CENTER FOR DEMOCRACY & TECHNOLOGY

LabMD v. FTC: Tackling "Unfair" Data Security Practices in the Eleventh Circuit

The latest skirmish in the nearly seven-year battle between diagnostic testing company LabMD and the Federal Trade Commission begins on Wednesday, June 21st, as oral arguments are held in the Eleventh Circuit Court of Appeals.[1] The case's eventual outcome promises to have serious ramifications for the FTC's much-needed ability to police industry data security practices. Thus far, the Eleventh Circuit has appeared skeptical of the FTC's legal authority to address the precise data security lapses alleged against LabMD, and a decision against the FTC could limit its data security enforcement activities.

Data security needs robust enforcement. The number of data breaches and security incidents continues to grow at a rapid pace,[2] and as recent headlines make clear, the healthcare industry is particularly susceptible to data security vulnerabilities.[3] Part of the challenge lies in both the inherent sensitivities of health data and evolving technologies such as interconnected devices. This combination raises the risk of systems intrusions via ransomware attacks[4] and a host of other cybersecurity vulnerabilities that healthcare entities have yet to address adequately.[5] The FTC has repeatedly stated that companies must implement "reasonable" security measures and that the failure to do so can be an unfair act or practice under Section 5(a) of the FTC Act.

LabMD argues that the FTC has overstepped its regulatory authority, and if the Eleventh Circuit agrees, it may undermine fifteen years of data security enforcement activities by the Commission. Across over sixty different enforcement actions, the FTC has played an important role in establishing a data security baseline and providing significant guidance on the evolution of good data security. These actions were initially tied to misleading privacy policies or other public promises under the FTC's authority to police *deceptive* statements,[6] but beginning in 2005, the FTC began to argue that unreasonable data security measures were also *unfair* under Section 5 of the FTC Act, regardless of any public representation

---

[1] Oral Arguments Calendar, *available at* http://www.ca11.uscourts.gov/sites/default/files/oral_arguments/cal22_0.pdf.

[2] In 2012, California businesses reported 131 breaches, affecting 2.6 million records; in 2015, 178 breaches affecting 24 million records; and in 2016, there were 657 data breaches, affecting a total of over 49 million records. *See* California Data Breach Report 2016, https://oag.ca.gov/breachreport2016.

[3] *See id.*

[4] *See e.g.,* How US healthcare spent the weekend protecting against WannaCry (May 2017), http://www.healthcareitnews.com/news/how-us-healthcare-spent-weekend-protecting-against-wannacry.

[5] *See e.g.,* Abraham Gitterm & Neha Patel, Not Enough: FDA Finds Ongoing Cybersecurity Vulnerabilities with St. Jude Medical's Implantable Cardiac Devices (April 2017), http://www.digitalhealthdownload.com/2017/04/not-enough-fda-finds-ongoing-cybersecurity-vulnerabilities-st-jude-medicals-implantable-cardiac-devices/.

[6] In 2002, the FTC brought its first data security enforcement case for the inadvertent disclosure of sensitive personal information when Eli Lilly revealed the email addresses of all Prozac users on a mailing list. Howard Beales, then director of the FTC's Bureau of Consumer Protection, warned that "[e]ven the unintentional release of sensitive medical information is a serious breach of consumers' trust. Companies that obtain sensitive information in exchange for a promise to keep it confidential must take appropriate steps to ensure the security of that information." Fed. Trade Comm'n, Press Release, Eli Lilly Settles FTC Charges Concerning Security Breach (Jan. 18, 2002), https://www.ftc.gov/news-events/press-releases/2002/01/eli-lilly-settles-ftc-charges-concerning-security-breach.

about a company's security practices.[7] In order for a data security practice to be considered unfair, the FTC must determine whether the data security practices are (1) likely to cause substantial injury to consumers, (2) that this injury is not reasonably avoidable by consumers themselves, and (3) that the injury is not outweighed by countervailing benefits to consumers or to competition.[8]

How these unfairness criteria may map onto data security lapses is at the core of the tension in the *LabMD* case. Specifically, oral argument may elucidate thinking around two key questions, previewed by the Third Circuit in another data security dispute between the FTC and Wyndham Worldwide Corporation:[9] (1) What are the contours of a "substantial injury" when evaluating unfair data security practices and how should data security's costs and benefits be evaluated? and (2) What constitutes fair notice and "ascertainable certainty" of the FTC's expectations for "reasonable" data security?

