FTC Exceeded Its Authority In Zoom Cybersecurity Settlement

By **Doug Meal, Michelle Visser and David Cohen** (November 17, 2020)

Doug Meal

Michelle Visser

David Cohen

The Federal Trade Commission's cybersecurity settlement last week with videoconferencing platform Zoom Video Communications Inc. reflects a concerning practice that has persisted for over two decades: In its zeal to address the problem of cybercrime, the agency regularly oversteps its authority in this arena.

Businesses need to be aware of how the FTC is overreaching and think carefully before accepting a settlement based on claims and remedies that exceed the agency's powers.

Many simply assume that, because virtually all businesses have agreed to settlements when faced with FTC cybersecurity enforcement, the agency must be acting within its rights. But this is not so, as illustrated by a key recent FTC cybersecurity enforcement defeat.

When medical laboratory LabMD Inc. decided several years ago to challenge in court the FTC's authority to order an overhaul of its cybersecurity practices, many were likewise highly skeptical of LabMD's chances. Presumably, many said, if there were no legal basis for the FTC's action, then the scores of other companies that had settled similar actions by the agency would not have done so.

But the U.S. Court of Appeals for the Eleventh Circuit blew that contention sky high when, in a series of three decisions, it not only overturned the FTC's order against LabMD for being unenforceably vague,[1] but — in two other decisions that have received less attention — also held that the FTC's action against LabMD was premised on unreasonably broad interpretations of the agency's statutory authority and ordered the FTC to pay LabMD $843,173.67 in attorney fees and expenses because the FTC's prior litigation positions were not substantially justified.[2]

As to the many previous FTC settlements with other companies, the court observed, "it is reasonable to assume that the private parties to these consent orders signed them to avoid the type of long and protracted legal battle that played out here."[3]

Since LabMD, the FTC has continued to strong-arm American businesses into settling ultra vires cybersecurity enforcement actions by threatening costly litigation. So it is once again critical to underscore that, merely because the FTC has brought actions of a particular type and companies have agreed to settle them, this does not mean that the actions have any basis in the law.

The FTC's cybersecurity settlement with Zoom is the latest illustration of this point. As in many prior FTC cybersecurity actions, the gravamen of the FTC's complaint was that Zoom deceived consumers about its cybersecurity practices. The proper remedy for that claim, assuming for argument's sake that the company did in fact commit deception, is a prohibition on further deception of the sort alleged.

But as it frequently does, the FTC did not merely prohibit Zoom from committing further

deception: It also imposed a sweeping substantive requirement that Zoom overhaul its cybersecurity practices, regardless of whether Zoom is deceiving consumers about those practices. This wide-ranging affirmative relief extends far beyond the bounds of the authority Congress gave the FTC, namely, to order that companies cease and desist from illegal conduct.

While the FTC's concern about cybersecurity is understandable, the fact remains that the FTC is a creature of statute and thus limited to the powers Congress has granted. If the FTC wants more authority, it should continue to ask Congress for it, rather than simply claiming it. And companies faced with legally unfounded FTC claims of authority should keep in mind that agreeing to unwarranted relief may not be their best option.

The FTC's Settlement With Zoom

The FTC's complaint against Zoom, like most FTC cybersecurity complaints, alleges that Zoom violated Section 5 of the FTC Act, which prohibits unfair or deceptive trade practices.

First, the FTC alleged that Zoom committed a deceptive trade practice by misrepresenting the extent to which it encrypted video conferences. Specifically, Zoom purportedly represented to consumers that the encryption was end-to-end when it was not, that it used AES 256-bit encryption when its encryption solution was actually a weaker AES 128-bit encryption, and that recorded conferences were encrypted immediately after a meeting ended when in fact they were encrypted only after being stored unencrypted for 60 days.

Second, the FTC alleged that Zoom committed deceptive and unfair practices with respect to its Zoom application for Apple Inc.'s Mac computers. Specifically, the FTC claimed that, as part of a manual update for the Zoom app, Zoom secretly installed software on Mac computers that introduced security vulnerabilities onto the devices. Among other vulnerabilities, the FTC claimed that the software bypassed an Apple Safari browser safeguard that provided users with a warning box, prior to launching the Zoom app, that asked users if they wanted to launch the app.

The FTC alleged that deploying the software without adequate notice or consent was an unfair practice and that the company's release notes for the update were deceptive because they did not adequately disclose that the update would install the software in question, that it would introduce the security vulnerabilities, or that it would remain on users' computers even after users deleted the Zoom app. Notably, the FTC did not allege that any malicious actor ever exploited any of the security vulnerabilities.

