ALSTON & BIRD

WWW.ALSTON.COM

Privacy & Data Security ADVISORY ■

JULY 9, 2018

LabMD: The End of the FTC in Cyber, or Just a New Path?

By Jim Harvey, Larry Sommerfeld,* and Kate Hanniford

Last month, the U.S. Court of Appeals for the Eleventh Circuit issued its opinion in *LabMD, Inc. v. FTC*, No. 16-16270 (11th Cir. June 6, 2018), declaring unenforceable a Federal Trade Commission (FTC) order requiring LabMD to implement an extensive cybersecurity plan. This article will review the history of the matter, which influences its posture, and the opinion itself. We also discuss potential future FTC cyber enforcement in light of both *LabMD* and a prior Third Circuit case, *FTC v. Wyndham Worldwide Corp*.

Procedural Background

The *LabMD* matter dates to 2005, when LimeWire file sharing software was installed on a company computer in violation of company policy. According to the Court, a LabMD employee designated the contents of the employee's "My Documents" folder for sharing. In doing so, the employee exposed a file containing the healthcare information of 9,300 patients. In February 2008, a computer security company, Tiversa, downloaded that file and used the healthcare information it contained to pitch its cybersecurity services to LabMD. When LabMD refused Tiversa's services, Tiversa gave the information to both the FTC and a college professor who used the information as part of a publication on data security in the healthcare industry.

After an investigation, the FTC issued an administrative complaint against LabMD and assigned an administrative law judge (ALJ) to the case, alleging that LabMD's data security program was inadequate and therefore constituted an "unfair act or practice" under 5(a) of the Federal Trade Commission Act. The FTC argued that LabMD's cybersecurity measures were deficient as a whole, eventually proposing an order "which would regulate all aspects of LabMD's data-security program" and "sweeping prophylactic measures" that would require the company to "maintain a data-security program 'reasonably designed' to the Commission's satisfaction" for at least 20 years. Meanwhile, LabMD denied that it had engaged in unfair trade practices and challenged the FTC's authority under Section 5 of the Federal Trade Commission Act to regulate its handling of personal information. LabMD is no longer in business and ceased to do business prior to the Eleventh Circuit decision.

The ALJ dismissed the FTC's complaint, holding that the agency failed to prove that LabMD did not "employ reasonable data security" measures that "caused, or [were] likely to cause substantial injury to consumers." The FTC appealed the ruling to the Commission itself, which unanimously reversed the ALJ's decision in July 2016, finding that LabMD's data security practices were unfair under Section 5 and that Section 5(a)'s unfairness standard was not void for vagueness. (The staff of the FTC Bureau of Consumer Protection may bring administrative complaints before an ALJ. Either the FTC staff or respondents may petition the full Commission for review of an ALJ initial decision.)

Following the Commission's opinion, LabMD requested and the Commission denied a stay of the order pending review by the Eleventh Circuit. LabMD moved the Eleventh Circuit to stay enforcement of the FTC order because "compliance with the order was unfeasible given LabMD's defunct status and *de minimis* assets," and in November 2016, the Court unanimously granted the motion over the FTC's objections. LabMD then petitioned the Eleventh Circuit for review.

The Eleventh Circuit Ruling

On June 6,, 2018, the Eleventh Circuit reversed the commission's ruling upon a de novo review. According to the Court, the FTC had the authority to simply order LabMD to implement a program preventing employees from installing third-party software on their company computers, thus addressing the relevant data security incident. Instead, the Eleventh Circuit held, the FTC's order required the company's data security program "to meet an indeterminable standard of reasonableness." Rather than "enjoin a specific act or practice," the order mandated "a complete overhaul of LabMD's data-security program and says precious little about how this is to be accomplished." The practical result, observed the Court, "is that the district court is put in the position of managing LabMD's business in accordance with the Commission's wishes...as if the Commission was LabMD's chief executive officer and the court was its operating officer." The Court held that "this micromanaging is beyond the scope of court oversight contemplated by injunction law."

In reaching its decision, the Court discussed the scope of the FTC's unfairness authority. The applicable standard defines unfairness as any act that "(1) caused consumers, competitors, or other businesses substantial injury; [or] (2) offended public policy as established by statute, the common law, or otherwise." The Court then explained that the second "public policy" prong of the unfairness test requires that unfairness "be grounded in statute, judicial decisions—i.e., the common law—or the Constitution."

