Boston College Law Review

Volume 60
Issue 9 *Electronic Supplement*

Article 12

3-21-2019

Policing Cyberspace: The Uncertain Future of Data Privacy and Security Enforcement in the Wake of *LabMD*

Julia Whall
Boston College Law School, julia.whall@bc.edu

POLICING CYBERSPACE: THE UNCERTAIN FUTURE OF DATA PRIVACY AND SECURITY ENFORCEMENT IN THE WAKE OF *LABMD*

Abstract: On June 6, 2018, in *LabMD, Inc. v. Federal Trade Commission* (*LabMD III*), the U.S. Court of Appeals for the Eleventh Circuit vacated a Federal Trade Commission order that required a small medical laboratory to maintain a reasonable data security program following a data breach. The case presented the Eleventh Circuit with the opportunity to clarify the FTC's data privacy and security enforcement powers under Section 5 of the FTC Act. The court, however, only addressed this issue briefly in dicta, and instead held that the order was unenforceable because it was overly-broad. This Comment argues that Eleventh Circuit's decision introduces further confusion about the scope of the FTC's enforcement authority and meaningfully constrains the FTC's approach to data privacy and security remediation.

INTRODUCTION

In recent years, reports concerning large-scale data breaches have grabbed headlines.[1] Not all data breaches, however, make front-page news.[2] In 2017, the majority of reported data breaches affected small businesses, as opposed to nationally known companies.[3] Compared to the losses data breaches cause larger enterprises, the damages faced by smaller companies are minimal.[4] Neverthe-

[1] *See, e.g.*, Vindu Goel & Rachel Abrams, *Hackers Stole Data from Millions of Cards at Saks*, N.Y. TIMES, Apr. 2, 2018, at B2 (detailing a data breach that resulted in the theft of five million credit and debit card numbers from affiliated retail chains); Mike Isaac et al., *Uber Breach, Kept Secret for a Year, Hit 57 Million Accounts*, N.Y. TIMES, Nov. 22, 2017, at B1 (reporting on Uber's response to a 2016 data breach); Nicole Perlroth, *Yahoo Breach in 2013 Affected All 3 Billion Accounts, Not Just One-Third*, N.Y. TIMES, Oct. 4, 2017, at B2 (commenting on the scope of cyberattacks on Yahoo's internal network).

[2] Matthew Goldstein, *Hackers Go After Little Fish, Too, While Trawling for Credit Cards*, N.Y. TIMES, June 11, 2015, at B2 (noting that data breaches affecting small businesses are often unreported because these businesses are not subject to the same public disclosure requirements as publicly-traded companies).

[3] VERIZON, 2018 DATA BREACH INVESTIGATIONS REPORT 5 (11th ed. 2018), https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf [https://perma.cc/4QNJ-Q6JE] (finding that 58% of data breach victims qualify as small businesses). Hackers commonly target small businesses because they store highly-sensitive consumer data, such as credit cards numbers and health information, but lack the resources needed to develop robust cybersecurity programs. Loren F. Selznick & Carolyn LaMacchia, *Cybersecurity Liability: How Technically Savvy Can We Expect Small Business Owners to Be?*, 13 J. BUS. & TECH. L. 217, 221, 225 (2018).

[4] *Compare* Vindu Goel, *Verizon's Cost to Buy Yahoo Is Reduced by $350 Million*, N.Y. TIMES, Feb. 22, 2017, at B3 (reporting that two highly-publicized data breaches devalued Yahoo's worth by $350 million), *with* AO KASPERSKY LAB, IT SECURITY: COST CENTER OR STRATEGIC INVESTMENT?

less, the potentially high costs associated with data breaches can silently kill small enterprises that normally operate under narrow profit margins.[5]

LabMD, Inc. ("LabMD") was a small business that sought to make a large impact in the wake of a data breach.[6] In 2009, the Federal Trade Commission ("FTC") investigated LabMD after a data breach exposed its patients' personal information.[7] After the FTC filed a complaint against the company, LabMD made the unusual decision to defend itself in court.[8] Hundreds of thousands of dollars in legal fees followed, ultimately causing LabMD to shutter its doors.[9]

Although the FTC's enforcement action eventually forced LabMD out of business, LabMD's choice to contest the complaint may have a significantly lasting impact on the FTC.[10] The U.S. Court of Appeals for the Eleventh Circuit's

---

4 (2017), https://go.kaspersky.com/rs/802-IJN-240/images/IT%20Security%20Econmics%20Report%209.18.17.pdf?aliId=488652022 [https://perma.cc/L3AL-QR4V] (finding that data breaches cost small- and medium-sized businesses with 50 to 999 employees an average of $117,000).

[5] *See Protecting Small Businesses from Cyber Attacks: The Cybersecurity Insurance Option*, *Testimony Before the H. Comm. on Small Bus.*, 115th Cong. 29 (2017) (statement of Robert Luft, President, SureFire Innovations, on behalf of the National Small Business Association, stating that cyberattacks on bank accounts cost small businesses an average of $32,021, which can destroy smaller companies that lack excess funds); COUNCIL OF BETTER BUS. BUREAUS, 2017 STATE OF CYBERSECURITY AMONG SMALL BUSINESSES IN NORTH AMERICA 14 (2017), https://www.bbb.org/globalassets/shared/media/state-of-cybersecurity/updates/cybersecurity_final-lowres.pdf [https://perma.cc/H2W3-PPS6] (finding that over 50% of small businesses would become unprofitable within a month if they "permanently lost access to essential data"). A data breach might generate costs related to consumer notification, public relations, legal fees, cybersecurity system improvements, insurance premiums increases, lost customer relationships, business devaluation, and more. DELOITTE, BENEATH THE SURFACE OF A CYBERATTACK: A DEEPER LOOK AT BUSINESS IMPACTS 3 (2016), https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-risk-beneath-the-surface-of-a-cyber-attack.pdf [https://perma.cc/W5UG-MNFW] (assessing the financial and reputational impact of a data breach).

[6] *See* Aaron Boyd, *Should FTC Regulate Commercial Cybersecurity?*, FED. TIMES (Aug. 25, 2015), https://www.federaltimes.com/2015/08/25/should-ftc-regulate-commercial-cybersecurity/ [https://perma.cc/K8YM-6KSN] (reporting that LabMD's CEO aims to change the data security enforcement landscape by litigating his company's case). LabMD provided cancer testing services to patients before going out of business. LabMD, Inc. v. Fed. Trade Comm'n (*LabMD III*), 894 F.3d 1221, 1224 (11th Cir. 2018) (vacating an FTC order on the grounds of unenforceability).

[7] *LabMD III*, 894 F.3d at 1225.