Background

Georgia-based LabMD was in the business of providing medical testing and diagnostic services. As a result of these activities, the company collected sensitive personal information including test results, Social Security numbers, and insurance data. At some point in 2008, a LabMD employee shared access to a computer folder on the now-defunct LimeWire peer-to-peer sharing platform. Exploiting security vulnerabilities in LimeWire, data security company Tiversa was able to acquire a LabMD insurance billing file containing 1,718 pages of sensitive data for over 9,300 patients. Tiversa then approached LabMD about the file, exhorting its fee-based data security services. In 2010, after LabMD rebuffed Tiversa's advances, the data security company forwarded information about the file, coined the "1718 File," to the FTC, beginning a multiyear investigation and protracted legal battle.

In 2013, the FTC brought an administrative complaint against LabMD, which was dismissed by an Administrative Law Judge (ALJ) in November 2015. The ALJ's decision rejected the FTC's theory that mere disclosure of the 1718 File caused, or was likely to cause, substantial injury to consumers as required by Section 5.[10] FTC staff appealed the decision before the full Commission, and one year later the agency unanimously overruled its own ALJ.[11] LabMD immediately appealed the agency's final ruling before the Eleventh Circuit Court of Appeals, asking the court for a stay of the FTC's order pending the appeal. LabMD, which had since been shuttered, argued that the company would likely win its appeal *and* be irreparably harmed in the meantime. In a surprising development, the Eleventh Circuit agreed

[7] BJ's Wholesale Club, Inc., Case No. C-4148 (Sept. 20, 2005), http://www.ftc.gov/sites/default/files/documents/cases/2005/09/092305do0423160.pdf (decision and order).
[8] 15 U.S.C. § 45(n).
[9] FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015).
[10] *See* In re LabMD, Inc., Docket No. 9357, ALJ's Initial Decision (F.T.C. Nov. 13, 2015), https://www.ftc.gov/system/files/documents/cases/151113labmd_decision.pdf.
[11] *See* In re LabMD, Inc., Docket No. 9357, Op. of the Comm'n and Final Order (F.T.C. July 29, 2016), https://www.ftc.gov/system/files/documents/cases/160729labmd-opinion.pdf [hereinafter FTC Opinion].

to the stay, suggesting the court might be more sympathetic to LabMD's legal arguments than expected.[12]

What Constitutes Substantial Injury?

Both the FTC's ALJ and the Eleventh Circuit challenged the agency's interpretation of "substantial injury," a key element for the FTC in determining unfairness. According to the ALJ, because the FTC could not show that anyone other than Tiversa (and FTC staff) had accessed or viewed the 1718 File, it was difficult to see how any individual had been or would be "harmed" in the future.[13] The Eleventh Circuit stayed the FTC's order against LabMD, suggesting that it was not clear that "a reasonable interpretation [of Section 5] includes intangible harms like those that the FTC found in this case," and it also questioned whether "emotional impact" is a cognizable harm under Section 5.[14]

By contrast, the FTC has long given closer scrutiny to business practices involving the use or disclosure of medical information, which it considers to be highly sensitive. Accordingly, in the *LabMD* dispute, the FTC has taken the position that the unauthorized disclosure of sensitive medical information is, in and of itself, a concrete privacy harm rising to the level of "substantial injury."[15]

Critics argue that this cannot be so. They point to the FTC's longstanding *Policy Statement on Unfairness*, which clarified that the FTC was "not concerned with trivial or merely speculative harm. In most cases a substantial injury involves monetary harm . . . Unwarranted health and safety risks may also support a finding of unfairness. Emotional impact and other more subjective types of harm, on the other hand, will not ordinarily make a practice unfair."[16]
Indeed, the FTC has traditionally focused on concrete harms that result from the misuse of information, such as risks to physical security from electronic stalking, economic injury resulting from identity theft, or unwanted intrusions into daily life via spam or telemarketing.[17]

---

[12] LabMD, Inc. v. FTC, No. 16-16270-D, Order Granting Stay (11th Cir. Nov. 10, 2016), http://f.datasrvr.com/fr1/016/73315/2016_1111.pdf.

