THOMSON REUTERS
Westlaw®

FTC v. D-Link Systems and the internet of things

Elizabeth McGinn, John Williams and Christopher Walczyszyn, *Buckley Sandler LLP*

OCTOBER 19, 2018

Businesses are selling consumers an increasing number of "internet of things" devices that connect directly to the internet against a backdrop of limited regulation, including wireless routers, video-enabled baby cameras and daily step trackers.

The Federal Trade Commission has taken notice and, to further its consumer protection mission, has undertaken efforts to compel businesses selling IoT products to enhance security and protect consumer data from unauthorized access.

The FTC's approach has been twofold. First, it has worked to foster a commitment among businesses to provide consumers with more secure devices as a best practice by publishing guidelines and working to educate businesses about data security. Second, it has positioned itself as a protector of consumer privacy on the IoT by bringing enforcement actions against businesses it views as providing their customers insufficient data protection.

THE FTC'S VIEWS OF ITS ROLE

The FTC has increasingly sought to regulate IoT devices sold to consumers to advance its consumer protection agenda. In January 2015, FTC staff issued a report titled "Internet of Things: Privacy & Security in a Connected World," as part of the agency's IoT regulatory efforts.

The report is designed to serve a number of functions, including providing businesses guidance and best practices for securing IoT devices, raising awareness about IoT-related issues and articulating the FTC's regulatory and enforcement priorities with respect to the IoT.

The report stresses the FTC's view that device security is a paramount concern in the IoT and identifies issues of importance to industry stakeholders.

For example, it notes that improperly secured devices can expose personal information, provide hackers with information needed to launch system attacks, and compromise consumer safety.

Beyond just advocating for enhanced security, the report takes the position that better security is good for business because "perceived risks to privacy and security" may pose a challenge to "widespread adoption" of IoT devices.[1]

FTC staff appears committed to providing regulatory oversight of IoT devices and "believes that a strong FTC law enforcement presence will help incentivize appropriate privacy and security-protective practices by [businesses] manufacturing and selling connected devices."

DUAL-TRACK APPROACH

In a regulatory landscape lacking directly applicable legislation related to IoT devices, the FTC has proactively sought to shape the IoT regulatory environment using a dual-track approach. First, it is encouraging businesses to voluntarily enhance the security features on their IoT devices, mainly by adopting best practices.

Beyond just advocating for enhanced security, the FTC takes the position that better security is good for business because the "perceived risks to privacy and security" may pose a challenge to "widespread adoption" of IoT devices.

Second, the agency pursues enforcement actions that are aimed at compelling businesses to adopt enhanced consumer-protective and IoT device security practices.

THE FTC'S APPROACH TO BEST PRACTICES

The FTC outlines best practices on its website, in the IoT report and in a shorter and more targeted companion report released in January 2015 titled "Careful Connections: Building Security in the Internet of Things."

These consumer-protective best practices address issues surrounding the IoT, including the security of the devices themselves, data storage and businesses' responses to security breaches and evolving security threats.

Specifically, the FTC recommends conducting product risk assessments, limiting data storage and testing device security. It further says businesses should properly train employees on responding to security flaws, work with trusted third parties that demonstrate an ability to provide reasonable data security, and implement risk response protocols.

Additional suggestions include providing software updates as needed and generally endeavoring to shield devices from hackers.

FTC V. D-LINK SYSTEMS INC.

In addition to encouraging best practices, the FTC has attempted to compel changes through enforcement actions. One recent example of the FTC's increased focus on IoT is an action it brought against D-Link Systems, a manufacturer of wireless routers, in January 2017.

The FTC claimed that D-Link misrepresented the integrity of the security features on its products in promotional materials and deceived its customers. Its complaint said D-Link acted unfairly by falsely claiming in marketing materials that its products offered a number of data security features, including data encryption and protection against unauthorized access.

The FTC also alleged that D-Link's failures "to take reasonable steps to secure the software for their routers and IP cameras" put consumers' data at risk.[2]

These security flaws, the FTC claimed, could allow hackers to target devices connected to D-Link's routers and obtain sensitive information from vulnerable D-Link devices by rerouting internet traffic and accessing files stored on networked devices like hard drives.

> Specifically, the FTC recommends conducting product risk assessments, limiting data storage and testing device security.

Hackers might also be able to access D-Link's IP cameras, turn them on remotely and spy on people without their knowledge, the complaint said.

The U.S. District Court for the Northern District of California dismissed a number of the FTC's claims, including that D-Link deceived consumers about the security features of its devices in promotional materials. The court reasoned that vague references to security in the materials would not have misled reasonable consumers.

