "backdoors" to gaining control over personal information.[331]

2. Authentication and Access Limitations

The FTC has brought numerous cases against companies for failing to limit personnel and third-party access to consumer information.[332] Here, the agency's assessment of reasonableness has focused on whether individuals and organizations have a legitimate business need to access the information, as well as the types of measures implemented to exclude those without a valid need.

---

326 *Id*. ¶¶ 8, 14-17.

327 Complaint ¶¶ 3-19, *In re Snapchat, Inc.*, No. C-4501 (F.T.C. Dec. 23, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/141231snapchatcmpt.pdf (mobile messaging app over-promised that its messages would "disappear forever" and that "snap" sender would be immediately notified if a recipient took a screenshot of the snap) (discussed *supra* Section II(D)(2)).

328 Complaint ¶¶ 30, 37-46, *In re ASUSTeK Comput. Inc.*, No. C-4587 (F.T.C. July 18, 2016), *available at* https://www.ftc.gov/system/files/documents/cases/1607asustekcmpt.pdf (hardware manufacturer's failure to use readily available secure protocols, to perform reasonable and appropriate software code review and testing, and to implement readily available, low-cost protections against well-known and reasonably foreseeable vulnerabilities alleged to be unfair and contrary to company's representations).

329 Complaint ¶¶ 20-22, *In re Oracle Corp.*, No. C-4571 (F.T.C. Mar. 28, 2016), *available at* https://www.ftc.gov/system/files/documents/cases/160329oraclecmpt.pdf (software company's failure to disclose, or to disclose adequately, that Java updates did not fully protect computers from malware alleged to be deceptive).

330 Complaint ¶ 14(b), *In re Upromise, Inc.*, No. C-4351 (F.T.C. Mar. 27, 2012), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2012/04/120403upromisecmpt.pdf (failure to test company's toolbar before distributing it or to monitor the toolbar's operation for compliance with company policies alleged to be unfair and contrary to company's claims) (discussed *supra* Section II(C)(1)(b)).

331 Fed. Trade Comm'n, Internet of Things: Privacy & Security in a Connected World iii, 28-29 (2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf; *see also* Fed. Trade Comm'n, Start with Security 10 (2015), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

332 *See, e.g.*, Complaint ¶¶ 20(c), 41-43, *FTC v. LifeLock, Inc.*, No. 2:10-cv-00530-MGM (D. Ariz. Mar. 8, 2010), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2010/03/100309lifelockcmpt.pdf (failure to limit access to personal information to employees and vendors needing access alleged to be deceptive in light of company's claims); Complaint ¶¶ 6(b), 9, *In re Accretive Health, Inc.,* No C-4432 (F.T.C. Feb. 5, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140224accretivehealthcmpt.pdf (medical billing company's failure to adequately restrict access to personal information based on employee need alleged to be unfair); *In re Dave & Buster's, Inc.*, 149 F.T.C. 1450, 1451-52 (2010) (complaint) (restaurant chain's failure to adequately restrict a third-party credit card processor's access to company network—for example, by restricting connections to specified IP addresses or granting temporary, limited access—alleged to be unfair).

a. Employee and Third-Party Access

In *In re Goal Financial*, the FTC alleged that the student loan originator and servicer's failure to restrict employee access to personal information stored in paper files and on its network was deceptive in light of the company's promises.[333] According to the agency's complaint, as a result of this and other lax practices, a group of employees transferred, without authorization, more than 7,000 consumer files containing sensitive information to third parties.[334]

The FTC also brought a case against Twitter for the social media company's failure to limit access to key administrative systems. The complaint alleged that the company granted almost all of its employees administrative control over Twitter's system, which allowed any employee to reset Twitter users' account passwords, to view users' nonpublic tweets, and to send tweets on users' behalf.[335] The agency alleged that this failure increased the risk that the misappropriation of a single employee's credentials could result in a serious breach, thereby contravening Twitter's representations to consumers about its security.[336]

The FTC has also entered into settlements with businesses that sold or provided consumer information without verifying the identities of their clients or the legitimacy of those clients' purposes in acquiring the information. In *United States v. ChoicePoint Inc.*, the FTC alleged violations of the Fair Credit Reporting Act and the FTC Act against the consumer reporting agency for accepting subscribers without verifying the identities or qualifications of those subscribers.[337] For example, ChoicePoint allegedly accepted, without further inquiry, "facially contradictory" information on subscriber applications, such as articles of incorporation that reflected that the business was suspended.[338] In addition to claimed violations of the FCRA, the FTC alleged that the company's lack of reasonable procedures to verify or authenticate the identities and qualifications of prospective subscribers was unfair under Section 5 and contrary to the company's representations that it implemented reasonable and appropriate measures to prevent unlawful access to consumers' information.[339] ChoicePoint agreed to pay $10 million in civil penalties and $5 million in consumer redress to settle the charges.[340]

The agency alleged similar violations against Rental Research Services, a company that, according to the Commission, used sensitive financial data from other consumer reporting agencies to create reports that property owners use to assess potential

---

333 *In re Goal Financial, LLC*, 145 F.T.C. 142 , 144, 146 (2008) (complaint).

334 *Id.* at 144.

335 *In re Twitter, Inc.*, 151 F.T.C. 162, 164, 167 (2011) (complaint).

336 *Id.* at 167-69.

337 Complaint ¶¶ 15-32, *United States v. ChoicePoint Inc.*, No. 06-CV-0198 (N.D. Ga. Jan. 30, 2006), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2006/01/0523069complaint.pdf.

338 *Id.* ¶ 13(c).

339 *Id.* ¶¶ 15-32.

340 Stipulated Final Judgment and Order for Civil Penalties, Permanent Injunction, and Other Equitable Relief at 4, 17, *United States v. ChoicePoint Inc.*, No. 06-CV-0198 (N.D. Ga. Feb. 15, 2006), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2006/01/stipfinaljudgement.pdf.

renters.[341] In addition to alleging violations of the FCRA,[342] the FTC charged as unfair the company's failure to verify or authenticate the identities and business purposes of prospective customers.[343] According to the complaint, the company gave identity thieves posing as property owners an account with unlimited online access to consumers' credit reports, which the unauthorized parties used to access at least 318 reports.[344] The company, and the named officer, agreed to pay $500,000 in civil penalties to settle the complaint.[345]

In its guidance, the agency has stated that it expects companies to limit the access of employees, third parties, and customers according to the legitimate business needs of those parties.[346]

b. Network Segmentation

Reasonable restriction of access may also require a company to segment its network, which limits the ability of computers on a system to communicate with each other.[347] In *In re DSW*, the FTC alleged that the shoe retailer's failure to segment its network allowed hackers to use one in-store network to access personal information on other in-store and corporate networks—resulting in the breach of sensitive information relating to more than more than 1.4 million credit card and debit card accounts and nearly one hundred thousand checking accounts and driver's license numbers.[348] According to the complaint, this failure was unfair under Section 5.[349] Similarly, in *FTC v. Wyndham*, the FTC alleged deception and unfairness counts against the hospitality chain for failing to use "readily

---

341 Complaint for Civil Penalties, Injunctive and Other Equitable Relief ¶ 9, *United States v. Rental Research Servs., Inc.*, No. 0:09-CV-00524-PJS-JJK (D. Minn. Mar. 5, 2009), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2009/03/090305rrscmpt.pdf.

342 *Id.* ¶¶ 18-26.

343 *Id.*¶¶ 13, 17, 28-29.

