American University Law Review

Volume 62 | Issue 5 Article 8

2013

FTC v. LabMD: FTC Jurisdiction over Information Privacy Is Plausible, But How Far Can It Go

Peter S. Frechette
American University Washington College of Law

FTC v. LabMD: FTC Jurisdiction over Information Privacy Is Plausible, But How Far Can It Go

Keywords
United States. Federal Trade Commission Act, Subpoena, United States. Federal Trade Commission -- Trials, litigation, etc., Jurisdiction -- United States -- Cases, Data security failures -- Lawsuits & claims, United States. District Court (Georgia : Northern District), Cyberspace -- Security measures, Actions & defenses (Law) -- United States

NOTES

FTC V. LABMD: FTC JURISDICTION OVER INFORMATION PRIVACY IS "PLAUSIBLE," BUT HOW FAR CAN IT GO?

PETER S. FRECHETTE*

TABLE OF CONTENTS

INTRODUCTION

Companies in nearly every industry collect, store, and use personal information from consumers. Recently, company databases have become the target of increasingly sophisticated attacks aimed at

* Editor-in-Chief, *American University Law Review*, Volume 62; J.D. candidate, May 2013, *American University Washington College of Law*; B.A., Linguistics and Philosophy, *University of Maryland*, May 2010. I am grateful for the support of my family, especially my wife, Clarise. I would like to thank the editors and staff of the *American University Law Review* for their careful work on this Note, in particular Brian Shearer, Kat Scott, Jay Curran, and Katie Wright. Any remaining errors are mine alone.

stealing this information. Data breaches occur with such regularity that the Federal Bureau of Investigation (FBI) has separated companies into two categories: "those that have been hacked, and those that will be."[1] The Federal Trade Commission (FTC) plays a large role in the cybersecurity world by enforcing specific statutes and, more generally, utilizing its authority under the Federal Trade Commission Act[2] (FTC Act) to penalize companies that allow data breaches.

Recently, however, businesses have begun to push back, contesting the FTC's authority to police information security. In *FTC v. LabMD, Inc.*,[3] a company under FTC investigation for an alleged data breach challenged the FTC's ability to issue an administrative subpoena.[4] LabMD indirectly disputed the FTC's role in information security and its use of the unfairness category of the FTC Act as a basis of enforcement in data breach cases.[5] The district court ultimately found that the FTC made a plausible case for its authority, but based its holding on the weight of precedent surrounding the FTC's general use of the FTC Act in information security cases.[6] Thus, the FTC's reliance on the FTC Act is currently permitted, but could be challenged in the future.

LabMD's challenge of the FTC's authority was significant however, because there is no legislative or executive action on privacy, so the FTC's guidance, best practices, and enforcement set the de facto "privacy law."[7] As the FTC casts an increasingly wider net with or without congressional or executive action on data security, the future of the FTC Act's scope in this area is uncertain.

---

1. Stacy Cowley, *FBI Director: Cybercrime Will Eclipse Terrorism*, CNNMONEY (Mar. 2, 2012, 7:55 AM), http://money.cnn.com/2012/03/02/technology/fbi_cybersecurity/index.htm. The Director went on to say "[e]ven that is merging into one category: those that have been hacked and will be again." *Id.*

2. 15 U.S.C. §§ 41–58 (2006, Supp. IV 2011, & Supp. V 2012).

3. No. 1:12-cv-3005 (N.D. Ga. Nov. 26, 2012).

4. *Id.* at 4 (outlining MDLab's attempts to quash the FTC subpoena).

5. *See* Brief in Opposition to Petition of the Federal Trade Commission for an Order To Enforce Civil Investigative Demands at 2–3, FTC v. LabMD, Inc., No. 1:12-cv-3005 (N.D. Ga. Nov. 26, 2012), ECF No. 13 (arguing that the FTC does not have jurisdiction over data security generally).

6. *Id.* at 12–14.

7. *See* Michael D. Scott, *The FTC, the Unfairness Doctrine, and Data Security Breach Litigation: Has the Commission Gone Too Far?*, 60 ADMIN. L. REV. 127, 145–49 (2008) ("The [FTC] has taken the lead in the United States in regulating privacy issues online.").

I. BACKGROUND

The FTC Act declares "unfair or deceptive acts or practices in or affecting commerce" to be unlawful.[8] The FTC has used both the "deceptive" and "unfair" categories of the FTC Act in data security cases.[9] These cases typically involve settlement discussions in which the company enters into a consent order with the FTC.[10] The consent orders are published for public comment, and, if acceptable, are approved by the FTC.[11] In the settlement, the FTC typically sets a privacy framework and retains the ability to review the company. For example, in a consent order with Google, Inc.,[12] the FTC included the enactment of a comprehensive privacy program as a term in the settlement of the action.[13] The FTC went further in a consent order with Facebook, Inc.[14] when it required Facebook to follow the U.S.-EU Safe Harbor Principles[15] in addition to enacting a privacy program.[16] These settlement and enforcement mechanisms can be controversial based on the FTC's broad exercise of power over information privacy and the relevant law.