Thus, the Court reasoned, for LabMD's actions to have been unfair, they must have violated "'clear and well-established' policies that are expressed in the Constitution, statutes, or the common law." While the commission's decision here failed to expressly cite any clearly established statute or common law principle that LabMD violated, the Court nevertheless reasoned that the judicially enshrined public policy used by the commission was the common law of negligence. And while both sides briefed the issue of substantial injury (the first prong of the unfairness test), the Court did not address it in its holding.

After reviewing the elements of negligence, the Court reframed LabMD's unfair practice as the unintentional invasion of the right to privacy. Having done so, the Court then assumed for the sake of argument that LabMD's negligence in failing to reasonably protect consumer information constituted an unfair practice.

Ultimately, the Eleventh Circuit held unenforceable the FTC's order because the agency's complaint lacked sufficient specificity. The Court observed that the FTC's Rule of Practice requires commission complaints to contain "[a] clear and concise factual statement sufficient to inform each respondent with reasonable definiteness of the type of acts or practices alleged to be in violation of the law." From there, the Court reasoned that any remedy a complaint seeks "must comport with this requirement of reasonable definiteness."

In the eyes of the Eleventh Circuit, the FTC's cease and desist order fatally contained "no prohibitions." Rather than instructing LabMD "to stop committing a specific act or practice," it commanded the company to "overhaul and replace its data-security program to meet an indeterminable standard of reasonableness." Put another way, the vagueness in the FTC's complaint—which alleged that LabMD's data security practices were deficient as a whole— translated into vagueness in the remedy sought by the FTC; it was that same vagueness that rendered the FTC order unenforceable.

FTC Enforcement Post-LabMD

The *LabMD* decision inevitably constrains the FTC's authority to impose a broad and comprehensive cybersecurity program on defendants, absent specific measures appropriate under the circumstances. In our view, though, it would be a mistake to interpret the decision as preventing the FTC from regulating cybersecurity and data privacy. The Eleventh Circuit indeed recognized the FTC's authority to do just that. Instead, *LabMD* requires the FTC to issue orders with greater specificity, depending on the facts of the case, and does not call into question the broader issue of whether the FTC can regulate data security at all.

The Eleventh Circuit's holding in *LabMD* must also be considered in light of the Third Circuit's earlier ruling in *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3rd Cir. 2015). There, Wyndham Worldwide's privacy statement promised its customers that the company would protect their data, including credit card information, using "industry standard practices," including encryption, firewalls, and other "commercially reasonable methods." In fact, the company implemented none of these measures. And after an initial security breach, the company apparently failed to appropriately remediate, resulting in two more breaches and the compromise of personal information of hundreds of thousands of consumers. The Third Circuit upheld the FTC's authority to enforce a cybersecurity order against Wyndham Worldwide, holding that the company had engaged in unfair trade practices, "unreasonably and unnecessarily exposing consumers' personal data to unauthorized access and theft."

Wyndham and *LabMD* are not necessarily inconsistent with one another. Rather, read together, the cases show how the individualized circumstances of a security incident informs whether there has been an unfair practice and, thus, the scope of the FTC's regulatory power to impose remedial measures. While *Wyndham* affirmed the FTC's power to regulate data security, and *LabMD* may appear to constrain it, both decisions are driven by the circumstances of each case's individual incident rather than a fundamental schism in the courts' interpretations of the FTC's unfairness authority. Rather than base its ultimate ruling on the FTC's unfairness authority, the Eleventh Circuit in *LabMD* limited its opinion to the enforceability of the FTC's order. Although the Court did not adopt a negligence standard to establish an unfair act or practice for purposes of FTC enforcement, it was willing to entertain it and "assume arguendo that the Commission is correct" that there was an unfair practice in the FTC's allegations. *LabMD*'s specific lesson is that the FTC

may not enforce a comprehensive and, yet, indeterminate security program that far exceeds the scope of the specific facts of the case. The FTC thus could not enforce a comprehensive program against a defunct company on the basis of a single data compromise unknowingly caused by a misbehaving employee. But, particularly when read with *Wyndham Worldwide*, the FTC may yet take appropriate action depending on the specific facts presented by the individual case.