[8] *See* Dune Lawrence, *A Leak Wounded This Company. Fighting the Feds Finished It Off*, BLOOMBERG (Apr. 25, 2016), https://www.bloomberg.com/features/2016-labmd-ftc-tiversa/ (specifying that LabMD was the first company to litigate, rather than settle, an FTC data security complaint). Most companies faced with FTC enforcement actions chose to settle because the possible litigation costs often exceed the potential penalties. Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 611–13 (2014) (arguing that the FTC has developed a body of data privacy and security law through a common law-like approach). Moreover, companies that settle with the FTC can do so without admitting liability. *Id.* at 613.

[9] Lawrence, *supra* note 8. By 2013, LabMD amassed over a half-million dollars in legal fees. *Id.* Within a year of the FTC's initial complaint, the company's annual revenue was cut in half. *Id.* LabMD was also unable to secure insurance. *Id.*

[10] *See* Rafael Reyneri, *Eleventh Circuit* LabMD *Decision Potentially Limits FTC's Remedial Powers*, COVINGTON: GLOBAL POLICY WATCH (June 11, 2018), https://www.globalpolicywatch.com/2018/06/eleventh-circuit-labmd-decision-potentially-limits-ftcs-remedial-powers/ [https://perma.cc/

2018 decision in *LabMD, Inc. v. Federal Trade Commission* (*LabMD III*) arguably calls into question the scope of the FTC's enforcement authority and remedial powers in the data privacy and security space.[11]

Part I of this Comment gives an overview of the factual background, legal framework, and procedural history of *LabMD III*.[12] Part II of this Comment examines and discusses the Eleventh Circuit's central holding.[13] Finally, Part III of this Comment argues that *LabMD III* perpetuates confusion about the scope of the FTC's authority and unduly constrains the FTC's remedial powers.[14]

I. THE CONTEXT AND HISTORY OF *LABMD*

Section of A of this Part details the facts underlying *LabMD III*.[15] Section B of this Part provides an overview of the FTC's regulation of data privacy and security in the United States.[16] Section C of this Part outlines the procedural history of *LabMD III*.[17]

A. Factual Background

LabMD was founded in Atlanta and, for several years, operated as a medical laboratory that tested patient samples for urologists.[18] In 2005, a LabMD billing manager installed LimeWire, an application that allowed users to share files between computers, on a work computer in violation of company policy.[19] Following LimeWire's installation, the billing manager unknowingly shared her "My Documents" folder to a peer-to-peer network that was accessible by mil-

---

6Z7W-6SDQ] (commenting on how *LabMD III* potentially curtailed the FTC's authority to enforce broad consent orders).

[11] *See LabMD III*, 894 F.3d at 1231, 1236 (addressing the question of the FTC's enforcement authority in dicta and holding that the FTC needs to employ greater specificity in its consent orders); Alison Frankel, *There's a Big Problem for the FTC Lurking in the 11th Circuit's* LabMD *Data-Security Ruling*, REUTERS (June 15, 2018), https://www.reuters.com/article/us-otc-labmd/theres-a-big-problem-for-the-ftc-lurking-in-11th-circuits-labmd-data-security-ruling-idUSKCN1J32S2 [https://perma.cc/JBJ6-E2Z2] (arguing that *LabMD III* potentially affects how the FTC will draft future consent orders and ground forthcoming complaints).

[12] *See infra* notes 15–51 and accompanying text.

[13] *See infra* notes 52–69 and accompanying text.

[14] *See infra* notes 70–108 and accompanying text.

[15] *See infra* notes 18–26 and accompanying text.

[16] *See infra* notes 27–42 and accompanying text.

[17] *See infra* notes 43–51 and accompanying text.

[18] Lawrence, *supra* note 8. LabMD no longer provides services to consumers, but the company still exists and continues to retain electronic consumer records. *LabMD III*, 894 F.3d at 1224 n.3.

[19] *LabMD III*, 894 F.3d at 1224. During the period relevant to *LabMD III*, LimeWire was popularly used for sharing music and video files. *Id.* In 2010, a court-ordered injunction mandated that LimeWire disable the functionality of its software after the company was found liable for inducement of copyright infringement, common law copyright infringement, and unfair competition. Arista Records LLC v. Lime Wire LLC, 2010 U.S. Dist. LEXIS 115675, at *6, *21–23 (S.D.N.Y. Oct. 27, 2010).

lions of LimeWire users.[20] Between July 2007 and May 2008, the shared folder included a 1,718-page spreadsheet containing the personal information of roughly 9,300 LabMD patients (the "Insurance File").[21] In May 2008, a third party discovered the Insurance File and reported it to the FTC, leading to an investigation of LabMD's data privacy and security practices.[22]

The FTC subsequently received news of a separate potential security breach involving LabMD patients.[23] In October 2012, local police in Sacramento, California raided the home of suspected identity thieves and discovered records containing the personal information of an additional 600 LabMD patients (the "Sacramento Documents").[24]

After assessing these two security breaches, the FTC filed an administrative complaint against LabMD in August 2013.[25] The complaint alleged that the laboratory engaged in unfair practices by failing to implement "reasonable and appropriate" data security measures.[26]

---

[20] *LabMD III*, 894 F.3d at 1224. Peer-to-peer networks allow users to exchanges files and information between computers over the Internet without connection to a centralized server computer. JAY DRATLER, JR., CYBERLAW: INTELLECTUAL PROPERTY IN THE DIGITAL MILLENNIUM § 6.03 (2018).

[21] *LabMD III*, 894 F.3d at 1224. The Insurance File included patient names, social security numbers, dates of birth, medical test codes and health insurance information. *Id.*

[22] *Id.* at 1224–25. Triversa, a cybersecurity consulting firm concentrating in peer-to-peer monitoring services, uncovered the Insurance File. *Id.* Triversa downloaded the Insurance File and later attempted to use the document to market its cybersecurity remediation services to LabMD. *Id.* LabMD, however, removed LimeWire from its computer systems and declined Triversa's services. *Id.* As a result, Triversa reported the incident to the FTC. *Id.*

[23] *In re* LabMD, Inc. (*LabMD I*), No. 9357, 2015 WL 7575033, at *30 (F.T.C. Nov. 13, 2015), *vacated*, *In re* LabMD, Inc. *(LabMD II)*, No. 9357, 2016 WL 4128215 (F.T.C. July 28, 2016), *vacated*, *LabMD III*, 894 F.3d 1221.

[24] *Id.* at *28. The Sacramento Documents included copies of billing documents, checks, patient names, and social security numbers. *Id.* LabMD's digital billing system likely created the billing documents found, but LabMD did not store these records electronically. *Id.* at *29. It is unclear how paper copies of LabMD billing documents made their way to California and how this security incident might have related to the LimeWire breach. *See id.* at *29–30 (summarizing the history of the Sacramento Documents without explaining how the alleged identity thieves procured them). The FTC alleged that some social security numbers found in the Sacramento Documents were used under different names, thereby signaling identity theft. Complaint at 5, *LabMD I*, 2015 WL 7575033 (2015) (No. 9357), 2013 WL 5232775, at *5 (F.T.C. Aug. 29, 2013).