344 *Id.* ¶ 15.

345 Stipulated Final Judgment and Order for Civil Penalties, Permanent Injunction, and Other Equitable Relief at 4, No. 0:09-CV-00524-PJS-JJK (D. Minn. Mar. 5, 2009), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2009/03/090305rrsorder.pdf.

346 Fed. Trade Comm'n, Start with Security 9 (2015), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf; Fed. Trade Comm'n, Protecting Personal Information 5 (2011) *available at*, https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf.

347 *See, e.g.*, Complaint for Civil Penalties, Permanent Injunction, and Other Relief ¶¶ 16, 29-30, *United States v. RockYou, Inc.*, No. CV-12-1487 (N.D. Cal. Mar. 26, 2012), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2012/03/120327rockyoucmpt.pdf (failure to segment servers alleged to be contrary to company's claims); *In re CardSystems Sols., Inc.*, 142 F.T.C. 1019, 1021-22 (2006) (complaint) (failure to use readily available security measures to limit access between computers on network and between such computers and the internet alleged to be unfair).

348 *In re DSW Inc.*, 141 F.T.C. 117, 120 (2006) (complaint).

349 *Id.* at 119.

available security measures," such as firewalls, to limit access among the chain's property management systems, corporate network, and the internet.[350]

These actions are consistent with the agency's guidance that companies should protect particularly sensitive data by housing it in a separate, secure place on a company's network.[351]

c. Strong Authentication

Strong authentication procedures are also an important component of reasonable security. The FTC has initiated several cases against businesses for lacking adequate password policies and systems.[352] In *In re Twitter*, the FTC alleged that Twitter let employees use common dictionary words—as well as passwords they were already using for other accounts—as administrative passwords.[353] According to the complaint, Twitter's failure to require employees to use unique or complex passwords left the company vulnerable to hackers who could use password-guessing tools or passwords stolen from other services to access Twitter's system.[354]

The FTC has also taken action against companies that failed to protect their authentication systems from outsider bypass. In *In re ASUSTeK Computer Inc.*, the agency alleged that design flaws in the computer hardware maker's router allowed unauthorized individuals to access a consumer's "private personal cloud" account by sending a specific command or entering a specific URL in a web browser, thereby bypassing the need to use the consumer's login credentials.[355] Similarly, in *In re Lookout Services, Inc.*, the FTC alleged that outsiders could bypass login requirements and access the company's sensitive

---

350 First Amended Complaint 10, ¶ 24(a), *FTC v. Wyndham Worldwide Corp.*, No. 2:12-cv-01365-PGR (D. Ariz. Aug. 9, 2012), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2012/08/120809wyndhamcmpt.pdf.

351 Fed. Trade Comm'n, Start with Security 7 (2015), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

352 *See, e.g.*, First Amended Complaint for Injunctive and Other Equitable Relief ¶ 24(f), *FTC v. Wyndham Worldwide Corp.*, No. 2:12-cv-01365-PGR (D. Ariz. Aug. 9, 2012), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2012/08/120809wyndhamcmpt.pdf (allowing use of easily guessed passwords to access systems alleged to be unfair and contrary to company's claims); Complaint ¶¶ 18, 30, *In re ASUSTeK Comput. Inc.*, No. C-4587 (F.T.C. July 18, 2016), *available at* https://www.ftc.gov/system/files/documents/cases/1607asustekcmpt.pdf (allowing consumers to retain the same default login credentials on every router, along with other security design flaws, alleged to be unfair and contrary to company's claims); *In re CardSystems Sols., Inc.*, 142 F.T.C. 1019, 1021-22 (2006) (complaint) (failure to use strong passwords, along with other security failures, alleged to be unfair); *In re Lookout Servs., Inc.*, 151 F.T.C. 532, 534, 536-37 (2011) (complaint) (failure to require strong user passwords alleged to be unfair and contrary to company's claims); *In re Nations Title Agency, Inc.,* 141 F.T.C. 323, 325, 327-28 (2006) (complaint) (failure to implement reasonable access controls, such as strong passwords, to prevent unauthorized access to stored personal information alleged to be deceptive in light of company's claims).

353 *In re Twitter, Inc.*, 151 F.T.C. 162, 167-68 (2011) (complaint).

354 *Id.* at 168-69.

355 Complaint ¶¶ 7, 10, *In re ASUSTeK Comput. Inc.*, No. C-4587 (F.T.C. July 18, 2016), *available at* https://www.ftc.gov/system/files/documents/cases/1607asustekcmpt.pdf.

employee information by typing a URL into a web browser.[356] The FTC charged that these failures were unfair and contrary to the company's promises.[357]

Strong authentication may also require implementing measures to guard against brute force attacks, which employ software programs to repeatedly guess different combinations of user login IDs and passwords in an attempt to gain access to a system. In its actions against Lookout Services and Twitter, the FTC alleged as unfair and deceptive the companies' failure to suspend or disable user credentials even after the companies' systems experienced a number of unsuccessful login attempts.[358] And in *FTC v. Wyndham*, the FTC alleged as unfair and deceptive Wyndham's failure to defend against brute-force attacks seeking access to an administrator account.[359]

The FTC has offered a variety of concrete tips for strengthening passwords and authentication procedures.[360] For example, it recommends that companies require employees and users to choose complex passwords and to instruct them not to use the same or similar passwords across multiple accounts.[361] It also recommends companies adopt policies and procedures to suspend or disable accounts after repeated failed login attempts and consider additional forms of protections, such as two-factor authentication.[362] But as the agency has noted, data security is an evolving process. In a recent blog post, the FTC's Chief Technologist discussed research showing that mandatory password changes may offer less security benefits than previously thought, in part because users forced to regularly change passwords tend to create passwords that follow predictable patterns—enabling attackers to more easily guess the next password.[363] The bottom line is that companies should continually re-evaluate their authentication methods as risks, technologies, and the latest thinking on security continue to evolve.

---

356 *In re Lookout Servs., Inc.*, 151 F.T.C. 532, 534-35 (2011) (complaint).

357 Complaint ¶¶ 37-46, *In re ASUSTeK Comput. Inc.*, No. C-4587 (F.T.C. July 18, 2016), *available at* https://www.ftc.gov/system/files/documents/cases/1607asustekcmpt.pdf; *In re Lookout Servs., Inc.*, 151 F.T.C. 532, 536-37 (2011) (complaint).

358 *Id*. at 534-37); *In re Twitter, Inc.*, 151 F.T.C. 162, 167-69 (2011) (complaint).

359 First Amended Complaint for Injunctive and Other Equitable Relief ¶ 26, *FTC v. Wyndham Worldwide Corp.*, No. 2:12-cv-01365-PGR (D. Ariz. Aug. 9, 2012), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2012/08/120809wyndhamcmpt.pdf.

360 *See, e.g.* Fed. Trade Comm'n, Start with Security 5 (2015), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf; Fed. Trade Comm'n, Protecting Personal Information 12-13 (2011), *available at* https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf.

361 Fed. Trade Comm'n, Protecting Personal Information 12 (2011), *available at* https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf; Fed. Trade Comm'n, Start with Security 5 (2015), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

362 Fed. Trade Comm'n, Protecting Personal Information 5 (2011), *available at* https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf.

363 Lorrie Cranor, *Time to Rethink Mandatory Password Changes*, Tech@FTC Blog (Mar. 2, 2016, 10:55 AM), https://www.ftc.gov/news-events/blogs/techftc/2016/03/time-rethink-mandatory-password-changes.

