Bloomberg Law

Privacy and Security Law Report®

FTC Enforcement

Acting Chairman Maureen Ohlhausen takes over at the Federal Trade Commission as the commission is embroiled in litigation challenging its data security enforcement authority, the outcome of which may demand the FTC scale back aggressive enforcement and adopt different administrative procedures in regulating cybersecurity, the authors write.

Litigation

Would an Appeals Court Ruling for LabMD Portend a Sea Change in the FTC's Data Security Enforcement?

BY JUDITH GREENSTONE MILLER AND DANIEL M. UNGAR

On Jan. 25, President Trump designated Maureen Ohlhausen, on the U.S. Federal Trade Commission (FTC) board of commissioners since 2012, as the acting chairman of the agency. Most discussion regarding the role of the FTC concerns anti-trust policy; however, the FTC is also heavily involved in the field of privacy and data protection, an area with which Ohlhausen is intimately familiar, having practiced in the field when she was in private practice. Her appointment comes at a time when the FTC is litigating a case in federal appellate court, *LabMD, Inc. v. FTC*, which has the potential to sharply curtail the FTC's authority in this very field. If the court decides the appeal in the petitioner's favor, as a recent order in the case suggests is likely, the decision may impact Ohlhausen's ability to continue business as usual at the FTC.

Judith Greenstone Miller is a partner at Jaffe Raitt Heuer & Weiss PC in Southfield, Mich. where she is a member of the Privacy and Data Security Practice Group.

Daniel Ungar is an associate at Jaffe Raitt Heuer & Weiss PC in Southfield, Mich., where he is a member of the Privacy and Data Security Practice Group.

The relevant procedural history of the *LabMD* case began in July 2016, when the FTC issued an opinion and final order in its long-running case against LabMD, Inc., finding that LabMD failed to maintain adequate data security practices. Opinion of the Commission, FTC Docket No. 9357 (F.T.C. July 29, 2016); *Final Order,* FTC Docket No. 9357 (F.T.C. July 29, 2016). The FTC ordered the company, among other things, to (i) overhaul its data security program, (ii) engage independent auditors to assess the efficacy of its new program and (iii) make records available to the FTC for up to five (5) years. *Id.* LabMD appealed the order to the U.S. Court of Appeals for the Eleventh Circuit and, as part of the appeal, sought a stay on enforcement of the order. On Nov. 10, 2016, LabMD received a temporary reprieve when the Eleventh Circuit granted LabMD's motion to stay the implementation of the FTC's order, pending final resolution of the appeal. Order Granting LabMD's ''Time Sensitive Motion to Stay Enforcement of the Commission's Final Order Pending Appeal, and for a Temporary Stay While the Court Considers the

 ISSN 1538-3423

Motion,'' *LabMD, Inc. v. FTC*, No. 16-16270-D, Slip Op. (11th Cir. Nov. 10, 2016).

Normally, a ruling on the issuance of a temporary stay would not be particularly newsworthy. However, in this case, the court used unusually strong language to question whether the FTC's interpretation of its authorizing statute—and thus the extent of its enforcement powers—was reasonable. *See id.* at 8 (''there are compelling reasons why the FTC's interpretation may not be reasonable.''). In granting the stay, the court appeared to be signaling that it believes there is a good chance LabMD will ultimately prevail on the merits. Therefore, if this order is any indication on how the merits of the case will be decided, it could mean a reversal of the FTC's decades-long campaign to be the nation's data security law enforcement agency, having unfettered discretion and little oversight.

FTC Enforcement Authority

Since the 1990s, the FTC has viewed itself as the federal agency tasked with enforcing digital privacy and data security issues. In contrast to Europe, the U.S. does not have a specific federal statute governing protection of data (although some states may have their own laws). Moreover, the FTC has not promulgated administrative regulations or standards through the traditional rulemaking process to address data security. Instead, the FTC has primarily relied on its general enforcement powers under the Federal Trade Commission Act, 15 U.S.C. § 45 (FTC Act), and the consent agreements that result from the agency's civil actions against individual companies, to shape industry norms. Under § 45(a) of the FTC Act, the FTC has authority to prevent businesses from engaging in ''unfair and deceptive acts or practices in or affecting commerce.'' 15 U.S.C. § 45(a).

The FTC takes the position that lax security measures that have the potential to endanger consumers' data or privacy constitute ''unfair acts or practices'' and thus fall under the FTC's purview. Accordingly, when the FTC initiates an enforcement action against a company for its cybersecurity practices, § 45(a) is what the accused company is charged with violating. In a subset of these cases, particularly where the FTC accuses an internet business of not complying with its own privacy policy, the action may allege a violation of the ''deceptive acts'' clause in addition to ''unfair acts.'' However, the FTC also maintains that deficient security alone satisfies the ''unfair'' prong, even without any representations being made to the public.