[25] Complaint, *supra* note 24, at 1. The FTC commences enforcement actions by investigating entities that it reasonably believes have violated statutory law or engaged in deceptive or unfair practices. Solove & Hartzog, *supra* note 8, at 609. When investigators conclude that an entity engaged in illegal activity, the FTC issues a complaint detailing the alleged violations and proposed remedies. *Id.* If an entity chooses to dispute an FTC complaint, it may respond before an administrative or federal district judge. *Id.*

[26] Complaint, *supra* note 24, at 5. For example, the complaint contended that LabMD failed to sufficiently train its employees to protect personal information. *Id.* at 3. The FTC also alleged that LabMD did not implement commonly available measures to detect system vulnerabilities or detect unlawful access to the personal information. *Id.* at 3.

B. Legal Framework

In the absence of robust federal data privacy and security laws, the FTC has emerged as the nation's primary privacy and data security enforcer.[27] The Federal Trade Commission Act ("FTC Act"), which establishes the FTC's role, does not expressly empower the FTC to police data privacy and security.[28] Nonetheless, as of December 2017, the FTC has brought over 500 enforcement actions related to consumer privacy protection and over 60 cases regarding data security.[29] The FTC derives its authority to enforce data privacy and security actions in part through powers conferred by sector-specific statutes.[30] Where such statutes

---

[27] Anne E. Kane, *Regulation Under Section 5: Data Security and the FTC:* FTC v. Wyndham Worldwide Corp., IN-HOUSE DEF. Q., Summer 2015, at 41. Several federal statutes target cybersecurity concerns within specific sectors, but there is no federal data privacy or security law that blankets all online activity. *Id.* Instead, states have enacted separate data privacy and security laws that vary significantly in scope, as demonstrated by differing definitions of "personal information" in data breach notification statutes. *Compare, e.g.*, CONN. GEN. STAT. § 36a-701b (2018) (defining "personal information" as a consumer's name used in combination with a social security number, state identification number, or financial account number), *with* MO. REV. STAT. § 407.1500 (2018) (defining "personal information" as an individual's name used in combination with a social security number, government identification number, financial account number or identifier, medical information, or health insurance information). In 2018, California enacted a new law that provides broad privacy protections to consumers. *See* California Consumer Privacy Act of 2018, 2018 Cal. Stat. ch. 55 (granting consumers the right to request deletion of their personal information, opt-out of the sale of their personal information, and receive information about businesses' data collection practices). Effective in 2020, this law may pave the way for more comprehensive privacy legislation at the state and federal levels. Lother Determann, *Broad Data and Business Regulation, Applicable Worldwide*, INT'L ASS'N OF PRIVACY PROFS. (July 2, 2018), https://iapp.org/news/a/analysis-the-california-consumer-privacy-act-of-2018/ [https://perma.cc/UZK5-DGZ7].

[28] *See* Gerard M. Stegmaier & Wendell Bartnick, *Psychics, Russian Roulette, and Data Security: The FTC's Hidden Data-Security Requirements*, 20 GEO. MASON L. REV. 673, 707 (2013) (discussing how the Federal Trade Commission Act ("FTC Act") fails to reference data security). *See generally* FTC Act, 15 U.S.C. §§ 41–58 (2012) (lacking mention of the FTC's authority to regulate data privacy and security matters). Although the FTC Act grants the Commission broad rulemaking authority, the FTC has resisted exercising this authority in the cybersecurity context because the process is slow and inefficient. Stegmaier & Bartnick, *supra*, at 598–99.

[29] FED. TRADE COMM'N, DATA PRIVACY & SECURITY UPDATE: 2017, at 2, 4 (2018), https://www.ftc.gov/reports/privacy-data-security-update-2017-overview-commissions-enforcement-policy-initiatives [https://perma.cc/UWE5-KF93]. The upswing in FTC enforcement actions has increasingly inspired companies to incorporate Chief Privacy Officers into corporate governance structures. Victoria L. Schwartz, *Corporate Privacy Failures Start at the Top*, 57 B.C. L. REV. 1693, 1741 (2016) (theorizing explanations for failures in corporate privacy).

[30] Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. 2230, 2251–52 (2015) (examining federal data privacy and security laws that expressly grant the FTC enforcement authority). For example, the Children's Online Privacy Protection Act of 1998 requires the FTC to regulate websites targeted to children thirteen and under and bring related enforcement actions. 15 U.S.C. §§ 6502(b), 6505. The Gramm-Leach-Bliley Act authorizes the FTC to issue and enforce data privacy and security regulations against financial institutions. *Id.* §§ 6804(a)(1)(C), 6805(a).

are inapplicable, Section 5 of the FTC Act ("Section 5") empowers the FTC with broad authority to regulate deceptive or unfair commercial practices.[31]

Early data privacy and security actions brought under Section 5 typically invoked its deception prong.[32] In those cases, the FTC argued that businesses deceived consumers by misrepresenting the nature of their data privacy or security controls in company policies.[33] In recent years, however, the FTC has increasingly regulated data privacy and security under Section 5's unfairness prong.[34] A business practice is unfair when it leads to a substantial consumer injury that consumers cannot prevent and is not counterbalanced by a benefit conferred to consumers or other businesses.[35]

The FTC's broad exercise of authority under the unfairness prong has proved controversial among scholars.[36] Yet because the vast majority of such FTC complaints are settled through consent order procedures, the FTC's authority has rarely been litigated in court.[37]

---

[31] FTC Act § 5(a)(2) (empowering the FTC to regulate "unfair or deceptive acts or practices in or affecting commerce"); *see* Hartzog & Solove, *supra* note 30, at 2253 (stating that Section 5 of the FTC Act ("Section 5") grants FTC jurisdiction over all industries except those expressly excluded). For example, in 2017, the FTC filed a complaint against VIZIO, Inc. alleging that the company engaged in unfair and deceptive acts by installing software on internet-connected televisions that tracked consumers' viewing data without consent. Fed. Trade Comm'n v. VIZIO, Inc., No. 2:17-cv-00758, 2017 U.S. Dist. LEXIS 219381, at *1 (D.N.J. Feb. 13, 2017).

[32] Hartzog & Solove, *supra* note 30, at 2235. The FTC finds an omission, practice, or representation to be deceptive when it misleads a reasonable consumer to their detriment. Letter from James C. Miller III, Chairman, Fed. Trade Comm'n, to Hon. John D. Dingell, Chairman, Comm. on Energy & Commerce (Oct. 14, 1983).

[33] Hartzog & Solove, *supra* note 30, at 2235.

[34] Alexander E. Reicher & Yan Fang, *FTC Privacy and Data Security Enforcement and Guidance Under Section 5*, 25 J. ANTITRUST, UCL & PRIVACY SEC. ST. BOARD CAL. 89, 90 (2016). Certain FTC data privacy enforcement actions have involved allegations of both deceptive and unfair practices. *See, e.g.*, *In re* Gateway Learning Corp., 138 F.T.C. 443, 449–50 (2004) (alleging that an educational company engaged in deceptive and unfair practices by providing third parties with children's personal data without properly revising its privacy policy).

