WILMERHALE

The FTC Brings Section 5 Charges Against Internet-of-Things Companies

JANUARY 5, 2017

On January 5, 2017, the FTC filed a complaint against the Taiwanese company D-Link and its US subsidiary, D-Link Systems. D-Link and its subsidiary manufacture and sell networked devices, including routers and Internet-protocol (IP) cameras that provide live feeds over the Internet. The FTC's complaint alleges that the companies engaged in unfairness pursuant to Section 5 of the FTC Act by failing to reasonably secure their devices and deception under Section 5 by making numerous misrepresentations relating to device security.

The crux of the FTC's allegations is that the companies "have failed to take reasonable steps to protect their routers and IP cameras from widely known and reasonably foreseeable risks of unauthorized access." Compl. ¶ 15. In particular, the FTC alleges that the companies did not use remediation measures to protect against widespread flaws like "'hard-coded" user credentials and other backdoors." *Id*. Nor, according to the FTC's complaint, did the companies use free software to secure users' mobile app login credentials. The FTC further alleges that the companies did not properly secure D-Link's "private key," which the FTC describes as a digital signature used by software to assure other entities that the software is genuine and not malicious. Consequently, according to the FTC, the private key was available on a public website for about six months.

In the FTC's view, these vulnerabilities left thousands of D-Link's devices at risk. For example, the FTC alleges that hackers could easily identify these vulnerable devices online and use them to attack devices on a router's network or monitor an IP camera. Further, the FTC posits that consumers could have downloaded malicious software signed by D-Link's publicly available private key.

Further, FTC's complaint alleges that the companies represented to consumers that their products were safe. In its Security Event Response policy, for example, D-Link Systems allegedly claimed that it "prohibits at all times . . . any intentional product features or behaviors which allow unauthorized access to the device or network." *Id*. at ¶ 20. The companies' promotional materials asserted, among other things, that the devices were "easy to secure" and that its router was "one of the safest." *Id*. ¶ 21. In light of these alleged misrepresentations, the FTC brought five claims for deceptive practices under the FTC Act.

The FTC's complaint is its third Internet-of-Things (IoT) data security enforcement action. As IoT devices proliferate along with security threats and vulnerabilities, we can expect the FTC to keep a watchful eye over this field.