A. Deception

The FTC Act lists deceptive practices that are unlawful.[17] The deception category is intended to combat statements and published policies breached or disregarded by the companies that published them.[18] The unauthorized collection of information, or collection

---

8. 15 U.S.C. § 45(a)(1) (2006).
9. *Id.*
10. *See, e.g.*, Facebook, Inc., No. C-4365, FTC File No. 092-3184 (July 27, 2012), *available at* http://www.ftc.gov/os/caselist/0923184/120810facebookdo.pdf (describing a settlement with the FTC for privacy violations); Google, Inc., No. C-4336, FTC File No. 102-3136 (Oct. 13, 2011) *available at* http://ftc.gov/os/caselist/1023136/111024 googlebuzzdo.pdf (same).
11. Facebook, Inc., No. C-4365, FTC File No. 092-3184 (Aug. 10, 2012) (statement of the Commission), *available at* http://ftc.gov/os/caselist/0923184/120810 facebookstmtcomm.pdf.
12. No. C-4336, FTC File No. 102-3136 (Oct. 13, 2011) *available at* http://ftc.gov/os/caselist/1023136/111024googlebuzzdo.pdf.
13. *Id.* at 4–7.
14. No. C-4365, FTC File No. 092-3184 (July 27, 2012), *available at* http://www.ftc.gov/os/caselist/0923184/120810facebookdo.pdf.
15. *Id.* at 4. The U.S.-EU Safe Harbor Framework allows U.S. companies to self-certify compliance with the European Commission's Directive on Data Protection, which prohibits data transfers to countries that do not have "adequate" privacy protection. *See U.S.-EU Safe Harbor Overview*, EXPORT.GOV, http://export.gov/safeharbor/eu/eg_main_018476.asp (last updated Apr. 26, 2012, 3:08 PM).
16. *Facebook*, No. C-4365, at 3–6.
17. 15 U.S.C. § 45(a)(4)(a) (2006).
18. *See* Scott, *supra* note 7, at 131 (describing the FTC's increased enforcement efforts to prevent websites from utilizing deceptive trade practices).

that extends beyond limits set by a company's stated privacy policy, is fertile ground for enforcement actions under the deception category.

Establishing a violation of the FTC Act's prohibition of deceptive practices requires a showing of a material representation or practice that is "likely to mislead consumers acting reasonably under the circumstances."[19] Additionally, the FTC Act imposes a heightened pleading requirement to prove a violation based on deceptive practices.[20]

The FTC has a relatively easy argument when it can show that a company has made promises to consumers that it has not kept. For example, the FTC leveraged a section 5 complaint into a consent decree with Google.[21] There, the FTC charged that Google's roll-out of "Google Buzz"—a social-media feature of Google's e-mail service, Gmail—allowed consumers to choose whether they took part in Google Buzz.[22] However, many consumers' personal information was added to Google Buzz despite the fact that they had opted out of the service.[23] Thus, by collecting this information without the user's permission, Google faced FTC charges for deceptive practices.[24] By finding a violation of the FTC Act when companies fail to fulfill their promises to consumers, the FTC has successfully used the deception category of section 5 against some of the largest players in the world of consumer data collection.[25]

B. Unfairness

The unfairness category of section 5 provides a broad yet more diffuse source of authority for enforcing information privacy. Under

---

19. FTC v. Stefanchik, 559 F.3d 924, 928 (9th Cir. 2009) (quoting FTC v. Gill, 265 F.3d 944, 950 (9th Cir. 2001)).

20. *See* FTC v. Ivy Capital, Inc., No. 2:11-CV-283, 2011 WL 2118626, at *3 (D. Nev. May 25, 2011) (applying the particularity requirements in Federal Rule of Civil Procedure 9(b) to a FTC Act claim for deception); FTC v. Lights of Am., Inc., 760 F. Supp. 2d 848, 853 (C.D. Cal. 2010) (same).

21. Google Inc., No. C-43436, FTC File No. 102-3136 (Oct. 13, 2011), *available at* http://ftc.gov/os/caselist/1023136/111024googlebuzzdo.pdf; *see* Francoise Gilbert, FTC v. Google*: A Blueprint for Your Next Privacy Audit*, J. INTERNET L., Dec. 2012, at 1, 15. The district court issued Google a $22.5 million civil penalty for violating the consent decree. *See* United States v. Google, Inc., CV 12-04177, 2012 WL 5833994, at *5–6 (N.D. Cal. Nov. 16, 2012).

22. Complaint at 2–3, Google Inc., No. C-4336, FTC File No. 102-3136 (Oct. 13, 2011) [hereinafter *Google* Complaint], *available at* http://www.ftc.gov/os/caselist/1023136/111024googlebuzzcmpt.pdf; *see also* Gilbert, *supra* note 21, at 15.