[35] FTC Act § 5(n).

[36] *See, e.g.*, Stegmaier & Bartnick, *supra* note 28, at 710–11 (contending that the FTC's complaints and consent orders are overly vague and do not provide businesses with fair notice of the cybersecurity practices that violate Section 5). The FTC's broad exercise of unfairness authority in the cybersecurity space also has its supporters. *See, e.g.*, Dennis D. Hirsch, *That's Unfair! Or Is It? Big Data, Discrimination and the FTC's Unfairness Authority*, 103 KY. L.J. 345, 361 (2015) (arguing that the FTC Act can provide a useful framework for policing "big data").

[37] Solove & Hartzog, *supra* note 8, at 610–11. To settle an FTC enforcement action, either the FTC or the respondent may propose the terms of a consent agreement that waives the parties' rights to judicial review. *Id.* at 610. Once the FTC approves the consent agreement, it makes the terms available for public comment for a specified period of time before finalizing the order. *Id.* Businesses tend to settle with the FTC in cybersecurity actions because the cost of litigation is significant, the likelihood of victory is small, and companies are not required to admit wrongdoing. *Id.* at 611–13.

Prior to the *LabMD* decision, the most significant challenge to the FTC's data privacy and security enforcement authority concluded in the FTC's favor.[38] In 2015, the U.S. Court of Appeals for the Third Circuit in *Federal Trade Commission v. Wyndham Worldwide Corp.* affirmed the FTC's authority to enforce data privacy and security under Section 5's unfairness prong.[39] The court further stated that the FTC provided the defendant with fair notice that its data privacy and security controls failed to meet the FTC's standards of fairness.[40] Because the defendant in *Wyndham* declined to appeal the Third Circuit's decision, open questions remained regarding the nature and scope of the FTC's authority.[41] Scholars anticipated that *LabMD III* might provide necessary clarifications.[42]

C. Procedural History

LabMD's decision to challenge the FTC's initial administrative complaint led to prolonged and publicly contentious litigation.[43] LabMD secured a relatively early victory when an administrative law judge ("ALJ") dismissed the case based on the FTC's reliance on evidence that lacked credibility.[44] The ALJ con-

---

[38] *See* Fed. Trade Comm'n v. Wyndham Worldwide Corp., 799 F.3d 236, 247 (3d Cir. 2015) (holding that the FTC may bring data security enforcement actions under Section 5's unfairness prong); Crystal N. Skelton, *FTC Data Security Enforcement: Analyzing the Past, Present, and Future*, 25 J. ANTITRUST, UCL & PRIVACY SEC. ST. BOARD CAL. 305, 309–10 (2016) (noting that *Wyndham* was the first federal case to challenge the FTC's data security enforcement authority).

[39] *See Wyndham*, 799 F.3d at 247–49 (concluding that deficient data security systems could be seen as unfair and the existence of sector-specific federal data security statutes does not preclude FTC enforcement of data security). The defendant in *Wyndham* was a hospitality chain that experienced three separate cyber-attacks between 2008 and 2009. *Id.* at 240. In total, hackers stole the personal information of approximately 619,000 consumers, leading to at least $10.6 million in consumer loss. *Id.* at 242. The defendant contested the complaint issued by the FTC in the aftermath of the attacks, arguing, in part, that the FTC did not have the authority to bring action on grounds of unfairness under Section 5. *Id.* at 244–47.

[40] *Id.* at 259. The defendant argued that, absent an official decree or regulation from the FTC, it lacked constitutionally fair notice of what the FTC considered a fair data security system under Section 5. *Id.* at 253–54. The court rejected this argument because the FTC had developed a significant volume of guidelines, complaints, and consent decrees outlining the FTC's position on cybersecurity matters. *Id.* at 256–57.

[41] *See* Stipulated Order for Injunction at 6, Fed. Trade Comm'n v. Wyndham Worldwide Corp., Civ. No. 2:13-CV-01887-ES-JAD (D.N.J. Dec. 11, 2015) (setting forth a settlement agreement between the parties).

[42] *See, e.g.*, Stuart L. Pardau & Blake Edwards, *The FTC, the Unfairness Doctrine, and Privacy by Design: New Legal Frontiers in Cybersecurity*, 12 J. BUS. & TECH. L. 227, 230 (2017) (speculating that the Eleventh Circuit's review of *LabMD III* could provide "fertile ground" for understanding the FTC's role in regulating cybersecurity).

[43] *See* Gabe Maldoff, LabMD *and the New Definition of Privacy Harm*, INT'L ASS'N OF PRIVACY PROFS. (Aug. 22, 2016), https://iapp.org/news/a/labmd-and-the-new-definition-of-privacy-harm/ [https://perma.cc/47Q3-NJYG] (noting that LabMD's CEO published a book, entitled *The Devil Inside the Beltway*, that criticized the FTC's perceived overextension of power in the data privacy and security enforcement context).

[44] *See LabMD I*, 2015 WL 7575033, at *65 (F.T.C. Nov. 13, 2015) (dismissing the FTC's complaint). The FTC's complaint argued that LabMD's two known security breaches caused, or were

cluded that LabMD's data security practices were unlikely to cause substantial injury to consumers, and thus, the FTC failed to support an essential element of its Section 5 unfairness claim.[45]

The FTC appealed the dismissal to the FTC's commissioners.[46] In 2016, the FTC commissioners reversed the ALJ's decision, finding that the FTC sufficiently demonstrated that the Insurance File's exposure caused substantial injury to consumers under Section 5's unfairness prong.[47] Contemporaneously with its reversal, the FTC issued a cease and desist order requiring LabMD to take certain corrective actions to establish a more reasonable data security system (the "Order").[48] LabMD appealed the Order to the Eleventh Circuit, arguing that the FTC lacked the authority to issue the Order and that the standard of reasonableness described in the Order was exceedingly vague.[49] In June 2018, the Eleventh Circuit vacated the Order on the grounds that it was not sufficiently specific.[50] The court declined to rule on the scope of the FTC's Section 5 enforcement authority.[51]

II. Discussing the Eleventh Circuit's Analysis in *LabMD III*

Section A of this Part discusses the Eleventh Circuit Court of Appeals' decision to bypass questions concerning the FTC's authority to bring data privacy

---

likely to cause, substantial injury to consumers. *Id.* at *2. The FTC's claim relied on evidence that Triversa found information contained in the Insurance File at numerous IP addresses, at least one of which belonged to a possible identity thief. *Id.* at *47. The administrative law judge ("ALJ") regarded this evidence as unreliable, concluding that there was no clear indication that the exposure of the Insurance File through LimeWire caused, or was likely to cause, identity theft harm. *Id.* The court further noted that the exposure of the Insurance File was unlikely to cause medical identity theft, reputational, or other harms. *Id.* at *50–53.

[45] *See supra* note 44 and accompanying text.