[13] As discussed in the LabMD administrative proceeding, 40 LabMD "day sheets" containing the information of 600 people were uncovered by Sacramento police which searching the home of suspected identity thieves, though the ALJ similarly found that the lack of any evidence of consumer complaints resulting from that incident also weighed against any finding of harm.

[14] The court further cited LabMD's suggestion that this case involves "conceptual" rather than intangible harms. LabMD, Inc., Order Granting Stay at 9.

[15] LabMD, Inc. v. FTC, No. 16-16270-D, Brief of the Fed. Trade Comm'n 17 (Feb. 09, 2017) [hereinafter FTC Brief].

[16] Fed. Trade Comm'n, Policy Statement on Unfairness (Dec. 17, 1980), https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness.

[17] Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change, Preliminary Staff Report (2010) (citing Remarks of FTC Chairman Tim Muris at the Privacy 2001 Conference (Oct. 4, 2001)).

In response to these criticisms, the FTC rejected the notion that an invasion of privacy is merely an "emotional harm."[18] Instead, the agency argues that the concrete harm comes from the exposure of and access to private information by unauthorized persons. This violation depends neither on a victim's mental state nor the emotional harms dismissed by the *Unfairness Policy Statement*.[19] It is an open question how far such logic should go with respect to information privacy generally, but the exposure of sensitive health information has been viewed as a harm historically.

Established public policy around medical information supports this argument. Numerous laws and court cases recognize that the unauthorized disclosure of this type of information, by itself, is a legally cognizable injury. Though LabMD argues that "legally cognizable" cannot mean "substantial,"[20] it is likely such an argument would come as cold comfort to the patients whose data found its way onto LimeWire.

Measuring Costs and Benefits of Reasonable Security

Determining whether an act or practice is unfair is ultimately a cost-benefit test, as the disagreement over how to quantify the magnitude of harm presented by LabMD's breach suggests.[21] In fact, the third prong of Section 5(n) explicitly instructs the FTC to weigh the potential harms to consumers against any countervailing benefits, and cost-benefit analysis has often become a flashpoint in privacy and security matters.

The normative role of qualitative costs and benefits in any legal analysis – including the protection of privacy and other intangible values – is a contentious issue.[22] Privacy advocates are skeptical of some of the alleged benefits of data collection and use, while economists minimize the costs of subjective privacy harms such as embarrassment or reputational damage, whether real or perceived.

LabMD brings renewed attention to the rigor of this balancing process.[23] One of LabMD's chief arguments is that the FTC failed to both accurately compare the company's present and future costs of

---

[18] FTC Brief at 23.

[19] FTC Brief at 28.

[20] LabMD, Inc. v. FTC, No. 16-16270-D, Reply Brief of LabMD, Inc. 4 (Mar. 09, 2017) [hereinafter LabMD Reply Brief].

[21] J. Howard Beales III & Timothy J. Muris, *Choice or Consequences: Protecting Privacy in Commercial Information*, 75 U. Chi. L. Rev. 109, 132 (2008).

[22] Remarks of FTC Commissioner Julie Brill before the TACD 16th Annual Forum, The Precautionary Principle in TTIP: Trade Barrier or Essential for Consumer Protection? (Jan. 26, 2016), https://www.ftc.gov/system/files/documents/public_statements/913213/160126tacdkeynote.pdf.