3. Security for Information throughout Its Life Cycle

Through its enforcement actions and guidance, the FTC has made clear that personal information in all formats must be reasonably secured throughout its life cycle.[364]

a. Encryption

Securing information in an electronic format will often require some form of encryption. The FTC has brought several cases against companies alleged to have failed to encrypt or to adequately secure consumer data. In *In re Henry Schein Practice Solutions, Inc.*, a dental software company purportedly represented that it used industry-standard encryption and that its product helped to protect patient data as required by HIPAA.[365] Instead of using encryption, however, the business used a less complex method of data masking that did not meet the National Institute of Standards and Technology (NIST) standard recommended by the Department of Health and Human Services for companies seeking to comply with HIPAA.[366] In its proposed complaint, the FTC alleged that the company's inadequate data obfuscation was deceptive in light of the company's claims.[367] The settlement requires the company to pay $250,000 as an equitable remedy and to notify customers that its software uses a less complex encryption than the standard recommended by the NIST.[368]

The agency has also taken action against companies that allegedly failed to properly configure the encryption they employed. In *In re Fandango* and *In re Credit Karma*, the FTC alleged that the companies used SSL encryption in their mobile apps, but turned off a critical security process known as "SSL certificate validation" without implementing any compensating security measures.[369] This failure made the companies' applications vulnerable to man-in-the-middle attacks in which unauthorized third parties position themselves between the online service and an application by presenting an invalid

---

364 Fed. Trade Comm'n, Start with Security 6-7, 13 (2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf; Fed. Trade Comm'n, Mobile App Developers: Start with Security (2013), *available at* http://business.ftc.gov/documents/bus83-mobile-app-developers-start-security; Fed. Trade Comm'n, Internet of Things: Privacy & Security in a Connected World 30 (2015), *available at* https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

365 Complaint ¶¶ 5, 9, 12, *In re Henry Schein Practice Sols., Inc.*, No. C-4575, *available at* https://www.ftc.gov/system/files/documents/cases/160523hspscmpt.pdf.

366 *Id.* ¶¶ 8, 10.

367 *Id.* ¶¶ 19-22.

368 Decision and Order at 4, 5, *In re Henry Schein Practice Sols., Inc.,* No. C-4575 (Jan. 5, 2016), *available at* https://www.ftc.gov/system/files/documents/cases/160523hspsdo.pdf.

369 Complaint ¶¶ 17, 19, 21(a), *In re Credit Karma, Inc.*, No. C-4480 (F.T.C. Aug. 13, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/1408creditkarmacmpt.pdf; Complaint ¶¶ 16, 18, 19(a), *In re Fandango, LLC*, No. C-4481 (F.T.C. Aug. 13, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140819fandangocmpt.pdf.

certificate to the application.[370] The FTC alleged that Fandango and Credit Karma's failures contravened their privacy and security promises.[371]

(1) Transmission

The FTC's data security cases involving the transmission of consumer data have focused on a number of different means of data transmission. Some of the FTC's cases in this area have centered around companies' alleged failures to secure the technology devices used by their employees to transport consumer information.[372] Other cases have focused on an alleged failure to use encryption (or adequate encryption) during the transmission of consumer information.[373] In *FTC v. Rennert* and *In re TRENDnet*, the FTC alleged that the companies' failures to use secure connections when transmitting consumer information contradicted the companies' representations.[374] The FTC also alleged as unfair TRENDnet's transmission of user login credentials in clear, readable text, despite the availability of free software that would have enabled the company to secure such transmissions.[375]

Even within a company, encryption of personal information during transmission may be necessary. In *In re Superior Mortgage Corp.*, the FTC alleged that, although the company used SSL encryption to secure the transmission of sensitive personal information between a customer's web browser and the company's website server, the company's third-party service provider decrypted the information once it reached Superior Mortgage's server and subsequently emailed the decrypted information in clear, readable text to the

---

370 Complaint ¶ 11, *In re Credit Karma, Inc.*, No. C-4480 (F.T.C. Aug. 13, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/1408creditkarmacmpt.pdf; Complaint ¶ 10, *In re Fandango, LLC*, No. C-4481 (F.T.C. Aug. 13, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140819fandangocmpt.pdf.

371 Complaint ¶¶ 27, 30, *In re Credit Karma, Inc.*, No. C-4480 (F.T.C. Aug. 13, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/1408creditkarmacmpt.pdf; Complaint ¶ 25, *In re Fandango, LLC*, No. C-4481 (F.T.C. Aug. 13, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140819fandangocmpt.pdf.

372 *See, e.g.*, Complaint ¶¶ 6(a), 7, 9 *In re Accretive Health, Inc.*, No C-4432 (F.T.C. Feb. 5, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140224accretivehealthcmpt.pdf (employee's leaving a laptop containing more than 600 files with information related to 23,000 patients in locked passenger compartment of a car, which was then stolen, alleged to be unfair); *In re CBR Sys., Inc.*, 155 F.T.C. 841, 844-45 (2013) (complaint) (employee's leaving unencrypted backup tapes, laptop, and an external hard drive with sensitive information in car alleged to be deceptive in light of company's promises).

373 *See, e.g.*, Complaint ¶¶ 20(a), 38-40, *FTC v. LifeLock, Inc.*, No. 2:10-cv-00530-MGM (D. Ariz. Mar. 8, 2010), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2010/03/100309lifelockcmpt.pdf (transmitting and storing personal information in clear, readable text violated company's representations).

374 Complaint ¶ 34, *FTC v. Rennert*, No. CV-S-00-0861-JBR (D. Nev. July 12, 2000), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2000/07/ftc.gov-iogcomp.htm; Complaint ¶ 8, *In re TRENDnet*, No. C-4426 (F.T.C. Jan. 16, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140207trendnetcmpt.pdf.

375 Complaint ¶ 8, *In re TRENDnet*, No. C-4426 (F.T.C. Jan. 16, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140207trendnetcmpt.pdf.

company's headquarters and branch offices.[376] According to the complaint, this practice contradicted the company's data security claims.[377]

(2) Storage

The FTC has taken action against companies for claims that the companies employed inadequate or no encryption to protect stored information.[378] The Commission has also settled with companies that allegedly put portfolios of consumer debt containing highly sensitive personal and financial information on public websites for purposes of selling those portfolios.[379]

(3) Remote Access

Failure to ensure that computers with remote access to company networks have appropriate endpoint security has also been an area of significant FTC enforcement.[380] In *FTC v. Premier Capital Lending*, the FTC alleged that a mortgage lender's failure to assess a business client's security before activating a remote login account for that client was contrary to the company's claim that it "maintain[ed] physical, electronic, and

---

376 *In re Superior Mortgage Corp.*, 140 F.T.C. 926, 930 (2005) (complaint).