23. *Google* Complaint, *supra* note 22, at 2–5; *see also* Gilbert, *supra* note 21, at 15.

24. *Google* Complaint, *supra* note 22, at 5–6 (alleging that Google used personal data in a different way from its express and implied uses, constituting a deceptive act).

25. *See, e.g.*, Gilbert, *supra* note 21, at 15 (describing how the FTC filed a deception claim against Google that resulted in a record-setting $22.5 million consent decree).

the unfairness category, the company practice must injure consumers and violate established public policy.[26] Recognizing that it would be impossible to create an exhaustive list of unfair trade practices, Congress left the FTC responsible for identifying such practices.[27]

The 1980 Unfairness Statement guides the analysis of whether the Commission properly applied the unfairness doctrine in a particular situation. In 1994, the FTC codified the Unfairness Statement in a revision to section 5(n), which now states that:

> The Commission shall have no authority under this section or section 57a of this title to declare unlawful an act or practice on the grounds that such act or practice is unfair unless the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition. In determining whether an act or practice is unfair, the Commission may consider established public policies as evidence to be considered with all other evidence. Such public policy considerations may not serve as a primary basis for such determination.[28]

The FTC has since used the unfairness category as a basis for complaints against companies that have inadequate data security. For example, in a complaint against BJ's Wholesale Club, the FTC alleged that BJ's lack of security allowed for thousands of consumers' credit and debit card information to be taken.[29] Similarly, the FTC filed a complaint against Designer Shoe Warehouse (DSW), alleging improper information practices.[30] DSW collected consumer credit card information—including names, card numbers, and expiration dates.[31] The company then stored the information unencrypted, in multiple places, and failed to use readily available security measures.[32] In both cases, the FTC used the unfairness category to hold the

---

26. *See* Letter from the Fed. Trade Comm'n to Senators Wendell H. Ford & John C. Danforth (Dec. 17, 1980) [hereinafter Unfairness Statement], *reprinted in* Int'l Harvester Co., 104 F.T.C. 949, 1070–76 (1984).

27. *Id.*; S. REP. NO. 63-597, at 13 (1914) (concluding that a "general declaration condemning unfair practices" that would be interpreted by the commission was preferable to an "attempt to define" unfair practices); William E. Kovacic & Marc Winerman, *Competition Policy and the Application of Section 5 of the Federal Trade Commission Act*, 76 ANTITRUST L.J. 929, 931 (2010) (stating that one of the motivations behind the FTC Act was to "adjust the boundaries of acceptable business conduct in light of evolving business practices and developments in economic and legal understanding").

28. 15 U.S.C. § 45(n) (2006).

29. BJ's Wholesale Club, Inc., 140 F.T.C. 465, 467–69 (2005).

30. DSW Inc., 141 F.T.C. 117, 119–20 (2006).

31. *Id.* at 118–20.

32. *Id.* at 119.

companies accountable, not for posting a deceptive policy, but for lacking adequate security measures.[33] These cases demonstrate the broad applicability of the unfairness category of the FTC Act.

C. FTC Privacy Reports 2000 & 2010

The FTC launched the Advisory Committee on Online Access and Security in 1999 to investigate the security of consumers' personal information online.[34] The 2000 Privacy Report, submitted on May 15, 2000, demonstrated that online "security" is a fluid and evolving concept that must address the changing threat and particular circumstances unique to each website.[35] The 2000 Privacy Report called for an appropriateness standard which would require each website to have a security program to protect personal information to the extent that is "appropriate to the circumstances."[36] Specifically, the 2000 Privacy Report called for legislation and application of the Fair Information Practice Principles (FIPPs), and asked for authority to implement the FIPPs.[37]

The 2000 Privacy Report is not without its detractors. Some view it as abandoning self-regulation in favor of government regulation and argue that the legislation called for in the Report would be overly

---

33. Scott, *supra* note 7, at 145–49.

34. *See Advisory Committee on Online Access and Security*, FED. TRADE COMM'N, http://www.ftc.gov/acoas (last visited Apr. 24, 2013).

35. *See* ADVISORY COMM. ON ONLINE ACCESS & SEC., FED. TRADE COMM'N, FINAL REPORT OF THE FEDERAL TRADE COMMISSION ADVISORY COMMITTEE ON ONLINE ACCESS AND SECURITY 25 (2000) [hereinafter 2000 PRIVACY REPORT], *available at* http://www.ftc.gov/acoas/papers/acoasfinal1.pdf.

36. *Id.*

37. 2000 PRIVACY REPORT, *supra* note 35, at 26; *see also* Scott, *supra* note 7, at 141 n.94 (noting that "[w]hile the Report refers to the 'implementing authority' generally, it is clear from the context of the Report that the Commission considered itself to be the appropriate agency to implement the Fair Information Practice Principles"). The FIPPs originated from a U.S. Department of Health, Education, and Welfare (HEW) proposal for fair information principles. 2000 PRIVACY REPORT, *supra* note 35, at 3–4 & nn.24–25. The FIPPs as summarized in the 2000 Privacy Report include:

> (1) Notice—data collectors must disclose their information practices before collecting personal information from consumers;
> (2) Choice—consumers must be given options with respect to whether and how personal information collected from them may be used for purposes beyond those for which the information was provided;
> (3) Access—consumers should be able to view and contest the accuracy and completeness of data collected about them; and
> (4) Security—data collectors must take reasonable steps to assure that information collected from consumers is accurate and secure from unauthorized use.