Acting Federal Trade Commission Chairwoman Maureen Ohlhausen is intimately familiar with the field of privacy and data protection, having practiced in the field when she was in private practice.

Over the past 15 years, the FTC has filed dozens of enforcement actions against businesses, both large and small. Virtually all have settled out of court, with the accused acquiescing to a consent decree. Only two holdouts have challenged the FTC in federal court: Wyndham Worldwide Corp. (Wyndham) and LabMD. In 2015, the FTC secured a significant victory against Wyndham, when the U.S. Court of Appeals for the Third Circuit affirmed that the FTC's statutory role in restraining ''unfair acts and practices'' does indeed invest the FTC with authority to regulate corporate cybersecurity. *FTC v. Wyndham Worldwide, Inc.*, 799 F.3d 236, 243 (3rd Cir. 2015). This new *LabMD* ruling, on the other hand, may represent a significant setback for the FTC—which may be good news for businesses under its jurisdiction.

The *Wyndham* Decision.

Briefly, the *Wyndham* case involved a hotel chain that was victim to three separate data breaches in which customer data was stolen. In 2012, the FTC sued Wyndham for unfair and deceptive business practices under § 45(a) for its failure to use readily available computer security measures. On appeal from the district court's denial of Wyndham's motion to dismiss the unfair practices claim, Wyndham argued that, because the FTC did not issue official rules, there was no guidance as to what specific practices could be considered ''unfair.'' The U.S. Court of Appeals for the Third Circuit rejected this argument, concluding that past complaints brought against other companies, and guidelines issued by the agency from time to time, gave Wyndham ''fair notice its specific cybersecurity practices could fall short'' of the statute. *Id.* at 240. Wyndham settled with the FTC soon after the Third Circuit's ruling.

The *Wyndham* decision was considered a big win for the agency, as it was the first time a higher court opined on the validity of the FTC's underlying mission regarding cybersecurity. However, the decision was not quite a total victory for the FTC. Notably, the court of appeals declined to decide, as urged by the FTC, that the FTC's enforcement practices constituted adequate notice to the public as to the FTC's interpretation of the statute. The court explained that it rejected Wyndham's argument not because it had run afoul of *the FTC's* interpretation of the unfairness clause, but because Wyndham had fair notice that ''a *court* could construe its conduct as falling within the meaning of the statute.'' *Id.* at 256 (emphasis added). However, the court agreed with Wyndham that the FTC's consent orders—as well as the agency's informal publications such as a data security guidebook—''were of little use to it in trying to understand the specific requirements imposed by § 45(a).'' *Id.* at 257, fn. 22. The court left the question open as to how much deference to give to the FTC's interpretation as to what specific security practices should be deemed unfair, and how the FTC may satisfy its notice requirements regarding such interpretations. *Id.* at 255 (''If later proceedings in this case develop such that the proper resolution is to defer to an agency interpretation that gives rise to Wyndham's liability, we leave to that time a fuller exploration of the level of notice required.''). As the case settled before any judicial resolution of this issue, the appropriateness of the FTC's attempts to create an entire body of data security regulation through individual enforcement actions remained unresolved.

  PVLR ISSN 1538-3423

The *LabMD* Decision.

Now, with this most recent *LabMD* decision from the Eleventh Circuit, it appears clearer that the FTC's authority to interpret the statute and determine what practices are ''unfair'' is not, and will not be determined to be, limitless. In its order granting LabMD a stay, the Eleventh Circuit analyzed whether LabMD's actions could reasonably be construed as ''unfair'' under the statute. The court concluded that LabMD had put forward compelling reasons why the FTC's interpretation may not be reasonable and had made a strong showing that it is likely to succeed on the merits. *LabMD v. FTC*, No. 16-16270-D, Slip Op. at 8.

The facts of the case are as follows: In 2005, an employee of LabMD, a clinical laboratory, accidentally shared a document containing confidential patient information (including social security numbers and medical and insurance information) while using LimeWire LLC, the peer-to-peer file-sharing service (which itself was shut down by a federal court in 2010 due to piracy violations). This file was found by a security firm called Tiversa Inc. that monitored peer-to-peer services specifically to find security breaches such as this in order to sell its security services to (some might say ''shake down'') the victim. When LabMD refused to hire Tiversa, Tiversa threatened to report the company to the FTC, and in 2009, after LabMD continued to rebuff Tiversa, it finally made good on its threat. Thereafter, in 2010, the FTC launched an investigation into LabMD's security practices and ultimately filed its complaint against the company in 2013. *Id.* at 1–3.