377 *Id.*

378 *See, e.g.*, First Amended Complaint for Injunctive and Other Equitable Relief ¶¶ 24(b), 47-49, *FTC v. Wyndham Worldwide Corp.*, No. 2:12-cv-01365-PGR (D. Ariz. Aug. 9, 2012), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2012/08/120809wyndhamcmpt.pdf (storage of payment card information in clear, readable text alleged to be unfair); Complaint ¶ 8, *In re TrendNET*, No. C-4426 (Jan. 16, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140207trendnetcmpt.pdf (storage of user login credentials in clear, readable text, despite existence of free software enabling securing of stored credentials, alleged to be unfair and contrary to company's claims); *In re Ceridian Corp.*, 151 F.T.C. 514, 516 (2011) (complaint) (indefinite storage of personal information in clear, readable text without a business need alleged to be unfair and contrary to company's claims); Complaint ¶¶ 20(a), 38-40, *FTC v. LifeLock, Inc.*, No. 2:10-cv-00530-MGM (D. Ariz. Mar. 8, 2010), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2010/03/100309lifelockcmpt.pdf (transmitting and storing personal information in clear, readable text alleged to be contrary to company's claims); *In re Guess?, Inc.*, 136 F.T.C. 507, 512-13 (2003) (complaint) (storage of consumers' personal information, including credit card numbers, in clear, readable text alleged to be contrary to company's claims); *In re Petco Animal Supplies, Inc.*, 139 F.T.C. 102, 106 (2005) (complaint) (failure to maintain sensitive information in an encrypted format alleged to be contrary to to company's claims); Complaint ¶¶ 34, 43-44 *FTC v. Rennert*, No. CV-S-00-0861-JBR (D. Nev. July 12, 2000), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2000/07/ftc.gov-iogcomp.htm (failure to encrypt customer information alleged to be contrary to company's claims).

379 *See, e.g.*, Complaint for Permanent Injunction and Other Equitable Relief ¶¶ 28-30, *FTC v. Cornerstone and Company, LLC*, No. 1:14-cv-01479-RC (D.D.C. Aug. 27, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/141001cornerstonecmpt.pdf (online posting of consumers' bank account and credit card numbers, birth dates, contact information, employers' names, and debt-related information alleged to be unfair); Complaint for Permanent Injunction and Other Equitable Relief ¶¶ 22, 31-33, *FTC v. Bayview Sols.*, LLC, Case 1:14-cv-01830-RC (D.D.C. Oct. 31, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/111014bayviewcmp.pdf (online posting of unencrypted documents containing consumers' names, addresses, credit card numbers, bank account numbers, and debt-related information alleged to be unfair) (discussed *supra* Section II(E)(3)).

380 *See, e.g.*, First Amended Complaint for Injunctive and Other Equitable Relief ¶¶ 24(c), 44-49, *FTC v. Wyndham Worldwide Corp.*, No. 2:12-cv-01365-PGR (D. Ariz. Aug. 9, 2012), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2012/08/120809wyndhamcmpt.pdf (allowing hotels to connect to network without ensuring that they implemented adequate information security policies and procedures alleged to be unfair and contrary to company's claims).

procedural safeguards that comply with federal standards."[381] When hackers accessed the client's system, they stole its remote login credentials and used those to obtain consumers' sensitive personal information.[382]

Similarly, in the agency's first action against LifeLock, the FTC alleged that the business's failure to install antivirus programs on computers that employees used to remotely access Lifelock's network was inconsistent with the company's claim that it used "highly secure physical, electronic, and managerial procedures."[383] The consent order in *In re Lifelock* requires the company, and its two co-founders, to establish a comprehensive information security program and to obtain independent third-party assessments every two years.[384] In 2015, the FTC filed a contempt action against LifeLock for violating the 2010 settlement by, among other things, failing to establish and maintain a comprehensive information security program and falsely advertising that it protected consumers' sensitive data with the same high-level safeguards as financial institutions.[385] Lifelock settled the action, agreeing to pay $100 million in equitable monetary relief.[386]

The FTC recommends that companies consider using encryption if they allow remote access to the computer network by employees or by service providers.[387]

(4) Sensitive Information

Through its guidance and enforcement actions, the FTC has identified several types of information that benefit from strong encryption during storage or transmission. Passwords and credentials, for example, must be stored securely.[388] Biometric data may

---

381 Complaint ¶¶ 1, 19-21, *In re Premier Capital Lending, Inc.*, No. C-4241 (F.T.C. Dec. 10, 2008), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2008/12/081206pclcmpt.pdf.

382 *Id.*

383 Complaint ¶¶ 19(f), 20(f), 35-37, *FTC v. LifeLock, Inc.*, No. 2:10-cv-00530-MGM (D. Ariz. Mar. 8, 2010), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2010/03/100309lifelockcmpt.pdf.

384 Stipulated Final Judgment and Order for Permanent Injunction and Other Equitable Relief as to Defendants Lifelock and Davis §§ II, III, *FTC v. LifeLock, Inc.*, No. 2:10-cv-00530-MGM (D. Ariz. Mar. 9, 2010), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2010/03/100309lifelockstip.pdf; Stipulated Final Judgment and Order for Permanent Injunction and Other Equitable Relief as to Defendant Maynard §§ II, III, *FTC v. LifeLock, Inc.*, No. 2:10-cv-00530-MGM (D. Ariz. Mar. 9, 2010), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2010/03/100309maynardstip.pdf.

385 Notice of Lodging Proposed Documents Under Seal at 1-2, *FTC v. LifeLock, Inc.*, 2:10-cv-00530-MHM (D. Ariz. July 21, 2015), *available at* https://www.ftc.gov/system/files/documents/cases/150721lifelocknotice.pdf.

386 Amended Order at 4, *FTC v. LifeLock, Inc.*, 2:10-cv-00530-MHM (D. Ariz. Jan. 4, 2016), *available at* https://www.ftc.gov/system/files/documents/cases/160105lifelockorder.pdf.

387 Fed. Trade Comm'n, Protecting Personal Information 15 (2011), *available at* https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf.

388 *See, e.g.*, Complaint ¶¶ 10(e), 14, *In re Reed Elsevier Inc.*, No. C-4226 (F.T.C. July 29, 2008), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2008/08/080801reedcomplaint.pdf (allowing customers to store user credentials in a vulnerable format alleged to be unfair); *In re Guidance Software, Inc.*, 143 F.T.C. 532, 535-36 (2007) (complaint) (storing network user credentials in clear, readable text alleged to be deceptive in light of company's claims).

also require some form of protection.[389] FTC guidance also makes clear that companies should encrypt sensitive information that is sent to third parties over public networks and should consider encrypting sensitive information stored on internal computer networks, disks, or portable storage devices.[390] For mobile applications, the agency recommends transit encryption for usernames, passwords, and other important data, such as application programming interface (API) keys.[391]

b. Physical Security

The physical security of information is also an important component of reasonable security. In *In re Lifelock*, the agency alleged that the company's practice of leaving faxed documents containing consumers' personal information in an open and easily accessible area contradicted the company's security representations.[392] Similarly, in *In re Gregory Navone*, the FTC charged that the mortgage broker's storage of sensitive consumer information in boxes in his garage, among other practices, violated the FCRA and contradicted the company's claims.[393]

The FTC has stated that it expects companies and their employees and service providers to take measures to protect paper and other physical materials containing personal information.[394] The agency recommends that paper documents containing personal information be stored in a locked room or container, and that access to the locked areas and containers be limited to employees with a legitimate business need.[395] As for the physical security of laptops and portable devices, the agency advises that they be stored in a secure place.[396] If a company stores consumer data on other portable devices, it

---

389 Fed. Trade Comm'n, Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies 17 (2012), *available at* http://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf ("[E]ven if a company does not itself intend to implement facial recognition technologies, it should consider putting protections in place that would prevent unauthorized scraping of the publicly available images it stores in its online database.").

390 Fed. Trade Comm'n, Protecting Personal Information 10 (2011), *available at* https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf.