Id.

broad.[38] The detractors assert that "extensive, yet vaguely phrased, privacy requirements" constitute a "blank check" to the FTC or any other agency.[39] Others have argued that the Report relies too heavily on FIPPs, which in turn relies heavily on reasonability.[40]

The FTC examined information privacy again through a series of roundtable discussions, culminating in a proposed framework.[41] The preliminary 2010 Privacy Report states that industry efforts to address privacy through self-regulation "have been too slow, and up to now have failed to provide adequate and meaningful protection."[42] As the 2010 Privacy Report highlights, FIPPs, and specifically the security principle, have formed the basis of the FTC's approach to self-regulation and online privacy policies.[43] The FIPPs have long been at the core of the FTC's approach to privacy and are used as a basis for the FTC's recommended best practices.[44] The FIPPs concept of "notice-and-choice" is a common foundation for the FTC's application of its authority under section 5 of the FTC Act for deceptive or unfair practices.[45] In addition to reaffirming the FIPPs, the FTC noted the shift from the use of the deceptive category to the unfairness category through the use of the "harm-based model."[46]

D. FTC Final Privacy Report 2012

In March 2012, the FTC issued a final report that incorporated public comments as well as commercial and technological advances.[47] The 2012 Privacy Report provides a guide to legislation and a set of

---

38. *See* FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE—A REPORT TO CONGRESS 1, 16–17 (2000) (dissenting statement of Commissioner Orson Swindle), *available at* http://www.ftc.gov/reports/privacy2000/privacy2000.pdf.

39. *Id.* at 27.

40. *See id.* at 1, 5–6 (statement of Commissioner Thomas B. Leary concurring in part and dissenting in part).

41. *See* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS—PRELIMINARY FTC STAFF REPORT 1–2 (2010) [hereinafter 2010 PRIVACY REPORT], *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf. The preliminary report proposed a framework and raised issues and questions for public comment. *Id.*

42. *Id.* at iii.

43. *Id.* at 7–9 & n.14.

44. *Id.*

45. *Id.* at 8–9.

46. *See id.* at 9 ("Rather than emphasizing potentially costly notice-and-choice requirements for all uses of information, the harm-based model targeted practices that caused or were likely to cause physical or economic harm, or unwarranted intrusions in [consumers'] daily lives." (alteration in original) (internal quotation marks omitted)).

47. FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS, at iii (2012) [hereinafter 2012 PRIVACY REPORT], *available at* http://ftc.gov/os/2012/03/120326privacyreport.pdf.

best practices to balance the privacy interests of consumers with innovation that relies on consumer information to develop beneficial new products and services.[48]

The 2012 Privacy Report again utilizes the FIPPs for its framework of best practices for protection of consumer privacy.[49] The Report embraces the concept of privacy by design, asking companies to incorporate "substantive privacy protections into their practices, such as data security, reasonable collection limits, sound retention and disposal practices, and data accuracy."[50] It urges Congress to enact data security and data broker legislation, and calls on industry to hasten self-regulation processes.[51] The Report also reaffirms the FTC's decision to enforce "reasonable security for consumer data" through section 5.[52]

The 2012 Privacy Report identifies five main "action items" in the realm of data security and privacy: (1) Do-Not-Track; (2) mobile security and privacy; (3) transparency in data brokerage; (4) security of "large platforms" such as ISPs, operating systems, browsers, and social media companies; and (5) further development of self-regulatory codes.[53]

The 2012 Privacy Report was not approved unanimously. Commissioner Rosch dissented from its issuance on several grounds, including what he views as conflicting with the FTC's statements to Congress indicating that it would base its enforcement in deception, rather than the unfairness category under the FTC Act.[54] Commissioner Rosch argued that "'[u]nfairness' is an elastic and elusive concept," the definition of which will vary according to a party's view of privacy and information gathering in general, and therefore is an inappropriate mechanism to govern information gathering and security practices.[55] Rosch asserted that by setting a high priority on privacy, the FTC has chosen to side with consumer

48. *Id.*
49. *Id.* at i.
50. *Id.* at 30.
51. *Id.* at viii.
52. *Id.* at 24 ("It is well settled that companies must provide reasonable security for consumer data. The Commission has a long history of enforcing data security obligations under Section 5 of the FTC Act . . . .").
53. *Id.* at 13–14.
54. *See id.* at C-3 to C-5 (dissenting statement of Commissioner J. Thomas Rosch) (noting that the 2012 Privacy Report defined "consumer harm" in a way that allowed the use of the unfairness category). Regarding the Google consent order, the 2012 Privacy Report states that "[a]lthough the complaint against Google alleged that the company used deceptive tactics and violated its own privacy promises when it launched Google Buzz, even in the absence of such misrepresentations, revealing previously-private consumer data could cause consumer harm." *Id.* at 8 n.37.
55. *Id.* at C-3 (dissenting statement of Commissioner J. Thomas Rosch).