[46] *LabMD II*, 2016 WL 4128215, at *7. Any party may appeal an ALJ decision by filing notice with the Secretary of the FTC and submitting an appellate brief. 16 C.F.R. § 3.52(b) (2015). Once the parties have had the opportunity to file reply briefs, the FTC will either schedule an oral argument or issue its final decision in the matter. *Id.* In this case, the FTC reviewed the factual findings and legal conclusions of the case *de novo*, applying new logical inferences, as needed. *LabMD II*, 2016 WL 4128215, at *7.

[47] *LabMD II*, 2016 WL 412821, at *21. The FTC reasoned that the unauthorized disclosure of personal information caused an intangible privacy harm and could likely result in substantial injury. *Id.* The FTC, however, held that the FTC did not sufficiently support the allegation that the exposure of the Sacramento Documents stemmed from failures in LabMD's computer security program. *Id.*

[48] *LabMD III*, 894 F.3d at 1227. By its terms, the cease-and-desist order the FTC issued (the "Order") was scheduled to terminate on the later of July 18, 2036, or twenty years from the last date that the FTC alleged violation of the Order. *Id.*

[49] *Id.* at 1230–31. LabMD also moved to stay enforcement of the Order, which the Eleventh Circuit granted. LabMD v. Fed. Trade Comm'n (*LabMD III Motion for Stay*), 678 F. App'x 816, 822 (11th Cir. 2016).

[50] *LabMD III*, 894 F.3d at 1224. The Eleventh Circuit reviewed the FTC's legal conclusions *de novo*, giving a degree of deference to the FTC's interpretation of unfairness. *Id.* at 1227.

[51] *Id.* at 1231.

and security actions under Section 5.[52] Section B of this Part examines the court's conclusion that the Order was unenforceable.[53]

A. The FTC's Authority to Enforce Data Privacy and Security

One of the questions presented on appeal was whether the FTC had authority to enforce data privacy and security matters under Section 5.[54] If the Eleventh Circuit accepted LabMD's argument that it did not, and accordingly held that the FTC overreached its powers, it would have split from the Third Circuit Court of Appeals, which previously upheld the FTC's enforcement authority.[55] A circuit split of this magnitude would have increased the likelihood that the Supreme Court would take the matter under review.[56]

The Eleventh Circuit avoided this potential split entirely by accepting, for the sake of argument, that LabMD's failure to implement a reasonable data security system qualified as an unfair act or practice under Section 5.[57] The FTC argued that LabMD's data security program was unfair because it caused substantial, unpreventable injury to consumers by invading their right to privacy and such injury was not counterbalanced by public policy considerations.[58] Accepting this *arguendo*, the court noted that an unfair act or practice must not only cause substantial injury, but also be rooted in the Constitution, statute, or com-

---

[52] *See infra* notes 54–61 and accompanying text.

[53] *See infra* notes 62–69 and accompanying text.

[54] LabMD, Inc. v. Fed. Trade Comm'n (*LabMD III*), 894 F.3d 1221, 1230 (11th Cir. 2018). Critics of the Eleventh Circuit Court of Appeals' opinion in 2018, in *LabMD, Inc. v. Federal Trade Commission,* believed this was a missed opportunity to clarify ambiguities in the cybersecurity enforcement space. *See, e.g.*, Jennifer M. Thomas, *11th Circuit Avoids Opining on FTC's Authority to Police Negligent Data Security Practices in Healthcare*, HYMAN, PHELPS & MCNAMARA (June 14, 2018), http://www.fdalawblog.net/2018/06/the-eleventh-circuit-avoids-opining-on-the-ftcs-authority-to-police-negligent-data-security-practices-in-healthcare/ [https://perma.cc/35VK-4HSP] (stating that many observers were disappointed by the court's failure to rule on the scope of the FTC's Section 5 authority).

[55] *See LabMD III*, 894 F.3d at 1231 (assuming *arguendo* that the FTC Act empowered the FTC to bring suit); Fed. Trade Comm'n v. Wyndham Worldwide Corp., 799 F.3d 236, 247–49 (3d Cir. 2015) (holding that the FTC could bring cybersecurity claims under its Section 5 authority).

[56] *See* Tejas N. Narechania, *Certiorari, Universality, and a Patent Puzzle*, 116 MICH. L. REV. 1345, 1359–60 (2018) (citing empirical studies demonstrating that the majority of the Supreme Court's cases involve circuit splits). Not all circuit splits, however, result in Supreme Court review. *Id.* at 1360. In deciding whether to grant certiorari, the Supreme Court will evaluate whether a circuit split causes a sharp division in the application of federal law that creates geographical inconsistency. *Id.* The Supreme Court is less likely to review alleged splits that stem from factual or doctrinal distinctions. *Id.*

[57] *LabMD III*, 894 F.3d at 1231.

[58] *Id.* Generally, in dismissing a case, a court will make assumptions *arguendo* when the outcome of the case hinges on another line of reasoning. Joshua S. Stillman, *The Dangers of Hypothetical Statutory Jurisdiction (Even When Jurisdiction Exists)*, 4 SAVANNAH L. REV. 129, 136 n.56 (2017).

mon law.[59] Although the FTC did not identify the legal principle underlying the unfairness of LabMD's data security program, the court assumed that the FTC's complaint was grounded in common law negligence for the purposes of its decision.[60]

After determining that it need not address questions regarding the scope of the FTC's enforcement authority to resolve the case, the Eleventh Circuit turned to the narrower issue of the Order's enforceability.[61]

B. Unenforceability of the FTC's Order

The Eleventh Circuit vacated the Order on the grounds that it was unenforceable due to vagueness.[62] The court noted that remedial orders generally require clarity and precision to ensure that each respondent can comply with reasonable certainty.[63] The Order, however, simply mandated that LabMD implement and maintain a "reasonably designed" cybersecurity program that would protect consumers' personal information.[64] The Order did not explicitly prohibit LabMD from engaging in any particular act or practice.[65] This lack of specificity made the Order unenforceable because it would be impossible for LabMD to comply with the FTC's vague standard of reasonableness without further guidance.[66]

---

[59] *LabMD III*, 894 F.3d at 1231. Subsection (n) of Section 5 states that the FTC may consider public policy in determining "unfairness," but "public policy considerations may not serve as a primary basis for such determination." FTC Act § 5(n), 15 U.S.C. § 45(n) (2012). In *LabMD III*, the Eleventh Circuit interpreted Section 5 to mean that the existence of a substantial consumer injury alone could not establish an unfairness claim under Section 5. *LabMD III*, 894 F.3d at 1229 n.24.

[60] *LabMD III*, 894 F.3d at 1231. The FTC's argument rested on the idea that LabMD unintentionally invaded its consumers' right to privacy. *Id.* The Eleventh Circuit noted that negligence theory can support unintentional invasion claims. *Id.*

[61] *Id.*

[62] *Id.* at 1236. Although the court's decision turned on the Order's vagueness, LabMD devoted comparatively little attention to this argument in its answer brief. *See* Brief of Petitioner, LabMD, Inc. at 51–52, *LabMD III*, 894 F.3d 1221 (No. 9357), 2016 WL 7474626, at *51–52 (dedicating only two paragraphs to the argument that the Order was "impermissibly vague").