391 Fed. Trade Comm'n, Mobile App Developers: Start with Security (2013), *available at* http://business.ftc.gov/documents/bus83-mobile-app-developers-start-security ("If you use HTTPS, use a digital certificate and ensure your app checks it properly.").

392 Complaint ¶¶ 20(h), 35-37, *FTC v. LifeLock, Inc.*, No. 2:10-cv-00530-MGM (D. Ariz. Mar. 8, 2010), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2010/03/100309lifelockcmpt.pdf.

393 Complaint for Civil Penalties, Injunction, and Other Equitable Relief ¶¶ 12-14, 15-16, 19-25, *FTC v. Navone*, No. 2:08-cv-01842 (D. Nev. Dec. 30, 2009), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2009/01/090121navonecmpt.pdf.

394 Fed. Trade Comm'n, Commission Statement Marking the FTC's 50th Data Security Settlement 1 (Jan. 31, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf; Fed. Trade Comm'n, Start with Security 13 (2015), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf; Fed. Trade Comm'n, Protecting Personal Information 8-9 (2011), *available at* https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0 pdf.

395 Fed. Trade Comm'n, Protecting Personal Information 8-9 (2011), *available at* https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf.

396 *Id* . at 13.

may also want to consider adding an "auto-destroy" function so that any data on a stolen device will be destroyed if an unauthorized individual tries to use it.[397]

4. Ongoing Monitoring

The FTC has stated that it expects companies to implement security on an ongoing basis.[398] Indeed, the agency has brought numerous actions against companies for failing to monitor the security of its service providers, activity on their networks, and security issues reported by consumers, researchers, or other third parties.

a. Network Activity

The FTC has brought numerous actions in which companies allegedly increased the risk or scope of a data breach by failing to monitor activity on their networks or to employ sufficient measures to detect unauthorized access.[399] In *In re Dave & Busters*, the FTC alleged that the company's failure to use an intrusion detection system and to monitor system logs for suspicious activity was unfair.[400] According to the complaint, an intruder was able to connect numerous times to the company's networks, to install unauthorized software, and to intercept personal information in transit from in-store networks to the company's credit

---

397 Fed. Trade Comm'n, Protecting Personal Information 13 (2011), *available at* https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf.

398 *See, e.g.*, Fed. Trade Comm'n, Start with Security 8 (2015), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf

399 *See, e.g.*, First Amended Complaint for Injunctive and Other Equitable Relief ¶¶ 24(g), 27, *FTC v. Wyndham Worldwide Corp.*, No. 2:12-cv-01365-PGR (D. Ariz. Aug. 9, 2012) *available at* http://www.ftc.gov/sites/default/files/documents/cases/2012/08/120809wyndhamcmpt.pdf (failure to employ reasonable measures to detect and prevent unauthorized access to network or to conduct security investigations alleged to be unfair and contrary to company's claims); Complaint ¶ 6, *In re EPN, Inc.*, No. C-4370 (F.T.C. June 7, 2012), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2012/10/121026epncmpt.pdf (failure to scan networks to identify unauthorized P2P file sharing applications on networks and failure to adequately log network activity and inspect outgoing transmissions alleged to be unfair); *In re Ceridian Corp.*, 151 F.T.C. 514, 516 (2011) (failure to employ reasonable measures to detect and prevent unauthorized access to personal information alleged to be unfair and contrary to company's claims); *In re Lookout Servs., Inc.*, 151 F.T.C. 532, 535 (2011) (complaint) (failure to employ sufficient measures to detect and prevent unauthorized access to computer networks, such as by employing an intrusion detection system and monitoring system logs, alleged to be unfair and contrary to company's claims); *In re Life Is Good, Inc.*, 145 F.T.C. 192, 194 (2008) (complaint) (failure to use readily available security measures to monitor and control connections from network to the internet and failure to employ reasonable measures to detect unauthorized access alleged to be contrary to company's claims); *In re CardSystems Sols., Inc.*, 142 F.T.C. 1019, 1021 (2006) (complaint) (failure to employ sufficient measures to detect unauthorized access to personal information or to conduct security investigations alleged to be unfair); *In re Nations Title Agency, Inc.*, 141 F.T.C. 323, 325, 327 (2006) (complaint) (failure to employ reasonable measures to detect and respond to unauthorized access to personal information or to conduct security investigations alleged to be contrary to company's claims); *In re BJ's Wholesale Club, Inc.*, 140 F.T.C. 465, 467 (2005) (complaint) (failure to employ sufficient measures to detect unauthorized access or conduct security investigations alleged to be unfair); *In re Microsoft Corp.*, 134 F.T.C. 709, 712 (2002) (complaint) (failure to implement reasonable and appropriate procedures to detect possible unauthorized access, failure to monitor system for potential vulnerabilities, and failure to record and retain system information sufficient to perform security audits and investigations alleged to be contrary to company's claims) (discussed *supra* Section II(A)(2)).

400 *In re Dave & Buster's, Inc.*, 149 F.T.C. 1449, 1451-52 (2010) (complaint).

card processing company—all of which allegedly led to several hundred thousand dollars of fraudulent charges on consumers' credit and debit cards.[401]

As these cases make clear, companies should monitor for unusual activity, including multiple failed login attempts from unknown users or computers and higher-than-average traffic.[402] The FTC also recommends that companies use an intrusion detection system and maintain a central log file of security-related information, which can help identify compromised computers if there is an attack.[403]

b. Service Providers and Clients

The FTC has stated that it expects companies to retain service providers that are capable of maintaining reasonable security and to monitor or verify that those service providers are indeed complying with the company's security requirements.[404] In *United States v. ChoicePoint Inc.*, the agency alleged as deceptive and unfair the data broker's failure to identify unauthorized activity by subscribers, even after receiving subpoenas from law enforcement authorities alerting the company to fraudulent subscriber accounts.[405] Similarly, in *In re Premier Capital Lending*, the agency alleged that the mortgage lender's failure to use readily available information to review access requests made by one account, such as spikes in the number of requests or blatant irregularities in the information used to make the requests, contradicted Premier Capital's representations that it used reasonable and appropriate data security measures.[406]

The FTC has brought several actions against companies for failing to include contractual provisions that require a service provider to adopt reasonable security precautions.[407] In *In re GMR Transcription Services*, the company hired service providers to transcribe sensitive audio files, but failed to require those providers to take reasonable

---

401 *Id.*

402 Fed. Trade Comm'n, Protecting Personal Information 16 (2011), *available at* https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf.

403 *Id.*

404 Fed. Trade Comm'n, Start with Security 11 (2015), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf; Fed. Trade Comm'n, Internet of Things: Privacy & Security in a Connected World iii (2015), *available at* https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

405 Complaint ¶¶ 14, 25-32, *United States v. ChoicePoint Inc.*, No. 06-CV-0198 (N.D. Ga. Jan. 30, 2006), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2006/01/0523069complaint.pdf.

406 Complaint ¶¶ 14(c), 19-21, *In re Premier Capital Lending, Inc.*,, No. C-4241 (F.T.C. Dec. 10, 2008), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2008/12/081206pclcmpt.pdf.