[23] FTC Acting Chairman Maureen Ohlhausen has recently re-committed the FTC to being thorough in the application of cost-benefit analysis to consumer protection matters. Remarks of FTC Acting Chairman Maureen Ohlhausen at the ABA 2017 Consumer Protection Conference (Feb. 2, 2017), https://www.ftc.gov/system/files/documents/public_statements/1069803/mko_aba_consumer_protection_conference.pdf.

complying with a consent order as well as the likelihood that implementing the FTC's requirements would have reduced the likelihood of substantial injury.[24] In response, the FTC has suggested that LabMD has pulled "from thin air" a complex formula for evaluating costs that is "unmoored from anything in the statute."[25]

That said, the matter is generally more clear in the context of data security. As the Third Circuit explained in *Wyndham*, when dealing with a failure to provide reasonable data security, "countervailing" benefits are the costs of "investment in stronger cybersecurity" in comparison to the cost of a company's existing "level of cybersecurity."[26]Industry practices may be especially unfair where security deficiencies are clear and low-cost steps could have been taken to readily address those problems.[27] In this case, LabMD focuses on many of the perceived costs to the company of complying with the FTC's demands, but this minimizes that some of LabMD's deficiencies were obvious and easily rectified. LabMD could have avoided exposure of the 1718 File by using tools to detect security vulnerabilities, employee training, and providing employees with non-administrative accounts that would have prohibited them from installing LimeWire.[28]

Employee File-Sharing and Expectations of Reasonable Data Security Measures

While LabMD acknowledged sensitive medical information should be kept "secure" and "private" and that disclosing this information was "a violation of Federal Law," the company continues to argue that it lacked fair notice of which of these assorted security measures were required by Section 5.[29] As the Supreme Court has explained, companies must "know what is required of them so they may act accordingly; and precision and guidance are necessary so that those enforcing the law do not act in an arbitrary or discriminatory way."[30]

According to the FTC, the answer to this question is simple: Businesses need only employ reasonable security measures.[31] But what are reasonable security measures? The FTC recognizes that data security threats and standards are constantly evolving and, as a result, the agency's evaluation of "reasonableness" assess issues, such as the costs of available security controls and tools, the sophistication and size of the company, and the sensitivity of consumer information, are at stake.[32]

---

[24] LabMD, Inc. v. FTC, No. 16-16270-D, Brief of LabMD, Inc. 4 (Dec. 27, 2016) [hereinafter LabMD Brief].

[25] FTC Brief at 38.

[26] Wyndham, 799 F.3d at 255.

[27] Beales & Muris, *supra* note 17, at 132-33 (acknowledging that unfairness theories can be subject to abuse and "[c]ases involving accidental or incidental information loss, however, are far more problematic.")

[28] FTC Brief at 37; FTC Opinion at 22-23.

[29] FTC Brief at 45; LabMD Brief at 38-43.

[30] FCC v. Fox Television Stations, Inc., 132 S. Ct. 2307 (2012).

[31] Fed. Trade Comm'n, Data Security, https://www.ftc.gov/datasecurity (last visited June 20, 2017).

[32] *Id.*

Admittedly, beyond those factors, it is not clear that this universe of materials provides "ascertainable certainty" as to what conduct is actually required under the FTC's interpretation of Section 5.

Furthermore, it is unclear what FTC guidance was available to LabMD in 2008. The Third Circuit largely avoided answering this question because Wyndham repeatedly and perhaps foolishly argued that none of the FTC's interpretations of Section 5 were valid.[33] However, the Eleventh Circuit may need to parse the relative authoritativeness of the FTC's public guidance and enforcement activities.

At a basic level, the FTC is arguing that no information security program that is reasonably designed to protect sensitive medical information would have allowed an employee to install and use LimeWire at LabMD.[34] The question for the Eleventh Circuit hinges on whether a company in LabMD's position in 2008 should have trained employees on the dangers of peer-to-peer file sharing or prevented them from installing software such as LimeWire.