LabMD ceased operations in early 2014, in large part due to the expense of fighting the FTC's charges. Since that time, it has been almost completely defunct except in a very limited capacity in which it responds to occasional requests for patient data which it is required to keep by law and which exist solely on an unplugged computer. As the court explained in its order, ''[w]hen LabMD is called upon to send a copy of a record to a former client, it plugs in the computer (without connecting to the internet), prints a hard copy, unplugs the computer and mails or faxes that hard copy to the client.'' *Id.* at 12.

In 2015, an administrative law judge (ALJ) dismissed the FTC's complaint against LabMD on the grounds that the FTC had failed to prove that any substantial consumer injury had occurred or would likely occur in the future, given that there was no evidence that anyone other than Tiversa had downloaded the file. *Initial Decision of the ALJ*, FTC Docket No. 9357 (F.T.C. Nov. 13, 2015). Section 45(n) of the FTC Act expressly provides that the FTC has no authority to deem an action or practice unfair unless it ''causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition'' 15 U.S.C. § 45(n).

FTC Acting Chairman Maureen Ohlhausen has advocated for a light touch in crafting government regulation and has frequently spoken of the need for ''regulatory humility.''

The ALJ's decision was rejected and reversed by the FTC in July 2016. The Commission concluded that the privacy harm resulting from the unauthorized disclosure of sensitive health information is ''in and of itself a substantial injury.'' *Opinion of the Commission*, FTC Docket No. 9357 (F.T.C. July 29, 2016). The FTC also held that a determination of the likelihood of whether an injury will take place must take into account the magnitude or seriousness of the injury if it does occur. Thus, reasoned the agency, ''a practice may be unfair if the magnitude of the potential injury is large, even if the likelihood of the injury occurring is low.'' *Id.* Therefore, the FTC concluded that the disclosure of the sensitive personal information itself caused ''additional harms that are neither economic nor physical in nature but are nonetheless real and substantial and thus cognizable'' under the law. *Id.*

LabMD appealed the Commission's order to the Eleventh Circuit and, as part of the appeal, sought a stay on enforcement of the commission's decision. In granting the stay and thereby finding that LabMD demonstrated a likelihood of success on the merits, the court identified several ''compelling'' reasons why the FTC's interpretation of the FTC Act may not be reasonable. *LabMD v. FTC*, No. 16-16270-D, Slip Op. at 8.

First, the court questioned whether ''a reasonable interpretation of § 45(n) includes intangible harms like those that the FTC found in this case.'' *Id.* The court noted that § 45(n) was modeled after the FTC's own 1980 Policy Statement on Unfairness, which provided that the FTC ''is not concerned with . . . merely speculative harms,'' and that ''[e]motional impact and other more subjective types of harm . . . will not ordinarily make a practice unfair.'' *Id.* (quoting FTC, *Policy Statement on Unfairness* (Dec. 17, 1980) as well as a Senate report on the legislative history of the statute, which was consistent with the Policy Statement and relied on by the FTC, S. Rep. No. 103-130, (1993)). Further, the court favorably acknowledged LabMD's argument that the injury at issue was ''not even intangible, as a true data breach of personal information to the public might be, but rather is purely conceptual because this harm is only speculative.'' *Id*. (internal quotation marks omitted).

Second, the court interpreted the ''likely to cause'' language contained in § 45(n) ''to require a higher threshold than that set by the FTC.'' *Id.* The court did not find the FTC's ''significant risk'' test, in which a large potential injury can counterbalance the low likelihood of that injury occurring, to be a reasonable reading of ''likely to cause.'' Rather, concluded the court, § 45(n) necessarily excludes any event that has a low likelihood of occurring, even if the magnitude of the potential injury is large, and any interpretation of the statute that includes low-probability events is inherently unreasonable. *Id.*.

Finally, the court found that the costs of LabMD complying with the enforcement order (estimated by LabMD to exceed $250,000) would cause LabMD irreparable harm in light of its financial condition and given that it was no longer an operational business (with less than $5,000 cash on hand, it could not even afford legal representation and was forced to rely on pro bono services for prosecuting the appeal). *Id.*. Thus, the court found clear grounds to stay the FTC's order to undertake expensive remedial and preventative actions.

New Face of the FTC

Though this new opinion from the Eleventh Circuit is not a final decision on the merits, nevertheless, the court's strong skepticism about the reasonableness of the FTC's statutory interpretations suggests that when the Eleventh Circuit addresses the merits of the case, it may overrule the decision of the FTC and thereby prompt a major change to the FTC's entire approach to policing corporate cybersecurity. The FTC's current policy is specifically designed to police and punish businesses with deficient security practices *prior* to any actual harm being imposed on consumers. As the FTC's July opinion pointed out, the law was drafted with a ''prophylactic purpose.''