407 *See, e.g.*, Complaint ¶¶ 29(B), 31-33, *In re Genelink, Inc.*, Nos. C-4456, C-4457 (F.T.C. May 8, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140512genelinkcmpt.pdf (failure to require, by contract, that service providers implement and maintain appropriate safeguards for consumers' personal information alleged to be unfair and contrary to company's claims); Complaint for Civil Penalties, Injunction, and Other Equitable Relief ¶¶ 11, 17-18, *FTC v. Navone*, No. 2:08-cv-01842 (D. Nev. Dec. 30, 2008), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2009/01/090121navonecmpt.pdf (failure to enter into agreements requiring service providers to safeguard information alleged to be contrary to company's claims).

security measures, which enabled hackers to post on the internet many files containing consumers' confidential health-related information.[408]

The FTC has also taken action against companies that failed to verify that their service provider actually complied with security requirements.[409] For example, in *In re Upromise*, the company purportedly claimed that its toolbar, which collected consumers' browsing information, would use a filter to remove any personally identifiable information before transmission.[410] According to the FTC, however, Upromise failed to verify that the service provider hired to create the toolbar actually implemented the promised security.[411] As a result, the toolbar collected sensitive personal information, including financial account numbers, and transmitted that information in clear text.[412] The agency alleged that this failure was unfair and contrary to Upromise's representations that it encrypted information transmitted by consumers using the toolbar and that it took other reasonable measures to protect consumer data.[413] For additional discussion of the case, see *supra* Section II(C)(1)(b).

In its guidance, the FTC recommends investigating a service provider's data security practices, for example, by visiting their facilities.[414] It also advises that companies consider requiring service providers to give notification of any security incidents, even if the incident may not have led to an actual compromise of company data.[415]

---

408 Complaint ¶¶ 11-13, 17-21, *In re GMR Transcription Servs., Inc.*, No. C-4482 (F.T.C. Aug. 14. 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140821gmrcmpt.pdf.

409 *See, e.g.*, Fed. Trade Comm'n, Start with Security 11 (2015), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf; Complaint ¶¶ 29(C), 30, 31-33, *In re Genelink, Inc.*, Nos. C-4456, C-4457 (F.T.C. May 8, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140512genelinkcmpt.pdf (failure to provide reasonable oversight of service providers, for instance by requiring that they implement simple, low-cost, and readily available defenses to protect consumers' personal information, alleged to be unfair and contrary to company's claims); *In re Nations Title Agency, Inc.* 141 F.T.C. 323, 325, 327-28 (2006) (complaint) (failure to provide reasonable oversight of service providers' handling of personal information alleged to be unfair and contrary to company's claims).

410 Complaint ¶¶ 5, 14(d), *In re Upromise, Inc.*, No. C-4351 (F.T.C. Mar. 27, 2012), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2012/04/120403upromisecmpt.pdf.

411 *Id.* ¶¶ 10, 14(a).

412 *Id.* ¶¶ 16-21.

413 *Id.* ¶¶ 16-21.

414 Fed. Trade Comm'n, Protecting Personal Information 19 (2011), *available at* https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf.

415 *Id.*

c. Security Complaints and Reports

Companies that lack a process for receiving and addressing security-related reports and complaints also been the subject of FTC enforcement.[416] In *In re TRENDnet*, the company allegedly failed to implement any process to monitor security vulnerability reports from third parties such as researchers and academics, despite the availability of free tools to conduct such monitoring.[417] In *In re Fandango*, the company relied on its general customer service system to respond to warnings about security risks, which led to a report from a security researcher being incorrectly marked as "resolved" without being flagged for further review.[418]

The FTC recommends that companies review and address complaints and reports of security vulnerabilities, and that they use a dedicated email address, like "security@yourcompany.com," to receive such submissions.[419]

5. Addressing Common Vulnerabilities

Companies' failures to test for and address commonly known and reasonably foreseeable vulnerabilities have led to FTC enforcement. For example, in *In re Lookout Services*, the FTC charged that the company failed to adequately test its web application for widely known security flaws, including one called "predictable resource location," which enables users to easily predict patterns and manipulate URLs in order to gain access to secured web pages.[420] As a result, a hacker could bypass the web application's authentication screen and gain unauthorized access to the company's databases.[421]

In other actions, the FTC alleged that companies failed to assess their applications for well-known vulnerabilities, such as Structured Query Language (SQL) injection attacks

---

416 *See, e.g.*, Fed. Trade Comm'n, Start with Security 12 (2015), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf; Complaint ¶ 30(e), *In re ASUSTeK Comput. Inc.*, No. C-4587 (F.T.C. July 18, 2016), *available at* https://www.ftc.gov/system/files/documents/cases/1607asustekcmpt.pdf (failure to maintain an adequate process for receiving and addressing security vulnerability reports from third parties alleged to be unfair and contrary to company's claims); *In re HTC America Inc.*, 155 F.T.C. 1617, 1619 (2013) (complaint) (lack of process for receiving and addressing reports about security vulnerabilities alleged to be unfair and contrary to the company's claims).

417 Complaint ¶ 8(c), No. C-4426 (F.T.C. Jan. 16, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140207trendnetcmpt.pdf.

418 Complaint ¶ 17, *In re Fandango, LLC*, No. C-4481 (F.T.C. Aug. 13, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140819fandangocmpt.pdf.

419 Fed. Trade Comm'n, Start with Security 12 (2015), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf; Fed. Trade Comm'n, Mobile App Developers: Start with Security (2013), *available at* http://business.ftc.gov/documents/bus83-mobile-app-developers-start-security.

420 *In re Lookout Servs., Inc.*, 151 F.T.C. 532, 535 (2011) (complaint).

421 *Id.* at 534-536.

or Cross-Site Scripting (XSS) attacks.[422] In *In re Guess*, the FTC alleged that the retailer failed to protect against SQL injection and other commonly known attacks by failing to test or otherwise assess its website's vulnerability to such attacks.[423]

a. Industry-Tested and Accepted Methods

Failure to use industry-tested and accepted methods is a factor in assessing the reasonableness of a company's data security practices.[424] For example, in *In re ValueClick*, the FTC alleged that the company stored sensitive customer information collected online in a database that used non-standard encryption.[425] Unlike widely accepted encryption algorithms that are extensively tested, ValueClick's method allegedly used a simple alphabetic substitution system that was subject to significant vulnerabilities.[426] The agency charged that the use of this weaker method, among other practices, was inconsistent with the company's representation that it used industry-standard security measures.[427] The FTC further alleged that ValueClick violated the CAN-SPAM Act by sending consumers emails with deceptive subject headers.[428] ValueClick agreed to pay a $2.9 million civil penalty to settle the charges.[429]

Failure to use inexpensive, readily available tools to improve security is another factor in assessing reasonableness. In *In re Petco* and in *In re Life is Good*, the FTC alleged that the companies' respective failures to use simple, readily available, and low-cost defenses that would have blocked SQL injection attacks was contrary to the companies'

---

422 *See, e.g.*, *In re Life Is Good, Inc.*, 145 F.T.C. 192, 194 (2008) (complaint) (failure to adequately assess the vulnerability of web application and network to SQL injection attacks alleged to be inconsistent with company's representations); *In re Cardsystems Sols., Inc.*, 142 F.T.C. 1019, 1021 (2006) (complaint) (failure to adequately assess the vulnerability of web application and computer network to SQL injection attacks alleged to be unfair); *In re Ceridian Corp.*, 151 F.T.C. 514, 516 (2011) (failure to protect network from SQL attacks alleged to be unfair and contrary to the company's claims); Complaint for Civil Penalties, Permanent Injunction, and Other Relief ¶ 16, *United States v. RockYou, Inc.*, No. CV-12-1487 (N.D. Cal. Mar. 26, 2012), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2012/03/120327rockyoucmpt.pdf (failure to protect website from commonly known or reasonably foreseeable attacks such as SQL injection attacks or XSS attacks contradicted company's claims).

