Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

With HTC Deal, FTC Claims Power To Set Security Standards

By **Allison Grande**

Law360, New York (February 22, 2013, 8:52 PM ET) -- The Federal Trade Commission on Friday resolved an action accusing HTC America Inc. of failing to properly secure its smartphones and tablet computers, a move that attorneys say shows the agency is confident in its authority to dictate security protocols despite the lack of legislation or regulation setting such standards.

The agency's complaint marked its first against a mobile device manufacturer. The agency alleged that HTC's failure to use "reasonable and appropriate" security measures in developing its software put sensitive information about millions of consumers at risk. The security flaws affected software it developed for mobile devices and tablets based on the Android, Windows Mobile and Windows Phone operating systems.

To settle the claims, HTC agreed to release software patches to fix the vulnerabilities, design a comprehensive program to address security risks during device development, and undergo independent security assessments every other year for the next two decades, according to the regulator.

“The FTC has been stating for some time that companies should develop and maintain a comprehensive and documented security program to avoid running afoul of Section 5 of the FTC Act,” Covington & Burling LLP communications and media practice group co-chair Yaron Dori told Law360 on Friday. “Apparently, HTC had not done that, which is surprising.”

But while this may put companies on notice, attorneys say the lack of binding legislation or regulation leaves them guessing at exactly what the regulator expects to see in an adequate security plan.

"It's really a shifting and unfair standard," said Morgan Lewis & Bockius LLP partner Gregory Parks. “The FTC has asked for legislation that has more concrete standards, but that hasn't happened. So the agency keeps going back to an 'adequate measures' standard, which provides no advance notice to companies about what is expected of them.”

For instance, the FTC's complaint criticized HTC for failing to include in its voice recorder application a “simple, well-documented software code” known as a permission check code.

“How is a company in this space supposed to know that they need to use permission check codes?” Parks asked. “If there is law out there that says mobile device makers need to have adequate security and it must include permission check codes, then everyone would know. But all companies have now is this complaint from the FTC that says that.”

The FTC claims the code would have ensured that third-party applications had permission before they could access the device's microphone, GPS-based information, and other sensitive data and features.

It also chided HTC for not providing its engineering staff adequate security training, not testing software for security vulnerabilities, and not having a process for receiving and addressing vulnerability reports from third parties.

Since no binding regulation requires these practices, the FTC uses its authority to police unfair and deceptive trade practices under Section 5 of the FTC Act to sustain such cases. In the HTC action, it alleged that user manuals for HTC Android-based devices contained deceptive representations, and said the user interface for the company's Tell HTC application was also deceptive.

While the FTC has long taken the position that Section 5 authorizes it to determine what sort of security standards are reasonable, "you don't have to scratch too far under the surface to notice that the FTC's standard for what amounts to reasonable security practices has been rising for some time," Dori said.

He cautioned that to avoid seeing the courts limit this authority, the agency must "strike a careful balance between leaving industry room to maneuver and stepping in when it believes an industry player has not met a certain standard."

Companies that believe the FTC "has gotten the balance wrong" can fight its findings in court, as Wyndham Hotels and Resorts LLC did in a rare challenge to the regulator, Dori noted. The agency had accused the company of failing to protect the personal information of its guests.

Instead of settling the claims privately, Wyndham lodged a motion to dismiss the suit in August, claiming the agency's attempt to establish data security standards for the private sector overstepped its statutory authority.

Although Friday's complaint linked HTC's allegedly flimsy security only to the threat of a breach, not to an actual one, the company, unlike Wyndham, chose to settle with the regulator.

"HTC privacy and security are important, and we are committed to improving practices that help safeguard our customers' devices and data," the company said in a statement Friday.

HTC confirmed that it is working to meet the FTC's directives to address the identified security vulnerabilities on the majority of devices released in the U.S. after December 2010.

"[This] demonstrates that the FTC now may begin to require companies to take remedial steps to fix security vulnerabilities," Dori said.

Despite the pending challenge to the agency's authority to bring these cases in the future, attorneys warn that companies should pay attention to the terms of the settlement when deciding what steps they should take to protect user data.

"These issues are not going away. If anything, stakeholders should be doubling down on their data security precautions," Dori said.

HTC is represented by Susan Lu Lyon of Cooley LLP.

The case is In the Matter of HTC America Inc., file No. 112-3049, in the Federal Trade Commission.

--Editing by Kat Laskowski and Chris Yates.