The FTC also has asserted that courts have agreed that preemptive action is necessary and that ''[w]e need not wait for consumers to suffer known harm at the hands of identity thieves.'' Nonetheless, industry advocates have long argued that the FTC's primary focus on enforcement actions and settlements as a vehicle to establish cybersecurity standards, rather than through notice-and-comment procedures generally undertaken and required for administrative rulemaking, represents an abuse of the FTC's enforcement authority under the FTC Act. *See, e.g.*, Gus Hurwitz, *LabMD Ruling Should be a Wake-Up Call for FTC Data Security Enforcement*, TechPolicyDaily.com (Nov. 23, 2015). The Eleventh Circuit's recent opinion appears consistent with this view. The question is, does it comport with the FTC's incoming acting acting chairman's goals for the agency?

Incoming FTC Acting Chairman Maureen Ohlhausen has advocated for a light touch in crafting government regulation and has frequently spoken of the need for ''regulatory humility.'' *See, e.g.*, Remarks by FTC Commissioner Maureen K. Ohlhausen at The Heritage Foundation, *Antitrust Policy for a New Administration*, Jan. 24, 2017 ; Remarks by FTC Commissioner Maureen K. Ohlhausen at American Enterprise Institute (AEI), *Regulatory Humility in Practice*, Apr. 1, 2015. However, this apparent laissez-faire approach to regulation does not necessarily mean that she will applaud a judicial decision against the FTC, as her criticism is of industry-wide standards, not aggressive enforcement, which she actually supports. She has explained that her regulatory philosophy supports the FTC's current common law approach, under which the agency addresses real companies' security practices on a case-by-case basis in light of prevailing industry standards, rather than prescriptive *ex ante* regulation, which she has criticized as one-size-fits-all rules that are not flexible enough to adapt to changes in technology and business models. Remarks at AEI, *Regulatory Humility in Practice*, at 5–6. As she explained further:

That is one of the challenges about saying everyone should have this level of security. It's a very fast changing area. The threats and the precautions are sort of in a race. So it would not be good for companies if the FTC chose some level of security. It would be out of date before the ink was dry. *Id.* at 13.

This approach is consistent with the recommendations of the American Bar Association (ABA). In January 2017, the Antitrust Law Section of the ABA released its *Presidential Transition Report: The State of Antitrust Enforcement*, in which the ABA suggested that the FTC should ''focus their limited enforcement resources on cases involving significant consumer harm,'' particularly in light of the effect that such enforcement activities have on small businesses.'' *ABA Presidential Transition Report*, at 27. For example, the ABA recommended that the FTC ''adopt a number of reforms to help it deploy its limited enforcement resources in a manner that enhances the impact of its actions while, at the same time, treating target companies in a way that is fair and proportionate to alleged offenses.'' *Id.*;*see also* Chris Bruce, *CFPB, FTC Enforcement Changes Urged by Bar Association*, Bloomberg BNA Privacy Law Watch (January 25, 2017).

These reforms should ''enhance the transparency and fairness of the enforcement process'' in order to prevent ''unintended damages to companies and the marketplace without corresponding benefits to consumer or competition.'' Although the ABA does not single out the FTC's treatment of LabMD, it is criticizes, as a misuse of enforcement resources, actions by regulatory agencies for ''technical violations of certain statutes against very small companies, in many cases where the challenged practices—and even the companies themselves—had ceased.'' *ABA Presidential Transition Report*, at 27.

In Ohlhausen's AEI speech, she argued that the FTC's ''nimble, transparent, and incremental'' approach is better for consumers and fairer to business because it ensures that the FTC focuses on specific practices that are actually harming or likely to harm consumers. Because of this, ''the FTC has generally limited forays into speculative harms, thereby preserving its resources for clear violations.'' Remarks at AEI, *Regulatory Humility in Practice*, at 6. However, the Eleventh Circuit's order in *LabMD* challenges the FTC on this very issue, finding that the FTC's enforcement is based on harm that is overly speculative. If the court ends up finding for LabMD on the merits of the appeal, and the court requires the agency to conform to the practices of other administrative agencies with prescriptive rulemaking, Ohlhausen's preferred approach for the FTC could be in jeopardy.

On the other hand, even if the court agrees with LabMD that the harm to consumers was not concrete enough, the decision may be limited to the particular facts of the case, and the overall approach of case-by-case enforcement may be preserved, so long as the FTC does a better job of identifying data breaches that pose a more immediate and substantial harm to consumers. We are sure that the new FTC chief will be watching this case closely to see whether the FTC will be forced to scale back its current aggressive enforcement campaign and adopt different administrative procedures in regulating cybersecurity.

  PVLR ISSN 1538-3423