organizations and large enterprises and placed a burden on smaller groups.[56]

Commissioner Rosch also worried about the future of the self-regulatory model, given that the 2012 Privacy Report's recommended best practices were nearly identical to the executive branch's Consumer Privacy Bill of Rights.[57] FTC enforcement of the "best practices" would effectively make the Consumer Privacy Bill of Rights compulsory, without adoption by Congress.[58] No statute or enforceable code of conduct would be needed if "firms fe[lt] obliged to comply with the 'best practices' or face the wrath of 'the Commission' or its staff."[59]

II. *FTC V. LABMD, INC.*

A. Background

After issuing a 2008 Resolution on procedures for investigating consumer privacy violations, in 2009 the FTC discovered that peer-to-peer (P2P) file sharing programs were disclosing private consumer data.[60] As a result, the FTC investigated whether companies had failed to use reasonable privacy protection measures or had violated any other applicable regulations.[61] To do so, the FTC issued Civil Investigative Demands (CIDs) to acquire digital copies of the private consumer information.[62] The FTC then received files containing private identifying information, such as names, dates of birth, and social security numbers of approximately 9000 LabMD customers.[63]

---

56. *See id.* at C-4 ("The 'final' Privacy Report . . . repeatedly sides with consumer organizations and large enterprises.").

57. *See id.* at C-8. The Obama Administration put forth a "Consumer Privacy Bill of Rights" and encouraged Congress to use it as a baseline for consumer privacy legislation. *See* EXEC. OFFICE OF THE PRESIDENT, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY, at ii, 45 (2012) [hereinafter CONSUMER PRIVACY BILL OF RIGHTS], *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

58. 2012 PRIVACY REPORT, *supra* note 47, at C-8 (dissenting statement of Commissioner J. Thomas Rosch).

59. *Id.*

60. FTC v. LabMD, Inc., No. 1:12-cv-3005, slip op. at 2 (N.D. Ga. Nov. 26, 2012). P2P is a method of sharing information directly between two or more computers on a network, such as LimeWire, KaZaa, or BitTorrent. *Peer-to-Peer File Sharing: A Guide for Business*, FED. TRADE COMM'N 1 (Jan. 2010), http://business.ftc.gov/sites/default/files/pdf/bus46-peer-peer-file-sharing-guide-business.pdf. The Bureau of Consumer Protection cautions about the security risks inherent in P2P systems because the systems allow other users to access entire drives on the sharing computer, not simply the files a person might have wished to share. *Id.* at 2.

61. *LabMD*, No. 1:12-cv-3005, slip op. at 2.

62. *Id.*

63. *Id.*

LabMD objected to the CIDs and filed an unsuccessful petition to limit or quash the CIDs.[64] After several months of LabMD's non-compliance, the FTC sought a court order to require LabMD to comply with the FTC's requests issued pursuant to its authority under 15 U.S.C. §§ 46, 57b-1 and the 2008 Resolution.[65] The FTC claimed that "[LabMD]'s failure to comply with the CIDs greatly impede[d] the Commission's ongoing investigation [into breaches of consumers' sensitive personal information], and prevent[ed] the Commission from completing its investigation in a timely manner."[66]

In September 2012, the court ordered LabMD to attend a hearing and file a pleading asserting its "legal and factual support for failing to comply with the FTC's CIDs" and explain why the court should refrain from ordering compliance with the CIDs.[67] Among other questions, the court asked how the FTC met the "within the authority of the agency" standard.[68]

One of the requirements for a governmental agency subpoena to be valid is a "plausible argument in support of its assertion of jurisdiction."[69] Thus, the district court has a somewhat limited role, and is constrained to analyzing the breadth of an agency's jurisdiction.[70] However, given the paucity of cases involving the FTC and consumer information security that are heard by the courts and the intense debate over the future of data security law, any judicial analysis is helpful. Thus, *LabMD* presented the court with an opportunity to provide some much needed judicial guidance.

B. FTC's Move Away from the Self-Regulation Model of Data Security

Until 2000, the model of FTC enforcement of consumer privacy and information security followed a standardized pattern.[71] Under the self-regulatory model, businesses could help develop standards by

---

64. *See* LabMD's Petition To Limit or Quash the Civil Investigative Demand, LabMD, Inc., FTC File No. 102-3099 (Jan. 10, 2012), *available at* http://www.ftc.gov/os/quash/120110labmdpetition.pdf.

65. *LabMD*, No. 1:12-cv-3005, slip op. at 4.