A timeline of general public awareness of these issues shows how difficult that analysis may be. Security researchers began flagging the security risks posed by online file sharing as early as 2002,[35] and the FTC held a workshop and published a staff report highlighting these dangers in 2005.[36] But the agency's guidance to companies on the risks posed by peer-to-peer software were not issued until 2010.[37] The risks associated with these types of software are more clearly understood in 2017, but whether or not LabMD should have been on notice is not so clear.

Data Security Enforcement Today

In the nine years since the 1718 File fell into Tiversa's hands, the FTC's interpretation of unfair and unreasonable data security has been fleshed out. The FTC's complaint against LabMD demonstrates

---

[33] Still, the Third Circuit offered some thoughts as to what segment of consent decrees, written guidance, and complaints could have provided the needed ascertainable certainty to LabMD. *See* Wyndham at 46.

[34] FTC Brief at 55. Specifically, the FTC has alleged that LabMD: (1) failed to develop, implement, or maintain a comprehensive information security program; (2) did not use readily available measures to identify known or potential security risks; (3) did not use adequate access controls; (4) did not provide adequate training to employees; (5) did not deploy common authentication-related security measures; (6) did not maintain or update computer operating systems; and (7) did not employ readily available measures to prevent unauthorized access to personal information on LabMD's computer systems.

[35] Peer-to-Peer File-Sharing Networks: Security Risks (2002), https://www.sans.org/reading-room/whitepapers/policyissues/peer-to-peer-file-sharing-networks-security-risks-510; Nathaniel S. Good & Aaron Krekelberg, Usability and Privacy: A Study of Kazaa P2P File-sharing (June 2002), http://graal.ens-lyon.fr/~abenoit/reso06/papier/kazaa.pdf.

[36] *See* FTC Staff Report, Peer-to-Peer File-Sharing Technology: Consumer Protection and Competition Issues (2005).

[37] Fed. Trade Comm'n, Peer-to-Peer File Sharing: A Guide for Business (Jan. 2010), https://www.ftc.gov/tips-advice/business-center/guidance/peer-peer-file-sharing-guide-business.

how times have changed: lawyers immediately advised businesses to "take heed and use the FTC's list of LabMD's failed security practices and procedures as guidelines."[38]

Reasonable data security is an evolving target, and the FTC has continued to issue new data security complaints and put forward guidance that elaborates upon these expectations. For example, the FTC's "Start with Security" guidance is a compendium of practical tips that is drawn directly from its data security enforcement cases. Among the data security practices discussed, it addresses the need to sensibly control access to data, to secure remote access to networks and computer systems, and to put procedures in place to keep security current and to address security vulnerabilities – three themes directly relevant to LabMD's alleged security lapses.[39]

The Eleventh Circuit must acknowledge that the FTC has now spent years convening workshops, issuing numerous reports, and working with industry and other multi stakeholder efforts to develop self-regulatory codes of conduct and best practices that address data security.[40] While there are limits to the FTC's approach to data security – and LabMD has raised important questions both as to how the FTC pursues data security lapses and what sorts of information might better inform industry players – the agency's actions have served to put companies on notice, giving information security professionals and company lawyers leverage to keep pushing for better industry security practices.[41]

The end result has been better data security that has protected individuals and their sensitive information. The Eleventh Circuit ought to consider carefully what impact limiting the reach of unfairness to address unreasonable data security practices may have. Oral arguments may provide a hint in either direction.

---

[38] *E.g.*, Linn Foster Freedman & Kathryn Sylvia, *What LabMD's Data Security Breach Tells Us About FTC* (Oct. 3, 2013), https://www.law360.com/articles/477398/what-labmd-s-data-security-breach-tells-us-about-ftc.

[39] Fed. Trade Comm'n, Start with Security (June 2015), https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business. LabMD, like Wyndham before it, takes issue with the FTC's 2007 business guidance, arguing that it was insufficient with respect to Section 5's demands.

[40] Kenneth A. Bamberger & Deirdre K. Mulligan, Privacy on the Books 286 (2015).

[41] *See id.*