Insight

Why the LabMD Case Matters for the Regulation of Privacy

WILL RINEHART, TYLER CRAGG | NOVEMBER 16, 2016

The Federal Trade Commission (FTC) acts as the regulatory watchdog for privacy. However, a recent case highlights how the agency has seemingly overextended its reach. As the case with LabMD shows, the FTC has set up a confusing legal standard that provides little guidance for consumer data security and establishes a very low threshold for enforcement. This set up only increases the chances that any company who stores customer information will be found in violation of the FTC Act.

What happened at LabMD?

LabMD was a medical testing lab that collected personal information from patients, such as social security numbers, insurance information, and test results. In 2013, a document containing LabMD patient records was discovered on the peer-to-peer network LimeWire. An employee of LabMD installed the file sharing program on her work computer, unbeknownst to her superiors, causing the document to be available for download. The security consulting firm Tiversa discovered the document and offered its consulting services to LabMD. LabMD chose not to hire Tiversa. Tiversa then reported the company the Federal Trade Commission (FTC). The FTC sued LabMD for maintaining unreasonable security practices, claiming that the sensitive information contained in the document was available to the public over the peer-to-peer network.

What is the legal history between LabMD and the FTC? What kind of suit did the FTC bring against LabMD?

Section 5 of the FTC Act prohibits unfair practices or acts. An unfair practice is one that causes or is likely to cause substantial injury and cannot be avoided by the consumer. The FTC sued LabMD over Section 5 violations because patients' personal records were released, including their social security numbers, over the peer-to-peer network. The FTC argued that the release of this information injured the patients and the practice was unfair because each patient could do nothing to prevent the release of this information. While LabMD countered that the FTC failed to prove an injury actually occurred, the FTC contended that an injury can be considered to take place if there is the *possibility* of an injury.

The Administrative Law Judge sided with the attorneys for LabMD, reasoning that an unspecified risk of harm to the consumer is not a sufficient threshold for agency enforcement actions. Under the FTC's interpretation, because the possibility of injury to the consumer is sufficient, and an injury can be a leak of the information, any company that stores information in a digital format could be in violation of Section 5 of the FTC Act. The FTC said their previous enforcement actions would serve as a guide to when a company's practices violated Section 5 of the FTC Act, however the Judge disagreed that it had provided the necessary due process.

The LabMD case was dismissed last November and in July the FTC rejected the findings of the Administrative Law Judge and continued with enforcement against LabMD. According to the agency, the Judge applied the wrong legal standard. The Judge concluded that a violation of Section 5 requires a real, cognizable harm such as

economic harm or health and safety risks.

Why does it matter to privacy more broadly?

The LabMD case calls into question the FTC's interpretation of Section 5, an underlying statute in privacy protection. While the case doesn't eviscerate the FTC's authority, it suggests that limitations might exist and that the FTC might be reaching too far. Under the agency's reading of the statute, the mere possibility of a data release as well as the possibility that a consumer suffers subjective harm is enough to allow enforcement.

Because the FTC required only a showing that a breach could possibly occur and that breach could possibly result in harm, the threshold for enforcement is concerningly low. A breach is always possible. No system is entirely secure. Although networks can never be completely secure, the risk of a breach can be so remote that consumers do not need to worry about the occurrence of this event.

The FTC's reading of Section 5 sets the standard, and under the current interpretation, every company that stores data electronically is subject to enforcement actions by the FTC. Coupled with the fact there is no other standard for when the FTC will pursue enforcement, only the whims of the FTC Commissioners decide when a company will be investigated. So, it seems as though companies can do nothing to ensure their security practices are sufficient. In a world of incentives, we should be wary of lose-lose situations.