423 *In re Guess?, Inc.*, 136 F.T.C. 507, 510, 512 (2003) (complaint).

424 *See, e.g.*, Complaint ¶ 8, *In re Henry Schein Practice Sols., Inc.*, No. C-4575 (F.T.C. May 20, 2016), *available at* https://www.ftc.gov/system/files/documents/cases/160105scheincmpt.pdf (use of data masking, instead of encryption, contradicted company's claim that it used industry-standard encryption and that its product helped to protect patient data as required by HIPAA).

425 Complaint for Civil Penalties, Permanent Injunction, and Other Equitable Relief ¶¶ 41, 47-48, *United States v. ValueClick, Inc.*, No. CV08-01711MMM(RZx) (C.D. Cal. Mar. 13, 2008), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2008/03/080317complaint.pdf.

426 *Id.*

427 *Id.* ¶¶ 38-39.

428 *Id.* ¶¶ 33, 55-56.

429 Stipulated Final Judgment for Civil Penalties and Permanent Injunctive Relief at 8, *United States v. ValueClick, Inc.*, No. CV08-01711MMM(RZx) (C.D. Cal. Mar. 13, 2008), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2008/03/080317judgment.pdf.

data security claims.[430] Similarly, in *In re HTC*, the agency alleged that the mobile device manufacturer not only used less secure methods for protecting communications, but also failed to use simple code to fix its device vulnerabilities.[431] The agency alleged that these practices, among others, were unfair and contrary to HTC's claims.[432] The consent order requires HTC to develop security patches to fix its various security vulnerabilities and to notify consumers about the availability of the patches.[433]

Consistent with its enforcement actions, FTC guidance recommends that companies use methods for addressing security vulnerabilities that experts already have tested and found to be effective.[434]

b. Platform Guidelines and Settings

The extent to which a company follows platform guidelines or security protections built into operating systems may also be a factor in assessing the reasonableness of a security practice. The FTC's complaints in *In re Fandango* and *In re Credit Karma* also charged the companies with failing to follow iOS and Android security guidelines for developers.[435] Likewise, in *In re HTC*, the agency alleged that the company undermined the Android operating system's permissions-based model by pre-installing an app that, if exploited, would give any third-party app access to the phone's microphone.[436] According to the complaint, HTC also pre-installed another app that could download and install apps outside of the normal Android permission process.[437]

The FTC recommends that companies understand and follow platform guidelines and security protections built into operating systems.[438] Where necessary, companies may have to implement security measures beyond those offered by the platform.[439]

---

430 *In re Life Is Good, Inc.*, 145 F.T.C. 192, 194 (2008) (complaint); *In re Petco Animal Supplies, Inc.*, 139 F.T.C. 102, 105-06 (2005) (complaint).

431 *In re HTC America Inc.*, 155 F.T.C. 1617, 1620-21, 1625 (2013) (complaint).

432 *Id.* at 1627-28.

433 *In re HTC America Inc.*, 155 F.T.C. 1617, 1631-35 (2013) (decision and order).

434 Fed. Trade Comm'n, Start with Security 6 (2015), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

435 *See supra* Section III(D)(3)(a).

436 *In re HTC America Inc.*, 155 F.T.C. 1617, 1620-21 (2013) (complaint).

437 *Id.*

438 Fed. Trade Comm'n, Start with Security 10 (2015), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf; Fed. Trade Comm'n, Mobile App Developers: Start with Security (2013), *available at* http://business.ftc.gov/documents/bus83-mobile-app-developers-start-security.

439 Fed. Trade Comm'n, Mobile App Developers: Start with Security (2013), *available at* http://business.ftc.gov/documents/bus83-mobile-app-developers-start-security.

c. Third-Party Software

The FTC has taken action against companies that failed to update and patch third-party software.[440] In *In re TJX Companies*, the FTC alleged that the retailer failed to patch or update its anti-virus software, increasing the risk that hackers could exploit known vulnerabilities or overcome the company's defenses.[441] An intruder allegedly exploited this and other failures, compromising tens of millions of consumer credit and debit payment cards.[442]

The FTC recommends that companies establish a reasonable process to regularly update and patch third party software.[443] Such a process may involve regularly checking expert websites and software vendors' websites for alerts about new vulnerabilities, as well as implementing policies for installing vendor-approved patches.[444] Companies may also want to follow general and library-specific mailing lists and create a plan for shipping security updates to consumers, if necessary.[445] In the context of the Internet of Things (IOT), the FTC has asked companies to pay particular attention to patching known vulnerabilities where feasible.[446] As the agency explained, many "[IOT] devices have a limited life cycle, resulting in a risk that consumers will be left with out-of-date [IOT] devices that are vulnerable to critical, publicly known security or privacy bugs."[447]

---

440 *See, e.g.*, Fed. Trade Comm'n, Start with Security 12 (2015), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf; Fed. Trade Comm'n, Protecting Personal Information 10, 17 (2011), *available at* https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf; Complaint ¶¶ 20(d), 35-37, *FTC v. LifeLock, Inc.*, No. 2:10-cv-00530-MGM (D. Ariz. Mar. 8, 2010), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2010/03/100309lifelockcmpt.pdf (failure to use readily available security measures to routinely prevent unauthorized access to personal information, such as by installing patches and critical updates on its network, contradicted company's security claims).

441 Complaint ¶ 8(e), *In re TJX Cos., Inc.*, No. C-4227 (F.T.C. July 29, 2008), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2008/08/080801tjxcomplaint.pdf.

442 *Id.* ¶¶ 9-11.

443 Fed. Trade Comm'n, Start with Security 12 (2015), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf Fed. Trade Comm'n, Mobile App Developers: Start with Security (2013), *available at* http://business.ftc.gov/documents/bus83-mobile-app-developers-start-security.

444 Fed. Trade Comm'n, Protecting Personal Information 10 (2011), *available at* https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf.

445 Fed. Trade Comm'n, Mobile App Developers: Start with Security (2013), *available at* http://business.ftc.gov/documents/bus83-mobile-app-developers-start-security.

446 Fed. Trade Comm'n, Internet of Things: Privacy & Security in a Connected World iii (2015), *available at* https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

447 *Id.* at 31.

6. Planning for Security Incidents

The agency has brought several actions against companies for failing to establish a plan for responding to security incidents.[448] In *In re EPN, Inc.*, the agency alleged as unfair the debt collector's failure to adopt an appropriate information security plan, including any type of "incident response plan."[449] These failures, among others, allegedly led to the disclosure of files containing financial and health information about thousands of debtors, including social security numbers, employer addresses, and in the case of healthcare clients, physician names, insurance numbers, and diagnosis codes, on a public P2P network.[450]

Planning for security incidents may also require establishing policies and procedures for notifying affected consumers. The FTC brought an action against ASUSTeK Computer for failing to notify customers of firmware updates until well after the company learned of the issues.[451] The agency alleged that the failure was unfair and contrary to ASUSTeK's data security promises.[452]

The FTC recommends that companies create a plan for responding to security incidents that includes investigating security incidents immediately, closing off vulnerabilities and threats to personal information, knowing whom to notify in the event of an incident, and designating a senior employee to coordinate and implement the plan.[453]

7. Training and Designating People

In many ways, the lynchpin to implementing reasonable data security is people—people who design, create, and update products and services, people who interact with consumer information, and people who establish and carry out policies and procedures needed to effect sound security. The centrality of people to sound security helps to

---

448 *See, e.g.*, First Amended Complaint for Injunctive and Other Equitable Relief ¶ 24(i), *FTC v. Wyndham Worldwide Corp.*, No. 2:12-cv-01365-PGR (D. Ariz. Aug. 9, 2012), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2012/08/120809wyndhamcmpt.pdf (failure to follow proper incident response procedures, including failing to monitor computer network for malware used in a previous intrusion, alleged to be unfair and contrary to company's claims); Complaint ¶ 8(b), *In re Franklin's Budget Car Sales, Inc.*, No. C-4371 (F.T.C. Oct. 3, 2012), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2012/10/121026franklinautomallcmpt.pdf (failure to adopt an incident response plan alleged to be deceptive in light of company's claims).