[63] *LabMD III*, 894 F.3d at 1235. The court noted that "an order's prohibitions should be clear and precise in order that they may be understood by those against whom they are directed." *Id.* (quoting Fed. Trade Comm'n v. Colgate-Palmolive Co., 380 U.S. 374, 392 (1965)).

[64] *Id.* at 1236. The applicable portion of the Order required LabMD to "establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers." *Id.* The court noted that the Order's other provisions were similarly vague. *Id.* at 1236 & n.41.

[65] *Id.* at 1236. The FTC's initial complaint did not allege that LabMD engaged in a particular unfair act or practice. *Id.* at 1225. Instead, it alleged that LabMD's data security program was unreasonable because the company failed to take certain data security measures that made the program deficient overall. *Id.*

[66] *Id.* at 1235–36. The court stated that the Order, if upheld, would require LabMD to completely revamp its data security program. *Id.*

The Eleventh Circuit reasoned that the Order's vagueness prevented it from being enforced through any available methods.[67] If the FTC filed a complaint in district court alleging that LabMD violated the Order's reasonableness requirements, the FTC would have difficulty proving by clear and convincing evidence that LabMD failed to comply with the Order because reasonableness is a flexible standard.[68] Alternatively, if the FTC filed a contempt motion related to a court-issued injunction, the district court would be placed in the difficult position of controlling LabMD's business decisions at the recommendation of the FTC.[69]

III. IMPLICATIONS OF *LABMD III*

Section A of this Part argues that the Eleventh Circuit Court of Appeals' decision in *LabMD III* creates unnecessary confusion regarding the scope of the FTC's enforcement powers under Section 5.[70] Section B of this Part contends that *LabMD III* places undue restrictions on the FTC's remedial powers in data privacy security actions.[71]

A. The Uncertain Scope of the FTC's Section 5 Enforcement Power Following LabMD III

By declining to evaluate the FTC's authority to enforce data privacy and security under Section 5's unfairness prong, the Eleventh Circuit missed a criti-

---

[67] *Id.* at 1237. There are two avenues for enforcing FTC cease and desist orders. *Id.* at 1234. First, the FTC may file a civil-penalty action in a district court alleging that a respondent violated an existing cease and desist order. FTC Act § 5(l). The district court may impose a penalty of up to $10,000 for each violation of the cease and desist order. *Id.* If the district court believes the respondent will continue to violate the cease and desist, it may issue an injunction. *Id.* Second, if the FTC has secured an injunction against the respondent, it may file a motion with the district court to find the respondent in contempt. *LabMD III*, 894 F.3d at 1234. In such cases, the respondent would be required to demonstrate that its actions have not violated the cease and desist order. *Id.* If the respondent fails to convince the court that a violation did not occur, the court will issue a show cause order. *Id.* For the respondent to ultimately be held in contempt, the FTC would need to prove by clear and convincing evidence that the respondent violated the injunction. *Id.*

[68] *LabMD III*, 894 F.3d at 1236–37. The court hypothesized what would happen if the FTC brought a complaint alleging that LabMD's failure to implement a specific data security measure ("X") that violated the Order. *Id.* The court theorized that LabMD and the FTC would then present competing expert testimony addressing whether X was a necessary component of a "reasonably designed" data security program. *Id.* The district court would then likely hold that it could not weigh the comparative value of the expert testimony, meaning that the FTC would fail to prove LabMD's contempt of the Order by clear and convincing evidence. *Id.* at 1236–37.

[69] *Id.* at 1237. If a district court held that LabMD's failure to implement X violated an injunction, the Eleventh Circuit believed that such holding would effectively modify the injunction. *Id.* Such holding would set precedent for future modifications, meaning that the FTC would essentially use the power of the court to direct LabMD's business. *Id.*

[70] *See infra* notes 72–89 and accompanying text.

[71] *See infra* notes 90–108 and accompanying text.

cal opportunity to clarify the scope of the FTC's enforcement powers.[72] If the court interpreted Section 5's unfairness prong as authorizing the FTC to enforce data privacy and security, it would have strengthened the FTC's enforcement efforts and further legitimized the current enforcement scheme.[73] Conversely, if the Eleventh Circuit held that the FTC lacked authority to bring suit against LabMD, it would have created a split with the Third Circuit Court of Appeals.[74] A circuit split would have increased the likelihood that the matter would be reviewed by the Supreme Court, thereby conclusively defining the scope of the FTC's authority.[75] Moreover, the broad invalidation of prior FTC data enforcement actions may have motivated Congress to explicitly implement a federal data privacy and security regulatory scheme.[76] Either way, a ruling on the question of the FTC's Section 5 enforcement authority would have brought greater transparency and predictability to the future of data privacy and security enforcement.[77]

Instead, the court allowed the FTC's enforcement authority under Section 5's unfairness prong to remain unchallenged, while simultaneously introducing an arguable restraint on the scope of that authority in dicta.[78] Under Section 5, an act or practice is unfair when it leads to a substantial consumer injury that consumers cannot prevent and is not outweighed by benefits to consumers or businesses.[79] *LabMD III* potentially limits which acts or practices qualify as unfair under Section 5 by asserting that unfairness must also be grounded in the Consti-

---

[72] *See* Pardau & Edwards, *supra* note 42, at 230 (noting that *LabMD, Inc. v. Fed. Trade Comm'n* (*LabMD III*), 894 F.3d 1221 (11th Cir. 2018), presented the Eleventh Circuit Court of Appeals with the opportunity to define the scope FTC's data privacy and security enforcement authority).

[73] *See id.* at 263 (stating that judicial approval of FTC enforcement actions could inspire the FTC to regulate data privacy and security with increasing regularity).

[74] *See* Fed. Trade Comm'n v. Wyndham Worldwide Corp., 799 F.3d 236, 246–47 (3d Cir. 2015) (validating the FTC's ability to bring data privacy and security enforcement actions under Section 5's unfairness prong).

[75] *See supra* note 56 and accompanying text.

[76] *See* Derek Hawkins, *The Cybersecurity 202: Google Faces Calls for Privacy Legislation, FTC Probe After Exposing User Data*, WASH. POST (Oct. 9, 2018), https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/10/09/the-cybersecurity-202-google-faces-calls-for-privacy-legislation-ftc-probe-after-exposing-user-data/5bbb86201b326b7c8a8d189f/?utm_term=.9205b09aaa34 [https://perma.cc/85U3-EFHD] (reporting that a Google data breach prompted Democratic officials to request an FTC investigation and the enactment of a federal privacy law).