66. *Id.*

67. *Id.* at 4–5.

68. *Id.* at 5.

69. EEOC v. Kloster Cruise Ltd., 939 F.2d 920, 922 (11th Cir. 1991) (internal quotation marks omitted).

70. *See* Casey v. FTC, 578 F.2d 793, 799 (9th Cir. 1978) (stating that a "district court's role in a subpoena enforcement proceeding is strictly limited where the subpoena is attacked for lack of agency jurisdiction"); *see also* FTC v. Ken Roberts Co., 276 F.3d 583, 586 (D.C. Cir. 2001) (noting that "courts of appeals have consistently deferred to agency determinations of their own investigative authority").

71. *See* Scott, *supra* note 7, at 130 (observing that the "FTC initially sought to deal with online privacy issues by encouraging industry self-regulation").

holding themselves to heightened duties and obligations regarding consumer information.[72] This is most evident in the FTC's use of the deceptive practices category to enforce compliance with published privacy statements; companies that made promises to consumers about the safety or usage of personal information were punished when they did not live up to those promises.[73]

However, the FTC has become increasingly forceful in its use of section 5 to enforce information privacy and security.[74] The transition away from using the deceptive practices category to the unfair practices category occurred when the FTC filed complaints in instances where there had been no violation of stated privacy policies.[75]

C. LabMD Contests the FTC's Authority

As LabMD argued and as the district court generally agreed, the FTC's power under the unfairness category is "not unlimited."[76] Specifically, LabMD asserted that the 2008 Resolution is overly vague, and attacked the FTC's use of the unfairness category as improper because the FTC had not shown an injury to consumers.[77]

The court disagreed with LabMD on its two attacks against FTC jurisdiction. It found that the 2008 Resolution "sufficiently specifies the nature, scope, and subject matter upon which subpoenas and demands for information may be made."[78] The court was much more circumspect on LabMD's second argument, finding that one could persuasively argue that section 5 does not grant the FTC authority to investigate data security breaches.[79]

---

72. *Id.*

73. *See id.* ("The main element of self-regulation included FTC enforcement of those privacy policies that companies collecting personal information posted on their websites."); *see also supra* Part I.A (highlighting the use of the deceptive practices category of section 5 in information privacy cases).

74. *See Challenges Facing the Federal Trade Commission: Hearing Before the Subcomm. on Commerce, Trade, & Consumer Prot. of the H. Comm. on Energy and Commerce*, 107th Cong. 12, 16 (2001) (statement of Timothy J. Muris, Chairman, Fed. Trade Comm'n) (describing the FTC as "primarily a law enforcement agency").

75. *See supra* Part I.B (discussing the use of section 5's unfairness category against BJ's Wholesale Club and DSW).

76. *FTC v. LabMD, Inc.*, No. 1:12-cv-3005, slip op. at 10 (N.D. Ga. Nov. 26, 2012) ("Although it is given broad discretion to determine what constitutes an unfair practice, the FTC's authority to investigate unfair practices using its subpoena enforcement power is not unlimited.").

77. *Id.* at 11.

78. *Id.* at 11–12.

79. *Id.* at 14–15.

Conversely, to support its ruling, the court turned to prior FTC information security enforcement cases.[80] The court found that, "in light of the threat of substantial consumer harm that occurs when consumers are victims of identity theft," the FTC successfully argued that protecting the privacy of electronic consumer data falls within the scope of the Commission's investigatory authority.[81] The court also relied on the weight of precedent in making its decision, stating that "federal courts have recognized the FTC's authority under Section 5 to investigate and use its authority to address unfair practices regarding related data security and consumer privacy issues."[82]

However, although the cases cited by the district court represent holdings in favor of FTC jurisdiction over data security, they do not sweep as broadly as more recent FTC enforcements.[83] The cases cited by the court fall easily into section 5's prohibition of deceptive practices and involve some action taken by the defendant companies that impacted their customers' information security.[84] *LabMD*, however, addressed alleged omissions in a company's information security practices and procedures that allowed a third party to illegally obtain consumer information.[85]

Throwing most of its argument behind the weight of history and precedent, the district court only briefly addressed the broader scope of section 5 that the FTC argued against LabMD. The court asserted:

> [I]t is a plausible argument to assert that poor data security and consumer privacy practices facilitate and contribute to predictable and substantial harm to consumers in violation of Section 5

80. *Id.* at 13 (noting that the FTC has engaged in enforcement related to information security in "at least forty-four instances since 2000").

81. *Id.*

82. *Id.*

83. *Compare* FTC v. Pricewert LLC, No. C-09-2407, 2010 WL 329913, at *1 (N.D. Cal. Jan. 20, 2010) (using section 5 against a company that specifically "distribut[ed] illegal, malicious and harmful electronic content"), *with LabMD*, No. 1:12-cv-3005 (using section 5 against a company that allegedly failed to use adequate security methods to protect its customers' data). The FTC has also settled with Franklin's Budget Car Sales, Inc., and EPN, Inc., for generally failing to implement "reasonable and appropriate data security measures." *See* Press Release, Fed. Trade Comm'n, FTC Charges Businesses Exposed Sensitive Information on Peer-to-Peer File-Sharing Networks, Putting Thousands of Consumers at Risk (June 07, 2012), *available at* http://www.ftc.gov/opa/2012/06/epn-franklin.shtm.

