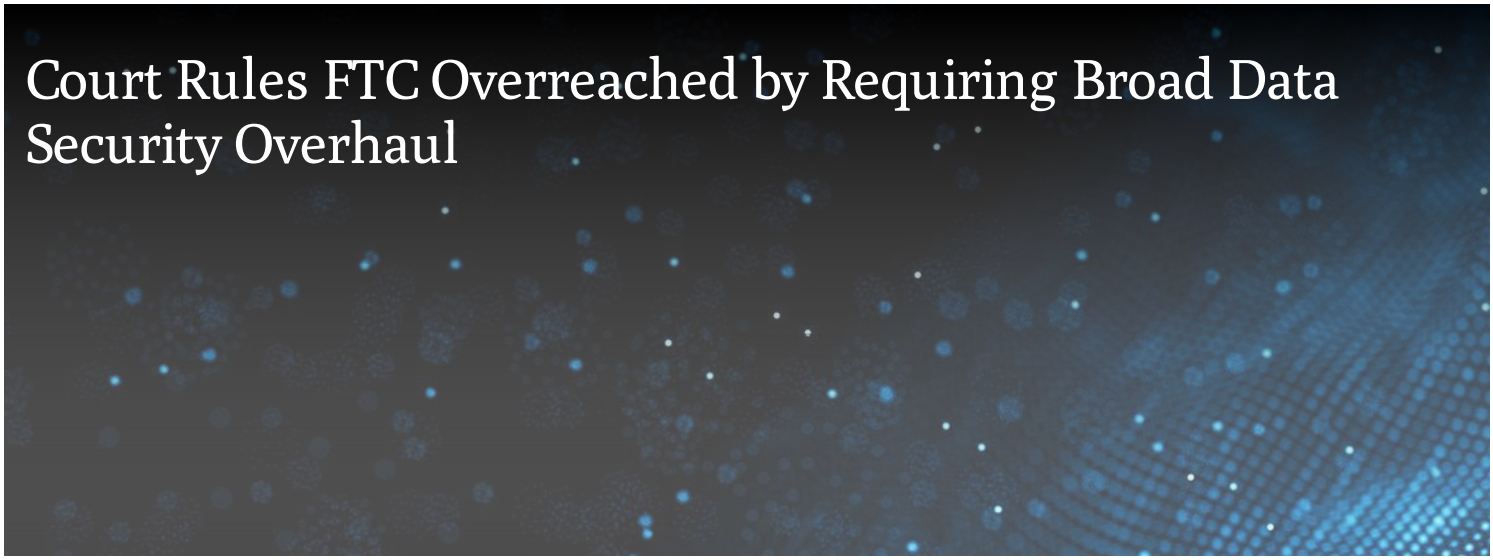
WINSTON & STRAWN LLP

BLOG

Court Rules FTC Overreached by Requiring Broad Data Security Overhaul



JULY 11, 2018

The Eleventh Circuit's ruling in *LabMD v. FTC* vacated a cease and desist order from the Federal Trade Commission (FTC) because it lacked specificity regarding the data security standards the FTC was enforcing.

Sometime in 2005, file-sharing software was installed on a LabMD office computer, contrary to company policy. The employee using the computer designated the computer's "My Documents" folder for sharing, exposing its contents to all other users on the peer-to-peer network. Between July 2007 and May 2008, a file containing over 9000 patients' sensitive information was available on the network. The file was downloaded and then at some point later accessed by a data security company who brought it to the attention of LabMD. LabMD then deleted the software from the office computer. After LabMD refused to hire the data security company, the company alerted the FTC.

After an investigation, the FTC found LabMD's data security procedures and the breach of sensitive patient data constituted an "unfair act or practice" under Section 5(a) of the FTC Act, eventually filing an administrative complaint alleging as such. The complaint was originally dismissed by an administrative law judge but reinstated on appeal back to the FTC. The FTC then issued a cease and desist order which required LabMD to overhaul its entire data security program, invoking a standard of reasonable protection of consumer data. LabMD appealed to the Eleventh Circuit arguing the order was unenforceable because it did not direct LabMD to cease an unfair act or practice.

The Eleventh Circuit agreed with LabMD and vacated the order. The court found that a narrower cease and desist order that required LabMD to stop employees from installing unauthorized programs on office computers would have been enforceable as opposed to a complete overhaul of the data security program. The court also noted that the order neither gave specific guidelines on how to meet the reasonableness standard that the FTC had invoked nor ordered LabMD to stop committing a specific unfair act or practice.

Experts in the field had hoped the Eleventh Circuit would address LabMD's argument that data security breaches are outside the FTC's jurisdiction under the unfairness prong of the FTC Act, an argument the Third Circuit rejected in *FTC v. Wyndham Worldwide Corporation*. The court discussed that what makes an act "unfair" is a violation of some existing policy in the law, eventually animating the FTC's complaint using the common law of negligence. However, the court's holding was limited to the unenforceability of the cease and desist order. The court did not decide the issue of the FTC's jurisdiction, instead assuming *arguendo* that the FTC was correct in alleging that an unfair practice had occurred.

TIP: The FTC maintains authority to regulate companies' data security practices under the unfairness prong of the FTC Act. Companies are advised to maintain reasonable security practices and to monitor FTC's enforcement practices and decisions.

2 Min Read

Related Topics

Data Breach | Consumer Privacy | Health Care Privacy

Related Capabilities

Privacy & Data Security | Compliance Programs | Trade Secrets, Non Competes & Restrictive Covenants | Intellectual Property | Health Care | Technology, Media & Telecommunications

Related Professionals

Steven Grimes

This entry has been created for information and planning purposes. It is not intended to be, nor should it be substituted for, legal advice, which turns on specific facts.