[77] Ganka Hadjipetrova & Hannah G. Poteat, *States Are Coming to the Fore of Privacy in the Digital Era*, LANDSLIDE, July/Aug. 2014, at 12, 14 (arguing that the FTC cannot regulate data privacy and security without assistance from state regulators, in part, because the scope of FTC's enforcement authority is still disputed).

[78] *See LabMD III*, 894 F.3d at 1231 (accepting the FTC's authority to regulate data privacy and security *arguendo*, while also requiring that authority to derive from the Constitution, statute, or common law).

[79] FTC Act § 5(n), 15 U.S.C. § 45(n) (2012).

tution, statute, or the common law.[80] The court stated that mere consumer injury is insufficient to support a Section 5 enforcement claim.[81]

Although the Eleventh Circuit stated this requirement in dicta, it introduced an additional factor to Section 5's unfairness test that would meaningfully restrain future FTC data security enforcement actions if followed by other courts.[82] The FTC would be unable to ground future Section 5 unfairness claims in a constitutional right to privacy because the Constitution does not protect against the mishandling of personal information by private companies.[83] The FTC would also struggle to root such actions in statute because it relies on its Section 5 authority in cases where existing data privacy and security statutes are inoperative.[84] Accordingly, the FTC would need to support its Section 5 unfairness actions by appealing to common law theories like negligence or breach of fiduciary duty.[85] Many courts, however, have struggled to find the requisite elements of common law causes of action in other data security cases.[86]

The Eleventh Circuit did little to clarify whether it believes that the introduction of a stricter unfairness test should significantly constrain Section 5 unfairness claims.[87] The court simply assumed *arguendo* that the FTC grounded its

---

[80] *See LabMD III*, 894 F.3d at 1231 (stating in dicta that an FTC enforcement action would be invalidated if it was not grounded in established policies found in the Constitution, statute, or the common law).

[81] *Id.* at 1229 n.24.

[82] *See* Frankel, *supra* note 11 (contending that future litigants could point to the Eleventh Circuit's dictum when challenging the validity of FTC complaints). A dictum does not carry the same authority as court holdings, but some construe dictum as "quasi-authority" because it generally influences future court decisions. EUGENE WAMBAUGH, THE STUDY OF CASES: A COURSE OF INSTRUCTION IN READING AND STATING REPORTED CASES, COMPOSING HEAD-NOTES AND BRIEFS, CRITICIZING AND COMPARING AUTHORITIES, AND COMPILING DIGESTS 103 (2d ed. 1894) (providing instruction on how to interpret court cases).

[83] William McGeveran, *Friending the Privacy Regulators*, 58 ARIZ. L. REV. 959, 975–76 (2016) (comparing the FTC's enforcement authority to that of its European counterparts).

[84] *See* Hartzog & Solove, *supra* note 30, at 2236 (positing that Section 5 is broadly drafted to allow the FTC to regulate sectors not otherwise regulated by statute).

[85] *See* Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737, 749 (2018) (listing negligence and breach of fiduciary duty as common causes of action alleged in the wake of data breach).

[86] *See* David J. Baldwin et al., *Insuring Against Privacy Claims Following a Data Breach*, 122 PENN. ST. L. REV. 633, 689–91 (2017) (noting that courts have been inconsistent in finding negligence in data breach cases). In particular, data breaches can bring into question whether a company that holds consumer data is under duty to protect it. *Id.* at 689–90. In cases where a hacker steals personal information from company computer systems, courts are reluctant to hold the company liable for third-party criminal activity. *Id.* at 690–91. Additionally, courts often reject the argument that data breaches lead to cognizable harm if consumers experience no monetary, property, or physical damage. Solove & Citron, *supra* note 85, at 754.

[87] *See LabMD III*, 894 F.3d at 1231 (accepting *arguendo* that the FTC's litigation against LabMD is supported by a theory of negligence without providing detailed support for that proposition). Although the Eleventh Circuit assumed *arguendo* that the FTC had sufficient grounds for bringing suit, it previously questioned whether Section 5 covered intangible consumer injuries when granting LabMD's motion for stay of the Order. *See* LabMD v. Fed. Trade Comm'n (*LabMD III Motion for Stay*), 678 F. App'x

complaint in common law negligence without in-depth analysis.[88] Accordingly, the Eleventh Circuit added further uncertainty into the data privacy and security enforcement arena by introducing a new unfairness test for consideration by other courts, yet failing to apply it.[89]

B. LabMD III*'s Undue Restrictions on the FTC's Remedial Powers in Data Privacy and Security Enforcement Actions*

The Eleventh Circuit's decision also placed unwarranted restrictions on the FTC's remedial power by invalidating its historical approach to data privacy and security consent orders.[90] The court struck down the Order because it required LabMD to comply with a standard of reasonableness that the court found unjustifiably vague.[91] The concept of reasonableness, however, is not as vague as the court suggested.[92] As noted in its appellate brief, the FTC regularly issues materials that clarify its position on established and emerging data privacy and security issues.[93] The FTC has also entered into numerous publicly available settlement agreements that specifically detail its view of reasonable data security programs.[94] The Third Circuit, in *Federal Trade Commission v. Wyndham Worldwide Corp.*, cited these materials and settlement agreements as relevant in de-

816, 820–21 (11th Cir. 2016) (holding that Section 5 does not clearly support the FTC's authority to enforce actions related to intangible harms). The court had intimated that LabMD made a persuasive argument that the injury contemplated in this case was "not even intangible . . . but purely conceptual." *Id.*

[88] *See LabMD III*, 894 F.3d at 1231 (stating that the FTC could conceivably establish an unfairness claim in data security actions by pointing to common law negligence).

[89] *See id.* (declining to analyze the supposed negligence claim underlying *LabMD III* in detail).

[90] *See* Daniel J. Solove & Woodrow Hartzog, *Did the* LabMD *Case Weaken the FTC's Approach to Data Security?*, TEACH PRIVACY (June 8, 2018), https://teachprivacy.com/did-labmd-case-weaken-ftc-approach-to-data-security/ [https://perma.cc/3FKE-PKB4] (indicating that the Eleventh Circuit's decision does not fully consider the context of the FTC's data privacy and security enforcement program).

[91] *LabMD III*, 894 F.3d at 1236–37.

[92] *See* Solove & Hartzog, *supra* note 90 (arguing that the Eleventh Circuit exaggerated the ambiguities created by the application of a reasonableness standard).

[93] Brief of the Federal Trade Commission, at 50–52, *LabMD III*, 894 F.3d 1221 (No. 9357), 2017 WL 562771, at *50–52. These materials are publicly-available on the FTC's website. *See, e.g.*, FED. TRADE COMM'N, DATA BREACH RESPONSE: A GUIDE FOR BUSINESS (2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0154_data-breach-response-guide-for-business.pdf [https://perma.cc/9NWC-MDRW] (recommending measures that businesses should take in the wake of a data breach); FED. TRADE COMM'N, PEER-TO-PEER FILING SHARING: A GUIDE FOR BUSINESS (2010), https://www.ftc.gov/tips-advice/business-center/guidance/peer-peer-file-sharing-guide-business [https://perma.cc/J8TU-MCFA] (outlining best practices for corporate use of peer-to-peer networks); Jessica L. Rich, Comment, *Big Data, Consumer Privacy, and Consumer Bill of Rights*, FED. TRADE COMM'N (Aug. 1, 2014), https://www.ftc.gov/system/files/documents/public_statements/573301/140801bigdatacomment.pdf [https://perma.cc/5W96-RP44] (clarifying the FTC's position on developments in "big data").