The proposed consent order, if accepted by the commission after a public comment period, would prohibit Zoom from misrepresenting its security and privacy practices. But it also goes further. Consistent with the FTC's typical approach to data security consent orders, it would require Zoom to establish, implement and maintain a comprehensive information security program that protects the security, confidentiality and integrity of a wide range of personal information.

The order then specifies four pages of requirements that Zoom must, at a minimum comply with in order for the program to satisfy the overall comprehensiveness requirement. The FTC's use of "at a minimum" leaves it with room to argue that the order's four pages of requirements, while being necessary, are not necessarily by themselves sufficient, to satisfy the general obligation to implement an information security program that is comprehensive.

The commission voted 3-2 to accept the settlement with Zoom. FTC Commissioner Rebecca

Kelly Slaughter issued a dissenting statement arguing that the consent order should also have required Zoom to improve its privacy practices, not merely its security practices, as well as provide recourse for Zoom's paying customers. Commissioner Rohit Chopra also issued a dissenting statement that likewise argued for consumer recourse and discussed various ways in which he believes the FTC's enforcement in the privacy and cybersecurity space is ineffective.

Chairman Joseph Simons, along with Commissioners Noah Joshua Phillips and Christine Wilson, issued a majority statement arguing that the settlement relief is effective to address the legal violations alleged, that the additional relief sought by Slaughter and Chopra likely would not be approved in court, and, in any event, that seeking that additional relief would delay the imposition of the injunctive relief contained in the order.

"Our goal," said the three commissioners, "is a safe and secure Zoom that can continue to provide essential services to enable Americans to conduct business, engage in learning, participate in religious services, and stay connected."

Overstepping its Authority

Slaughter and Chopra were correct that the Zoom settlement is problematic, but the reason it is problematic is that it went too far in imposing relief on Zoom, not that it failed to go far enough. Among other things, there is no statutory basis for the order's sweeping requirement that Zoom implement a comprehensive information security program.

Affirmative relief is an improper remedy for deceptive statements.

While we appreciate the majority commissioners' desire for a safe and secure Zoom, the fact is that Congress has never actually given the FTC authority to order American businesses to have safe and secure data security.

Except in narrow segments of the economy as to which Congress has passed specific data security legislation, the FTC's authority is limited to preventing unfair or deceptive trade practices under Section 5 of the FTC Act.[4]

And even when a business commits such a practice, Section 5 permits the FTC only to enter an order requiring the alleged law violator to cease and desist from the violation of the law.[5]

The FTC is permitted to include ancillary affirmative relief only when some affirmative action must necessarily be taken in order for the company to cease and desist from the allegedly unlawful practice, for instance, requiring patent licensing to remedy monopolistic behavior.[6]

Accordingly, a legally proper order to cease and desist from misrepresenting privacy or data security measures, as Zoom allegedly did, would merely require the company to cease the alleged misrepresentations — not to affirmatively change its privacy or data security practices — because refraining from the misrepresentations would terminate the allegedly unlawful conduct.

Former Commissioner Orson Swindle expressed this view in an early deception-based data security case when dissenting from the commission's imposition of information security requirements analogous to the relief imposed on Zoom:

The privacy requirements [imposed by the order] also are intended to some extent to remedy the false claim concerning the defendants' security technology that is challenged by Count II of the proposed complaint, but the prohibition on misrepresentations concerning the defendants' "services or facilities" in Part I.B.2 is sufficient by itself to protect consumers. Indeed, when a defendant makes the false claim that its product is efficacious, the usual remedy is to prohibit the defendant from making the same or similar false efficacy claims, not to mandate that the defendant make its product "reasonably efficacious." See Part IV.A. (requiring that the defendants establish and maintain "reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from consumers").[7]

Here, as in many prior FTC cybersecurity actions, the gravamen of the FTC's complaint was that Zoom deceived consumers about its cybersecurity practices. The only proper remedy for that claim, assuming for argument's sake that the company did in fact commit deception, is a prohibition on further deception of the sort alleged.

The unfairness claim also does not justify affirmative cybersecurity relief.

The FTC's allegation that the manual update for the Zoom app for Mac computers was unfair also does nothing to justify the order's sweeping requirement to institute a comprehensive security program. That claim also hinged on the deceptive nature of the conduct at issue: The FTC alleged that the update was unfair because Zoom installed the software at issue without adequate notice or consent.