84. *See* FTC v. Accusearch, Inc., No. 06-CV-105, 2007 WL 4356786, at *1, *7–8 (D. Wyo. Sept. 28, 2007) (addressing the unauthorized disclosure of confidential customer phone records), *aff'd*, 570 F.3d 1187 (10th Cir. 2009); FTC v. Seismic Entm't Prods., Inc., No. Civ. 04-377, 2004 WL 2403124, at *2–4 (D.N.H. Oct. 21, 2004) (addressing a company's use of methods that cause unauthorized changes to computers and that affect data security).

85. *LabMD*, No. 1:12-cv-3005, slip op. at 12–15.

> because it is disturbingly commonplace for people to wrongfully exploit poor data security and consumer privacy practices to wrongfully acquire and exploit personal consumer information.[86]

Thus, the court did not fully address the FTC's enforcement of data privacy because the FTC's investigatory authority needs only a "plausible argument" for jurisdiction.[87]

III. THE FUTURE OF THE FTC'S SELF-REGULATORY DATA SECURITY REGIME

In testimony before the Committee on Energy and Commerce, Chairman Leibowitz described "the three main principles" of the FTC's approach to information security and privacy.[88] According to Chairman Leibowitz, businesses should (1) customize and (2) simplify their electronic data privacy protections, as well as (3) provide increased transparency regarding such practices.[89] The Chairman also stated that "enforcement remains a top priority for the [FTC]"; indicating that the FTC will continue to make use of the "unfair" and "deceptive" language of the FTC Act to enforce FIPPs.[90]

Section 5, however, does not expressly include information security and privacy in the FTC's jurisdiction.[91] Rather, the FTC has authority to regulate unfair practices that "cause[] or [are] likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[92] This is a necessarily fluid jurisdiction, given the constant evolution of business practices and norms.[93]

---

86. *Id.* at 14–15.

87. *Id.* at 15 (finding that LabMD's argument against the FTC's jurisdiction "is not a sufficient reason to deny the FTC's request for enforcement").

88. *Balancing Privacy and Innovation: Does the President's Proposal Tip the Scale?: Hearing Before the Subcomm. on Commerce, Mfg. & Trade of the H. Comm. on Energy & Commerce*, 112th Cong. 4 (2012) (statement of Jon Leibowitz, Chairman, Fed. Trade Comm'n), *available at* http://energycommerce.house.gov/sites/republicans.energycommerce.house.gov/files/Hearings/CMT/20120329/HHRG-112-IF17-WState-JLeibowitz-20120329.pdf.

89. *Id.*

90. *Id.* at 15–18.

91. *See* 15 U.S.C. § 45(n) (2006).

92. *Id.* Administrative agencies like the FTC are also limited by the reasonableness test. *See* Genuine Parts Co. v. FTC, 445 F.2d 1382, 1391 (5th Cir. 1971) (explaining reasonableness requirements in investigations initiated by administrative agencies).

93. *See* FTC v. Sperry & Hutchinson Co., 405 U.S. 233, 239–44 (1972) (reasoning that Congress refused to provide a specific definition of "unfair methods of competition" because it would be impossible to include them all); *see also* Orkin Exterminating Co. v. FTC, 849 F.2d 1354, 1367–68 (11th Cir. 1988) (giving the FTC the authority to interpret section 5 in light of new business practices).

Unfairness, as the courts have interpreted it, does not only rely on "the machinations of those with ill intentions;" it relies on the foreseeable results of "ill intentioned schemes."[94] Additionally, the FTC itself has consistently been seen as having a role in interpreting section 5,[95] and has developed a history of enforcing the FTC Act in data security and privacy areas in over forty instances since 2000.[96] Precedent seems to be firmly on the side of the FTC and its role in enforcing information security and consumer privacy.[97] However, the FTC faces a different challenge to its use of the FTC Act's unfairness category in *FTC v. Wyndham Worldwide Corp.*[98] Both Wyndham and amicus parties argue that the FTC's authority to regulate unfair practices does not extend to data breaches caused by third parties.[99]

---

94. FTC v. Neovi, Inc., 604 F.3d 1150, 1156 (9th Cir. 2010); *see also* FTC v. R.F. Keppel & Bro., 291 U.S. 304, 314 (1934) (holding a retailer liable for unfair practices when the manufacturer was responsible for the unfairness); Regina Corp. v. FTC, 322 F.2d 765, 768 (3d Cir. 1963) ("One who places in the hands of another a means of consummating a fraud or competing unfairly in violation of the Federal Trade Commission Act is himself guilty of a violation of the Act." (quoting C. Howard Hunt Pen Co. v. FTC, 197 F.2d 273, 281 (3d Cir. 1952))).