[94] DANIEL J. SOLOVE & PAUL M. SCHWARTZ, PRIVACY LAW FUNDAMENTALS 165–66 (4th ed. 2017) (indicating the FTC settlement agreements have common requirements surrounding privacy policies, auditing, recordkeeping, risk assessment, and employee training).

termining whether the petitioner had been provided fair notice of the FTC's interpretation of unfairness.[95] Although these material and settlement agreements do not constitute binding precedent, courts frequently consider administrative materials that are neither regulations nor binding court decisions.[96] Indeed, privacy professionals generally regard FTC settlement agreements as carrying precedential force.[97] Nevertheless, the Eleventh Circuit wholly ignored them.[98] Furthermore, the court did little to clarify why reasonableness is an exceedingly vague standard within the data security enforcement context, but it is sufficiently specific in other areas of the law.[99]

The court also did not address the long-term implications of constraining the FTC's remedial powers.[100] *LabMD III* mandated that the FTC remediate data privacy and security actions with greater specificity.[101] In effect, this requires the FTC to issue backward-looking consent orders that obligate companies to implement data security programs built on then-existing technologies.[102] Before *LabMD III,* FTC consent orders accounted for new and emerging technologies because the FTC could easily redefine reasonableness through its guidelines and settlements.[103] Post-*LabMD III*, the FTC will likely struggle to draft language that is sufficiently broad enough to accommodate key technological changes.[104]

---

[95] Fed. Trade Comm'n v. Wyndham Worldwide Corp., 799 F.3d 236, 256–57 (3d Cir. 2015). *But see* Geoffrey A. Manne & Kristian Stout, *When "Reasonable" Isn't: The FTC's Standardless Data Security Standard*, 15 J.L. ECON. & POL'Y 67, 75 (2019) (contending that the FTC's materials and settlement agreement fail to create a common law-like framework that shares the "rigor of a judicial opinion").

[96] *Wyndham*, 799 F.3d at 257.

[97] Solove & Hartzog, *supra* note 8, at 621.

[98] *See generally LabMD III*, 894 F.3d 1221 (lacking consideration of FTC administrative materials and settlement agreements).

[99] *See, e.g.*, Solove & Hartzog, *supra* note 90 (arguing that the body of law surrounding data privacy and security enforcement is not particularly vague in comparison to other areas of the law). For example, the Eleventh Circuit previously held that credit reporting agencies must conduct reasonable investigations of consumer disputes under the Fair Credit Reporting Act. Hinkle v. Midland Credit Mgmt, Inc., 827 F.3d 1295, 1302 (11th Cir. 2016). The court also held that plaintiffs cannot bring employment discrimination suits under the Americans with Disabilities Act if the employer's actions were reasonably motivated. Chapman v. AI Transport, 229 F.3d 1012, 1030–31 (11th Cir. 2000).

[100] *See LabMD III*, 894 F.3d at 1236–37 (addressing the perceived ill-effects of upholding the reasonableness standard, but failing to consider the long-term implications of requiring specificity in consent orders).

[101] *Id.* at 1236–37

[102] *See* Skelton, *supra* note 38, at 306 (suggesting the pre-*LabMD III* FTC enforcement scheme provided a meaningful contrast to federal laws that lagged behind developments in technology).

[103] *See id.* at 323 (noting that, prior to *LabMD III*, the FTC efficiently policed companies working with new technologies that failed to implement reasonable safeguards).

[104] *See* Jim Harvey et al., LabMD: *The End of the FTC in Cyber, or Just a New Path?*, ALSTON & BIRD: PRIVACY & DATA SECURITY ADVISORY (Jul. 9, 2018), https://www.alstonprivacy.com/labmd-the-end-of-the-ftc-in-cyber-or-just-a-new-path/ [https://perma.cc/3FPR-F6LG] (positing that *LabMD III* will challenge the FTC to draft consent orders that are narrow enough to comply with the Eleventh Circuit's decision, but also broad enough to account for technological developments).

By restraining the FTC's remedial powers, *LabMD III* also casts doubt over the FTC's ability to enforce existing consent orders that employ similarly broad remedial language.[105] If the FTC attempts to enforce these consent orders, the respondents would be in strong defensive positions to invalidate them.[106] Even though *LabMD III* is not binding outside the Eleventh Circuit, it could serve as highly persuasive authority in federal courts nationwide.[107] Accordingly, companies that have experienced massive data security failures could be held unaccountable for future data breaches.[108]

CONCLUSION

LabMD III presents more questions than answers about the future of FTC data privacy and security enforcement actions. The Eleventh Circuit should have seized the opportunity to provide necessary clarity as to the scope of the FTC's enforcement authority. Instead, the court perpetuated uncertainty by evading *LabMD III*'s central issue, while also introducing a new requirement surrounding the meaning of unfairness. Moreover, the court unduly constrained the FTC's remedial powers. By striking down the FTC's interpretation of reasonable consent order, the Eleventh Circuit ignored the history and context surrounding FTC enforcement actions. As a result, *LabMD III* placed the FTC in a weakened position without creating a clear mechanism for the regulation of new technologies or existing consent orders.

JULIA WHALL

Preferred citation: Julia Whall, Comment, *Policing Cyberspace: The Uncertain Future of Data Privacy and Security Enforcement in the Wake of* LabMD, 60 B.C. L. REV. E. SUPP. II.-149 (2019), http://lawdigitalcommons.bc.edu/bclr/vol60/iss9/11/.

---

[105] *Eleventh Circuit* LabMD *Decision Significantly Restrains FTC's Remedial Powers in Data Security and Privacy Actions*, WILSON, SONSINI, GOODRICH & ROSATI (June 18, 2018), https://www.wsgr.com/WSGR/Display.aspx?SectionName=publications/PDFSearch/wsgralert-LabMD.htm [https://perma.cc/6722-CMCL] [hereinafter *Remedial Powers*] (addressing possible implications of *LabMD III*).

[106] *See id.* (suggesting that companies currently bound by broadly-worded FTC consent orders could cite *LabMD III* as authority for invalidating those consent orders).

[107] *See* Chad Flanders, *Toward a Theory of Persuasive Authority*, 62 OKLA. L. REV. 55, 63–64 (2009) (indicating that the opinions of other circuit courts carry greater weight than any other form of persuasive authority).

[108] *See Remedial Powers*, *supra* note 105 (contending that the validity of all existing FTC data privacy and security settlement agreements brought under Section 5's unfairness prong remains uncertain).