The court did allow deception claims to proceed because they identified specific alleged misrepresentations about router and IP camera security. It also rejected the FTC's unfairness claim as speculative, noting that it failed to allege actual injury to consumers.

The practical effects of the order in the D-Link action may be minimal for several reasons.

First, the court noted that the FTC could have satisfied the injury requirement of an unfairness claim by alleging that D-Link's insufficiently secure IoT devices caused consumers injury in the aggregate.

While the FTC chose not to argue there was aggregate injury to consumers in its action against D-Link, nothing precludes it from relying on this or similar arguments in other enforcement actions.

Second, not all courts appear equally concerned with the FTC's reliance on speculative injury to consumers as the harm in an unfairness claim.

For example, while the 11th U.S. Circuit Court of Appeals reversed the FTC's finding that a laboratory's failure to maintain the security of its customer's data constituted an unfair practice, the court did so on the basis that the FTC's order was vague and assumed arguendo that the laboratory had committed an unfair practice.[3]

Third, the FTC has taken a strong stance on data security in the IoT space and has enforcement authority under other statutes that could arguably apply to the use of popular IoT devices.

FTC'S CONSENT ORDERS AND SETTLEMENTS

In addition to its enforcement efforts regarding D-Link, the FTC has brought enforcement actions for failing to properly secure IoT devices against another business that makes routers, ASUS (in 2016), and a business that makes baby cameras, TRENDnet (in 2013).[4]

The agency resolved the actions against ASUS and TRENDnet through consent orders that required the businesses to (1) establish security programs designed to provide consumers with secure devices and robust data security practices; (2) conduct routine audits of their security practices for the next 20 years; and (3) provide audit reports to the FTC upon request.

In its actions against D-Link, ASUS and TRENDnet, the FTC relied primarily on its authority under the FTC Act, 15 U.S.C.A. § 45, to combat "deceptive and unfair practices."

But the agency maintains it can also choose from a panoply of statutes to pursue enforcement actions against businesses manufacturing IoT devices. It has done so in at least one instance: In 2018, it filed a complaint against children's toy manufacturer VTech Electronics Ltd. to assert violation of the Children's Online Privacy Protection Act, 15 U.S.C.A. § 6501, also known as COPPA.[5]

That case included allegations that VTech failed to get parental consent before using children's personal information and failed to adequately secure their devices, and resulted in a $650,000 settlement. In addition to COPPA, the FTC could also rely on provisions in the HI-TECH Act related to healthcare-information breaches to subject business that sell medical IoT devices to FTC scrutiny.

CONCLUSION

Given the FTC's stated commitment to enhancing consumer protection in the IoT space, and the avenues available for enforcement, it is unlikely the FTC's efforts will be slowed or that IoT devices will evade the FTC's regulatory scrutiny.

It is critical that businesses manufacturing devices that connect to the internet and collect or distribute consumer data ensure that the data is collected in a way that complies with consumer data protection laws the FTC administers and that they provide consumers with adequate data security.

NOTES

[1] COMMISSION STAFF, FTC INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD 53 (Jan. 2015).

[2] Complaint at 11, *FTC v. D-Link Sys. Inc.,* No. 17-cv-39, 2017 WL 65168 (N.D. Cal. Jan. 5, 2017).

[3] *See In the Matter of LabMD Inc.,* No. 9357, 2016 WL 4128215 (F.T.C. July 28, 2016), vacated by *LabMD Inc. v. Fed. Trade. Comm.*, No. 16-16270 (11th Cir. June 6, 2018).

[4] Decision and Order, *ASUSTeK Computer Inc.*, FTC File No. 142 3156 (July 18, 2016) (Dkt. No. C-4587); Decision and Order, *TRENDnet INC.*, FTC File No. 122 3090 (Jan. 16, 2014) (Dkt. No. C-4426).

[5] Complaint, *United States v. VTECH Electronics North America, LLC*, No. 18-cv-114, 2018 WL 317978 (N.D. Ill. Jan. 8, 2018).

This article first appeared October 8, 2018, on Practitioner Insights Data Privacy *page*.

ABOUT THE AUTHOR



Elizabeth E. McGinn (L) is a partner in the Washington and New York offices of **Buckley Sandler LLP. John B. Williams** (C) is counsel in the firm's Washington office, where **Christopher M. Walczyszyn** (R) is an associate. They advise clients on consumer financial services, privacy and cybersecurity-related matters, and electronic discovery.