95. *See* Am. Fin. Servs. Ass'n v. FTC, 767 F.2d 957, 967 (D.C. Cir. 1985) ("Congress has not at any time withdrawn the broad discretionary authority originally granted the Commission . . . ."); FTC v. Windward Mktg., Ltd., No. Civ. A. 1:96-CV-615F, 1997 WL 33642380, at *11 (N.D. Ga. Sept. 30, 1997) ("Congress has not enacted any more particularized definition of unfairness . . . .").

96. *See* Plaintiff's Response in Opposition to Wyndham Hotels and Resorts' Motion To Dismiss at 7, FTC v. Wyndham Worldwide Corp., No. 2:12-cv-01365 (D. Ariz. filed Oct. 1, 2012), ECF No. 45; *Legal Resources*, FTC BUREAU OF CONSUMER PROT., http://business.ftc.gov/legal-resources/29/35 (last visited Apr. 24, 2013) (listing forty-six cases).

97. *See* FTC v. Pricewert LLC, No. C-09-2407, 2010 WL 329913, at *2 (N.D. Cal. Jan. 20, 2010) (explaining an unsuccessful Fourth Amendment challenge to the FTC's seizure of electronic property and granting the FTC's request to prohibit Pricewert from "distributing or hosting" certain electronic programs harmful to consumers); FTC v. CyberSpy Software, LLC, No. 6:08-cv-1872-Orl-31GJK, 2009 WL 455417, at *1 (M.D. Fla. Feb. 23, 2009) (determining that Congress granted the FTC the authority to bring suits in district courts against anyone it suspects of violating any law within its jurisdiction); FTC v. Accusearch, Inc., No. 06-CV-105-D, 2007 WL 4356786, at *1, *7–10 (D. Wyo. Sept. 28, 2007) (finding that the FTC has jurisdiction over breaches of private data when it results in "substantial injury to consumers"), *aff'd* 570 F.3d 1187 (10th Cir. 2009); FTC v. Seismic Entm't Prods., Inc., No. Civ. 04-377, 2004 WL 2403124, at *2–4 (D.N.H. 2004) (describing that for an FTC claim against pop-up advertisements the court must give greater deference to public interests). *But see* FTC v. LabMD, Inc., No. 1:12-cv-3005, slip op. at 14 (N.D. Ga. Nov. 26, 2012) (finding "*significant merit* to Respondents' argument that Section 5 does not justify an investigation into data security practices and consumer privacy issues" but holding that "it is a plausible argument to assert that poor data security and consumer privacy practices" violate section 5 since "it is disturbingly commonplace for people to wrongfully exploit poor data security" (emphasis added)).

98. Motion to Dismiss by Defendants Wyndham, Worldwide Corp., Wyndham Hotel Group, LLC, & Wyndham Hotel Management, Inc., FTC v. Wyndham Worldwide Corp., No. CV 12-1365 (D. Ariz. filed Aug. 27, 2012), *transferred to* No. 2:13-CV-01887 (D.N.J. docketed Mar. 26, 2013), 2012 WL 3916987.

99. *See id.* at 1 (claiming that the FTC brought a claim against one corporation for the actions of another); *see also* Brief of Amici Curiae Chamber of Commerce of

This challenge to the FTC's authority will shape the Commission's role in the data security realm in the future.[100]

CONCLUSION

Through its use of section 5, the FTC fills a void in information security law and provides necessary protections for consumers. The FTC itself, however, recognizes the incompleteness of its jurisdiction when it comes to consumer privacy and data security, and has repeatedly called on Congress to pass legislation to delineate a framework.

Information security is complicated by the fact that companies that collect consumer information often become targets of increasingly sophisticated attacks. These attacks pull data breaches away from the standard types of cases pursued through the FTC Act's unfairness category.

In the absence of legislation or executive action, it is left to the FTC's discretion, ultimately reviewed by the courts, to determine what failures fall into its purview. *FTC v. LabMD*, however, breaks the norm and challenges the FTC's self-regulatory model. Although future court decisions may decide that the FTC can use the unfairness category of section 5 to investigate companies and protect consumer privacy, they may also stop short of allowing the FTC to create its own authority through resolutions that have no legislative or executive backing.

---

the United States of America et al. at 2–3, *Wyndham Worldwide Corp.*, No. CV 12-1365, 2012 WL 4766977 (arguing that giving the FTC enforcement authority would go against congressional intent by allowing government action whenever a private business suffers a third-party data privacy violation).

100. *See* Corey Dennis, *FTC's Authority to Regulate Data Security*—FTC v. Wyndham, GOVERNO L. FIRM LLC (Nov. 29, 2012), http://www.governo.com/TheFirm/News.asp?NewsID=665 (asserting that the *Wyndham* case could "severely limit" the FTC's power to regulate data privacy in the future).