449 Complaint ¶¶ 6, 11 *In re EPN, Inc.*, No. C-4370 (F.T.C. June 7, 2012), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2012/10/121026epncmpt.pdf.

450 *Id.* ¶¶ 8, 10.

451 Complaint ¶ 13, *In re ASUSTeK Comput. Inc.*, No. C-4587 (F.T.C. July 18, 2016), *available at* https://www.ftc.gov/system/files/documents/cases/1607asustekcmpt.pdf.

452 *Id.* ¶ 30(g).

453 Fed. Trade Comm'n, Protecting Personal Information 22-23 (2011), *available at* https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf; *see also* Fed. Trade Comm'n, Start with Security 1 (2015), *available at* ,https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

explain why the FTC has taken action against companies for failing to adequately train employees and service providers on data security.[454]

Some cases highlight the importance of employee training in secure information disposal.[455] Other cases make clear the importance of offering training in secure coding. In *In re TRENDnet*, the FTC alleged as unfair and deceptive the company's failure to implement reasonable guidance or training to employees responsible for testing, designing, and reviewing the security of its IP cameras and related software.[456] Similarly, in *In re HTC America*, the FTC alleged as unfair and deceptive the company's failure to implement adequate privacy and security guidance or training for its engineering staff.[457] This purportedly contributed to the company's failure to implement readily available secure communication mechanisms in its logging applications, which allowed malicious third-party apps to communicate with the logging application and placed consumers' text messages, location data, and other sensitive information at risk.[458]

---

454 *See, e.g.*, Complaint ¶¶ 8, 13-14, *In re Franklin's Budget Car Sales, Inc.*, No. C-4371 (F.T.C. Oct. 3, 2012), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2012/10/121026franklinautomallcmpt.pdf (failure to adequately train employees about information security alleged to be deceptive in light of company's claims); Complaint ¶¶ 6, 11 *In re EPN, Inc.*, No. C-4370 (F.T.C. June 7, 2012), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2012/10/121026epncmpt.pdf (failure to adequately train employees about security alleged to be unfair); Complaint ¶¶ 14(c), 18-20, *In re Upromise, Inc.*, No. C-4351 (F.T.C. Mar. 27, 2012), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2012/04/120403upromisecmpt.pdf (failure to ensure that employees responsible for information collection program received adequate training about security risks and policies alleged to be unfair and contrary to company's claims) (discussed *supra* Section II(C)(1)(b)); Complaint for Civil Penalties, Injunction, and Other Equitable Relief ¶¶ 11, 13, 15-16, *FTC v. Navone*, No. 2:08-cv-01842 (D. Nev. Dec. 30, 2009), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2009/01/090121navonecmpt.pdf (failure to alert employees or third parties to sensitivity of consumer information, or to instruct them to take precautions with information, alleged to be contrary to company's claims); *In re MTS, Inc.*, 137 F.T.C. 444, 448 (2004) (complaint) (failure to provide appropriate training and oversight for employees regarding application vulnerabilities and security testing alleged to be contrary to company's claims); *In re Eli Lilly & Co.*, 133 F.T.C. 763, 767-68 (2002) (failure to adequately train employees regarding consumer privacy and information security and failure to properly oversee and to assist an employee who sent out an email containing email addresses of 669 people who used Prozac.com alleged to be contrary to company's claims).

455 *See, e.g.*, *In re Rite Aid Corp.*, 150 F.T.C. 694, 696-97 (2010) (complaint) (failure to adequately train employees to dispose personal information securely alleged to be unfair and contrary to the company's claims); Complaint ¶¶ 7, 9-11, *In re CVS Caremark Corp.*, No. C-4259 (F.T.C. June 18, 2009), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2009/06/090623cvscmpt.pdf (failure to adequately train employees to dispose personal information securely alleged to be unfair and contrary to the company's claims); Complaint ¶¶ 5, 11-13, *In re Nations Title Agency, Inc.* (F.T.C. June 19, 2006), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2006/06/0523117nationstitle_complaint.pdf (failure to implement reasonable policies and procedures in employee training about handling of personal information alleged to be contrary to company's claims).

456 Complaint ¶ 8(d)(ii), *In re TrendNET*, No. C-4426 (Jan. 16, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140207trendnetcmpt.pdf.

457 *In re HTC America Inc.*, 155 F.T.C. 1617, 1619 (2013) (complaint).

458 *Id.* at 1621-23.

The FTC has offered several points of guidance on employee training.[459] One is to create a "culture of security" by implementing a regular schedule of training for staff.[460] Such training could include updates about new security risks and vulnerabilities, explanations of why passwords should not be shared, and explanations of why sensitive personal data should not be transmitted via unsecured email.[461] If an employee fails to attend trainings, companies should consider blocking that person's access to the network.[462]

The FTC also recommends that companies designate persons(s) responsible for security, including those at appropriate levels of responsibility within an organization.[463] In the mobile app context, for example, the agency recommends that a developer team include at least one person responsible for considering security at every stage of an app's development.[464]

The agency also offers a series of free, plain-language videos discussing tips and lessons from the agency's law enforcement actions.[465] Companies can use these videos, as well as FTC reports, guides, and blogs, to help employees understand how to implement reasonable data security throughout the organization.

---

459 Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers 30 (2012), *available at* https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf; Fed. Trade Comm'n, Internet of Things: Privacy & Security in a Connected World 29 (2015), *available at* https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf; *see also* Fed. Trade Comm'n, Start with Security 9 (2015), *available at* ,https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf Fed. Trade Comm'n, Protecting Personal Information 18 (2011), *available at* https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf.

460 Fed. Trade Comm'n, Protecting Personal Information 18 (2011), *available at* https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf.

461 *Id.* at 12-13, 18.

462 *Id.* at 18.

463 *Id.*

464 Fed. Trade Comm'n, Mobile App Developers: Start with Security (2013), *available at* http://business.ftc.gov/documents/bus83-mobile-app-developers-start-security.

465 The videos are available at the FTC's webpage for the Start with Security initiative. Fed. Trade Comm'n, *Start with Security*, https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business (last visited Mar 22, 2016).

IV. CONCLUSION

The FTC's litigated cases, public settlements, and guidance materials are key to understanding the agency's Section 5 privacy and data security enforcement. This article provided an introductory framework to sketch the boundaries of Section 5 liability in this area. Sections II and III offered a bird's-eye view of a number of relevant FTC enforcement actions involving a wide variety of privacy and data security issues. There is of course no substitute for consulting the complaints, consent orders, guidance, and other materials—almost all of which are available online at www.ftc.gov.