Thus, here again, Zoom could have ceased the allegedly unlawful conduct by merely enhancing its communications with consumers. Moreover, this unfairness claim related to only one narrow aspect of Zoom's services, hardly justifying a sweeping overhaul of Zoom's overall security program.

In any event, the unfairness allegation does not satisfy the basic requirements of an unfairness claim under Section 5 of the FTC Act. Section 5(n) of the act provides that "the Commission shall have no authority under this section … to declare" an act or practice unfair, unless, among other things, "the act or practice causes or is likely to cause substantial injury to consumers."

Here, the FTC claimed that Zoom's installation of software on Mac computers without notice or consent "harmed consumers by limiting the intended benefit of a privacy and security safeguard provided by their Safari browser" as well as by introducing additional security vulnerabilities.

But the commission, in its own opinion in the LabMD matter, already disclaimed the idea that conduct creating merely a risk of harm to consumers — as a mere vulnerability on a computer does — is tantamount to causing actual consumer injury within the meaning of Section 5.

Rather, if a malicious actor has not yet exploited the vulnerability, the conduct creating the vulnerability is not unfair unless harm is likely to result from the vulnerability.[8] The FTC did not argue that any malicious actors had exploited the vulnerabilities purportedly created by Zoom or even that they were likely to do so — it merely alleged that they could.[9] This is not sufficient to allege likely consumer injury.[10]

What is more, intangible injuries such as privacy harms of the sort cited by the FTC's complaint, without some tangible injury like financial loss, are not "substantial" within the

meaning of Section 5(n). Indeed, in LabMD the Eleventh Circuit rejected the FTC's contention that purported privacy harms inherent in the disclosure of sensitive information are substantial.[11]

And in FTC v. Wyndham Worldwide Corp., although the U.S. Court of Appeals for the Third Circuit rejected arguments that the FTC has no authority whatsoever to police cybersecurity using its unfairness power, it clarified that in wielding its authority in a given case, the FTC would need to satisfy the burdensome requirement of proving consumer injury beyond mere inconvenience.[12]

Thus, even assuming arguendo that the FTC has some authority to regulate cybersecurity using its unfairness power, the unfairness claim against Zoom, like the deception claim, could not come close to justifying the sweeping affirmative cybersecurity requirements imposed by the FTC's order.[13]

Prior settlements do not create precedent in the FTC's favor.

As LabMD illustrates, the fact that scores of companies have agreed to similarly sweeping FTC cybersecurity requirements does not show that those requirements are grounded in the law. To the contrary, as the Eleventh Circuit noted:

> The FTC asserts that it was substantially justified in issuing the cease and desist order here because it has used the same language in fifty consent orders without any problems. ... However, the FTC fails to show that those cases were litigated and that a court ruled on the legality of the requirements imposed by the consent orders. Indeed, the title of these orders, i.e., "consent orders," is telling. Entry of such orders, which are submitted jointly by the parties with the request that they be approved, should not have given the FTC confidence that either its legal position or the terms it was imposing on companies were reasonable. Instead, it is reasonable to assume that the private parties to these consent orders signed them to avoid the type of long and protracted legal battle that played out here.[14]

Conclusion

The FTC's concern about cybersecurity in an age of prevalent cyberattacks is understandable. But the fact remains that the FTC is a creature of statute and thus limited to the powers Congress has granted. As the U.S. Supreme Court has explained, "an agency literally has no power to act … unless and until Congress confers power upon it."[15] If the FTC wants more authority, it should continue to ask Congress for it, rather than simply claim it.

In the meantime, companies facing FTC cybersecurity enforcement should not necessarily assume that agreeing to unfounded relief is always in their best interest, even though challenging the FTC could result in costly litigation.

Rather, whether to settle involves a delicate calculation of risks and benefits. In that regard, it is worth noting that the two other companies besides LabMD who have chosen to litigate FTC cybersecurity actions — Wyndham and D-Link Systems Inc. — ultimately achieved settlements with affirmative relief that was significantly narrower than the affirmative relief typically included in FTC cybersecurity consent orders, including the relief obtained against Zoom.

And this makes sense: A company that demonstrates a willingness to assert the limits on

the FTC's authority in court puts the FTC on notice that it may well lose at trial, making the agency more willing to settle on better terms. And, as in LabMD, the company may well be able to topple the agency's action altogether.

If the FTC persists in exceeding its statutory authority as it did in the claims it made against Zoom and in the relief it sought from Zoom, it is only a matter of time before another company decides to put the FTC's claimed authority to the test and wins.

Doug Meal and Michelle Visser are partners, and David Cohen is of counsel, at Orrick Herrington & Sutcliffe LLP.

