A POTENTIAL SHIFT IN ENFORCEMENT PRIORITIES FOR THE FTC

by Julie O'Neill, Partner, Privacy + Data Security Group, Morrison & Foerster

During the course of a long-running data security action against a medical testing laboratory, the Federal Trade Commission (FTC) has been steadfast in its position that legally actionable harm to consumers exists even where there is no evidence of actual harm. Although it is probably too late for that particular company, it appears that the FTC's position may be shifting.

The FTC's Unfairness Doctrine

Section 5 of the FTC Act broadly prohibits unfair and deceptive acts and practices. When it comes to privacy and data security, the FTC has typically alleged deception where a company has misrepresented its practices—for example, where a company's privacy policy extols its security measures but the company does not take even the most basic precautions.

The FTC has also challenged security practices on an unfairness theory, alleging that, irrespective of any representation, a company's failure to have reasonable security measures in place is unfair. To establish "unfairness," the FTC must prove that the act or practice (1) causes or is likely to cause substantial injury to consumers that (2) is not reasonably avoidable by them and (3) is not outweighed by countervailing benefits to consumers or competition.

The Ongoing LabMD Matter

The last few years have seen great debate over the first prong of the unfairness test, most notably in connection with the FTC's litigation against LabMD, a clinical testing laboratory. The FTC alleged that the company's security was unreasonable after a LabMD report containing sensitive health and other personal information was made available on a peer-to-peer file-sharing network. There has been no evidence that any of the information was ever misused.

The dispute has resulted in the shuttering of LabMD's business and conflicting decisions. In November 2015, the FTC's Administrative Law Judge (ALJ) ruled in LabMD's favor, finding that FTC staff had failed to establish that consumers had suffered, or were likely to suffer, any injury as a result of the company's allegedly unreasonable data security practices.

The ALJ reasoned that, to rise to the level of substantial injury under the first prong of the unfairness test, the FTC must prove tangible injury and not merely subjective or emotional harm. With no evidence of such injury, the ALJ decided that LabMD was not in violation of Section 5.

The FTC's Commissioners (the "Commission") reversed the ALJ's decision in July 2016. The crux of the ruling was rejection of the ALJ's harm analysis. Specifically, the Commission found that LabMD's conduct was unfair because the company had failed to provide even basic security for sensitive personal information, and that failure caused, or was likely to cause, substantial consumer injury.

According to the Commission, the disclosure of sensitive personal information *caused substantial injury* because, due to the types of harms that could result (e.g., embarrassment, reputational harm), the disclosure itself was inherently harmful. Similarly, the Commission supported its finding that the disclosure of sensitive personal information was *likely to cause substantial injury* with the argument that "significant risk" of harm meets the "likely to cause" standard. (It disagreed with the ALJ's conclusion that "likely to cause" means "probable.")

In its view, because the magnitude of the potential injury was large, LabMD's data security practices were unfair. The fact that there was no evidence eight years on that anyone had suffered embarrassment or reputational or other harm was not relevant.

LabMD appealed the Commission's decision to the U.S. Court of Appeals for the Eleventh Circuit, and oral arguments took place last month. If the Court agrees with the Commission, the FTC will not have to prove actual consumer injury in order to bring a data security enforcement action on an unfairness theory. If, on the other hand, the Court sides with LabMD, the FTC will, going forward, have to prove more than just speculative injury.

The Effect of New Leadership

Regardless of the Court's eventual ruling, the FTC may now be less inclined to proceed with an allegation of unfairness where consumers have not, in fact, suffered injury. President Trump appointed Republican Maureen Ohlhausen acting Chairman in January, and the change in leadership has brought a not-unexpected shift in enforcement priorities.

At an event considering the FTC at 100 days into the new administration, Chairman Ohlhausen highlighted her desire to avoid federal overreach and pursue "good government efforts." To those ends, she has instructed FTC staff to focus on where the agency's efforts will do the greatest public good, with "enforcement efforts on those matters that involve substantial harms."

Moreover, Chairman Ohlhausen has set up a task force to help identify such harms. She explained that, in much of the agency's consumer protection work, the harm it seeks to stop is obvious (e.g., where a company sells a bogus product).

In its privacy and data security work, however, the question of harm is more complex. The task force is intended to help address this difficulty by studying the economics of privacy. According to the Chairman:

> *The goal of the task force is to encourage and clarify economic reasoning on issues relating to the privacy and data security marketplace. The task force seeks to better understand the markets for consumer information, incentives for the various parties in that marketplace, and how to quantify costs and benefits of different actions that the FTC or others could take.*

The task force's ultimate work product has not yet been decided. There may be some overlap with the third installment of the FTC's multidisciplinary "PrivacyCon" series, scheduled for February 2018.

The conference will have the same focus as the task force: the economics of privacy and, more particularly, how to quantify the harms that result from companies' failure to secure consumer information and how to balance the costs and benefits of privacy-protective technologies and practices.

While it is premature to speculate as to the task force's ultimate findings, Chairman Ohlhausen's philosophy will, in the meantime, almost certainly influence which privacy and data security matters are pursued.

While FTC watchers do not necessarily believe that enforcement will slow, many are of the opinion that the Commission will be unlikely to proceed on an unfairness theory against a practice that does not result in actual (not speculative) harm to consumers.

About The Author

Julie O'Neill is a partner in the Privacy + Data Security Group at global law firm Morrison & Foerster, where she advises on cutting-edge issues at the intersection of privacy and consumer protection laws.

She provides clients with practical solutions to compliance challenges around a wide variety of privacy issues, including online and offline tracking, interest-based advertising, geo-targeting and other mobile tracking, personalization, and cross-device tracking.

She also creates compliance programs for a wide variety of channels, including email, telephone, text message, and fax. As a former FTC staff attorney, Ms. O'Neill regularly defends companies in investigations by the FTC and before data protection authorities around the world. She has been recognized as a "Next Generation Lawyer" by *Legal 500 US* 2017 in the area of Cyber Law, including data protection and privacy.

She can be reached online at joneill@mofo.com and at www.mofo.com.