While the FTC may need to draft more tightly drawn orders in the cyber space, it remains one of the few federal agencies providing meaningful cyber enforcement, particularly outside the healthcare and financial services arenas. If the FTC is to maintain a positive posture in the cyber arena (absent congressional action or other fundamental changes), it must strike a balance that specifically addresses the circumstance giving rise to the dispute, while at the same time avoiding orders that pinpoint the problematic behavior so narrowly that they lose value over time, particularly given the ever-changing technology landscape. While it may be more expedient for the FTC to impose wide-ranging, comprehensive, "reasonable" cybersecurity remedies, the Eleventh Circuit's holding in *LabMD* serves notice that should the FTC reach too broadly, such orders are likely a luxury the FTC will no longer be afforded under ordinary circumstances.

There are other avenues that are potentially available to the FTC, even without fundamental congressional action changing its investigative or remedial powers. Indeed, there is broad agreement that the FTC should avoid orders that provide a roadmap to vulnerabilities or adopt technology-specific or other pinpoint remedies that are ill-equipped to deal with evolving risks. As an alternative, the FTC might reference third-party standards, such as the National Institute of Standards and Technology's Cybersecurity Standards or Payment Card Industry Data Security Standard, in an attempt to balance these demands. It might also require a third-party assessment and then consider and approve sufficiently specific remedial measures based on the findings of that assessment. These and other avenues may remain available to the FTC, despite the Eleventh Circuit decision in *LabMD*, which many have mistakenly described as the end of the FTC's presence in cyber-related enforcement actions.

Cybersecurity, and particularly the FTC's regulation of it, continues to be an evolving area with sometimes subtle distinctions requiring discerning judgment. We will continue to update you and look forward to working with you by providing effective and proactive advice to assist you in navigating the changing landscape of court decisions and federal regulations.

---

*Larry Sommerfeld is the former chief of the Appeals & Legal Advice Division of the U.S. Attorney's Office for the Northern District of Georgia.

You can subscribe to future *Privacy & Data Security* advisories and other Alston & Bird publications by completing our **publications subscription form**.

If you have any questions or would like additional information, please contact your Alston & Bird attorney or one of the following:

Members of Alston & Bird's Privacy & Data Security Group

James A. Harvey
404.881.7328
jim.harvey@alston.com

David C. Keating
404.881.7355
202.239.3921
david.keating@alston.com

Kristine McAlister Brown
404.881.7584
kristy.brown@alston.com

Angela T. Burnette
404.881.7665
angie.burnette@alston.com

Lisa H. Cassilly
404.881.7945
212.905.9155
lisa.cassilly@alston.com

Helen Christakos
650.838.2091
helen.christakos@alston.com

Cari K. Dawson
404.881.7766
cari.dawson@alston.com

Jan Dhont
+32 2 550 3709
jan.dhont@alston.com

Derin B. Dickerson
404.881.7454
derin.dickerson@alston.com

Clare H. Draper IV
404.881.7191
clare.draper@alston.com

Christina Hull Eikhoff
404.881.4496
christy.eikhoff@alston.com

Sarah Ernst
404.881.4940
sarah.ernst@alston.com

Peter K. Floyd
404.881.4510
peter.floyd@alston.com

Daniel Gerst
213.576.2528
daniel.gerst@alston.com

Jonathan M. Gordon
213.576.1165
jonathan.gordon@alston.com

Elizabeth Helmer
404.881.4724
elizabeth.helmer@alston.com

John R. Hickman
404.881.7885
john.hickman@alston.com

Donald Houser
404.881.4749
donald.houser@alston.com

Stephanie A. Jones
213.576.1136
stephanie.jones@alston.com

William H. Jordan
404.881.7850
202.756.3494
bill.jordan@alston.com

W. Scott Kitchens
404.881.4955
scott.kitchens@alston.com

John L. Latham
404.881.7915
john.latham@alston.com

Dawnmarie R. Matlock
404.881.4253
dawnmarie.matlock@alston.com

Kimberly Kiefer Peretti
202.239.3720
kimberly.peretti@alston.com

T.C. Spencer Pryor
404.881.7978
spence.pryor@alston.com

Karen M. Sanzaro
202.239.3719
karen.sanzaro@alston.com

Jessica C. Smith
213.576.1062
jessica.smith@alston.com

Peter Swire
240.994.4142
peter.swire@alston.com

Daniel G. Taylor
404.881.7567
dan.taylor@alston.com

Katherine M. Wallace
404.881.4706
katherine.wallace@alston.com

Richard R. Willis
+32.2.550.3700
richard.willis@alston.com

Follow us: On Twitter @AlstonPrivacy
On our blog – www.AlstonPrivacy.com

ALSTON & BIRD

WWW.ALSTON.COM