FTC Files Complaint Against D-Link, Alleging Failure to Take Reasonable Measures to Secure Routers and Internet Cameras

By Mary Ellen Callahan, Peter Hanna and Amit Patel

On January 5, 2017, in one of its first acts in the new year, the FTC filed a complaint in the Northern District of California against Taiwanese manufacturer D-Link Corp. and its US subsidiary (together, D-Link), alleging that D-Link overstated the security of its routers and internet-connected cameras and, at the same time, failed to take reasonable steps to secure those devices from unauthorized access. The lawsuit against D-Link signals the FTC's continued commitment to police data privacy and security in the fast-developing "Internet of Things" (IoT) space, particularly when a company's internet-connected product and security designs depart from established best practices.

The complaint focuses on two of D-Link's popular product offerings: its internet routers and internet-connected cameras, both of which are designed and advertised as remotely accessible and controllable through D-Link's free "mydlink Lite" mobile application. The complaint highlights prominent promotional material on D-Link's website, manuals and brochures that emphasizes the D-Link routers are "EASY TO SECURE," offer "ADVANCED NETWORK SECURITY," and utilize "the same" encryption technology "used in E-commerce or online banking." The FTC charges, however, that despite its claims of security, D-Link failed to take simple steps such as "reasonable software testing and remediation measures" necessary "to protect [D-Link's] routers and IP cameras against well-known and easily preventable software security flaws." Further noting that internet-connected cameras such as D-Link's are often used for home surveillance and security purposes (including homeowners' live monitoring of their homes while away or parents' live monitoring the safety of their children), the FTC also alleges in the complaint that D-Link gave consumers a false sense of security by using "SECURITY" and/or "SECURICAM" branding and graphics on product packaging, literature and user interfaces, and by posting a misleading "Security Event Response Policy" on the D-Link website that suggested D-Link had taken "reasonable steps to secure their products from unauthorized access," when, the FTC alleges, D-Link had not taken such steps.

According to the complaint, the result of D-Link's failure to take necessary reasonable steps to secure its devices – a claim that D-Link contested the day after the lawsuit was filed, asserting in a press release that its security processes were "more than reasonable" – not only put consumers' privacy at risk, but left open common security vulnerabilities that allowed hackers to gain control of consumers' devices remotely. These vulnerabilities include, for example, D-Link's integration of "hard-coded" and easily guessable login credentials into D-Link camera software – such as the username "guest" and password "guest" and the storing of login credentials for D-Link's mobile application in unsecured, clear and readable text format.

The existence of such vulnerabilities in connected devices that sit at the perimeters of networks – such as D-Link's routers and internet cameras – is particularly problematic. As the FTC alleges in the D-Link complaint, such critical vulnerabilities essentially render meaningless even true and accurate representations of the use of other security measures (such as "best possible" encryption and digital signature technologies); moreover, compromised perimeter devices can be used as a gateway to other information and devices on the same network, including sensitive personal information and/or other increasingly widespread connected devices, including home appliances and other pieces of the connected home.

This marks the third time that the security of internet-connected devices has been the subject of an FTC action. In 2013, the FTC filed a complaint alleging that TRENDnet marketed its "SecurView" internet-connected cameras as "secure," when in fact those cameras had software flaws that allowed widespread unauthorized access of the camera feeds including, in some instances, access by anyone who had a given SecurView camera's IP address. In early 2016, the FTC settled with ASUSTeK Computer, Inc. (Asus) over charges that security flaws in Asus routers put consumers' home networks at risk of unauthorized access as well.

The complaint against D-Link shows that the FTC is continuing to pursue companies who have deviated from the FTC's relatively recent (non-binding but informative) guidance on how to preserve privacy and security in IoT connected products. In its January 2015 Internet of Things Staff Report, the FTC encouraged makers of connected devices to use a risk-based approach during the design process and embrace best practices developed by security experts, such as strong encryption and proper authentication, in their products.

The complaint against D-Link suggests that promoting IoT devices as "secure" while allowing such devices to have backdoor passwords, clear-text passwords stored locally, command-injection bugs and public private keys, is not reasonable, and the failure to address such vulnerabilities through basic and inexpensive security best practices could mislead and harm consumers.

Makers of internet-connected devices, particularly of devices that include remote access and control capabilities, must use diligence and care not only when making claims about the security of their devices (to avoid charges of deception), but more importantly during the design process (to avoid charges of unfairness). As the actions against TRENDnet, Asus and now D-Link all show, FTC scrutiny of claims of product security will analyze both public statements and whether reasonable security has been achieved.

Contact Us

Mary Ellen Callahan, Partner, Jenner & Block

Phone: 202 639-6064 Email: mecallahan@jenner.com Download V-Card

Peter Hanna, Associate, Jenner & Block

Phone: 312 840-7229 Email: phanna@jenner.com Download V-Card

Amit Patel, Associate, Jenner & Block

Phone: 312 840-7337 Email: apatel@jenner.com Download V-Card

Unsubscribe | **Manage preferences** | **Forward to a friend**

© Copyright 2017 Jenner & Block LLP, 353 North Clark Street, Chicago, IL 60654, 312 222-9350. Jenner & Block is an Illinois Limited Liability Partnership including professional corporations. Under professional rules, this communication may be considered advertising material. The material contained in this document has been authored or gathered by Jenner & Block for informational purposes only. It is not intended to be and is not considered to be legal advice. Transmission is not intended to create and receipt does not establish an attorney-client relationship. Legal advice of any nature should be sought from legal counsel. Tax Matters: To the extent this material or any attachment concerns tax matters, it is not intended or written to be used, and cannot be used by a taxpayer, for the purpose of avoiding penalties that may be imposed on the taxpayer under law.