Orrick associate Chad Smith contributed to this article.

Disclosure: Doug Meal, Michelle Visser and David Cohen represented LabMD in LabMD v. FTC at the Eleventh Circuit. Meal and Cohen also represented Wyndham in FTC v. Wyndham.

[1] See LabMD, Inc. v. FTC, 894 F.3d 1221, 1237 (11th Cir. 2018).

[2] See LabMD, Inc. v. FTC, No. 16-16270-QQ (11th Cir. Dec. 23, 2019) ("adopting" special master's report and recommendation found at No. 1:19-mi-00071-WEJ (N.D. Ga. Oct. 1, 2019) and granting LabMD's application for attorney fees and expenses in the amounts recommended by the special master's report and recommendation); see also LabMD v. FTC, 678 F. App'x 816 (11th Cir. 2016) (granting stay of FTC order).

[3] No. 1:19-mi-00071-WEJ (N.D. Ga. Oct. 1, 2019), at 25, adopted by No. 16-16270-QQ (11th Cir. Dec. 23, 2019).

[4] 15 U.S.C. § 45(a).

[5] Id. § 45(b).

[6] See, e.g., Congoleum Indus., Inc. v. C.P.S.C., 602 F.2d 220, 225-26 (9th Cir. 1979) (discussing FTC authority).

[7] Statement of Comm'r Orson Swindle, In re Int'l Outsourcing Grp., No. 992-3245 n.1 (July 12, 2000), http://www.ftc.gov/os/2000/07/iogswin.htm.

[8] See In re LabMD, No. 9357, at 21 n.65 (F.T.C. July 2016) ("Complaint Counsel also argues that an act or practice that creates a 'significant risk of concrete harm' thereby causes a substantial injury. We believe the practices in this case [i.e., failing to prevent a computer network vulnerability that exposed personal information to a risk of unauthorized access] creating a significant risk of injury are more properly analyzed under the 'likely to cause' portion of Section 5(n)"), vacated on other grounds by LabMD v. FTC, 891 F.3d 1286 (11th Cir. 2018).

[9] In particular, the complaint alleged that the vulnerabilities "could expose consumers to remote video surveillance by strangers," "allow malicious actor to execute code on the user's computer," or enable a denial of service attack that would "effectively cause the targeted machine to lock up."

[10] See FTC v. D-Link Systems, Inc., 2017 WL 4150873, at *5-6 (N.D. Cal. Sept. 19, 2017) (actual or likely injury not adequately pled where FTC merely alleged consumers were at "risk" because "remote attackers could take simple steps, using widely available tools, to locate and exploit Defendants' devices, which were widely known to be vulnerable"); see also LabMD, 678 F. App'x at 821 (rejecting FTC position that harm can be "likely" under Section 5(n) even if it "has a low likelihood").

[11] See No. 1:19-mi-00071-WEJ, at 24-28 (N.D. Ga. Oct. 1, 2019), adopted by No. 16-16270-QQ (11th Cir. Dec. 23, 2019); see also LabMD v. FTC, 678 F. App'x 816 (11th Cir. 2016) (granting stay of FTC order after agreeing with LabMD that there were "compelling reasons" establishing that the FTC's contention that intangible harm can constitute substantial injury "may not be reasonable").

[12] F.T.C. v. Wyndham Worldwide Corp., 799 F.3d 236, 248 (2015) (distinguishing Section 5 of FTC Act from Gramm-Leach-Bliley Act, which makes "inconvenience" actionable).

[13] The order against Zoom also suffers from the very same infirmities that we discussed in Doug Meal, Michelle Visser, David Cohen and Joe Santiesteban, FTC Data Security Consent Orders Are New but Not Improved, Law360 (Mar. 23, 2020), https://www.law360.com/articles/1255727/ftc-data-security-consent-orders-are-new-but-not-improved. Among other things, the order does not define with sufficient specificity what security measures are required by the order, as LabMD requires. And the order is vulnerable to criticism for prohibiting deception relating to "privacy," not merely security, even though the complaint's allegations related solely to security. Under longstanding precedent, the scope of an FTC order must always have a "reasonable relation to the unlawful practices." FTC v. Nat'l Lead Co., 352 U.S. 419, 428 (1957).

[14] See No. 1:19-mi-00071-WEJ, at 25-26 (N.D. Ga. Oct. 1, 2019), adopted by No. 16-16270-QQ (11th Cir. Dec. 23, 2019).

[15] La. Pub. Svc. Comm'n v. FCC, 476 U.S. 355, 374 (1986).