D-LINK SYSTEMS: POSSIBLE SIGNS FOR THE FUTURE OF FTC DATA SECURITY ENFORCEMENT

by Ronald Cheng and Mallory Jensen[1]

I. INTRODUCTION

Enforcement actions by administrative regulators have been increasingly important for understanding the key requirements for data security compliance. In particular, the U.S. Federal Trade Commission (FTC or Commission) has asserted a major role, through its enforcement authority against unfair and deceptive practices under the Federal Trade Commission Act. Recently, as "Internet of Things" (IoT) products, such as security cameras, smart watches, and web-enabled refrigerators have proliferated in the marketplace, FTC enforcement action has adapted to address security issues that arise from the increased flow of data handled by these products.

Part of this trend is the FTC's civil action for injunctive relief against the Taiwanese IoT manufacturer, D-Link Corporation, and its U.S. subsidiary, D-Link Systems, Inc. (collectively "D-Link").[2] D-Link has fought the charges, and trial is pending for early next year in San Francisco federal court. This article describes the FTC's recent approach to data security enforcement, with examples from the *D-Link* case to illustrate those enforcement practices.

II. THE FTC AND DATA SECURITY

The Federal Trade Commission Act empowers the Commission to prevent "unfair or deceptive acts or practices."[3] In the area of data privacy, the FTC typically has investigated whether the privacy policy and other representations to the public by manufacturers and service providers fail to account for security deficiencies. The FTC has brought civil complaints in federal courts, which to a great degree have been resolved through consent decrees. Areas that have been the subject of FTC actions include safeguards for customer personal information, protections against outside attacks and other compromise, remote access, and supervision of service providers.

From its experience, the FTC has issued "Start with Security,"[4] a summary of "lessons learned" that have been distilled from over 50 enforcement actions, organized by the following topics:

1. Start with security.
2. Control access to data sensibly.

---

1 Ronald Cheng is a partner in the Data Security and Privacy group at O'Melveny, co-located in Los Angeles and Hong Kong. Mallory Jensen is counsel in O'Melveny's Data Security and Privacy group, based in San Francisco.

2 *Federal Trade Commission v. D-Link Corp.*, No. 3:17-cv-00039-JD (N.D. Cal.) (complaint filed Jan. 5, 2017).

3 15 U.S.C. § 45(a)(1).

4 Federal Trade Commission, "Start with Security," *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

3. Require secure passwords and authentication.

4. Store sensitive personal information securely and protect it during transmission.

5. Segment your network and monitor who's trying to get in and out.

6. Secure remote access to your network.

7. Apply sound security practices when developing new products.

8. Make sure your service providers implement reasonable security measures.

9. Put procedures in place to keep your security current and address vulnerabilities that may arise.

10. Secure paper, physical media, and devices.

"Start with Security" illustrates each of these topics with examples from specific enforcement actions. For instance, one principle under the heading of "Apply Sound Security Practices" is the advice to "[t]rain your engineers in secure coding." The FTC notes that in several cases, including one against a telecom company, the FTC had alleged that the companies failed to train employees in secure coding practices, leading to "questionable design decisions, including the introduction of vulnerabilities into the software." In particular, the FTC notes that the telecom company "failed to implement readily available secure communications mechanisms in the logging applications it pre-installed on its mobile devices," making it possible for malicious third party apps to communicate with the logging apps so that consumers' data was at risk.

To illustrate the principle that service providers include appropriate security standards in contracts, the FTC cites the case of a company that hired service providers to transcribe audio files containing sensitive health information, but did not require those third parties to take reasonable security measures, with the result that the files were exposed on the internet. And in discussing the FTC's recommendation that companies must keep safety standards in place when data is en route, the pamphlet cites another FTC case in which unencrypted backup tapes, a laptop, and an external hard drive, all of which contained sensitive information, were stolen from an employee's car, when the company should have had a policy limiting employees' ability to transport such material.

The FTC has updated and expanded the summary provided in the "Start with Security" pamphlet through a series of blog entries, "Stick with Security," which has entries on the same topics.[5] The "Stick with Security" series is also illustrated by examples from the FTC's enforcement actions, though company names are not used.

Although the FTC is careful in these publications not to provide any insider or nonpublic information about these cases, or to make any statements that would prejudice its position in active cases, these commentaries are nonetheless useful indicators of the direction of the FTC's interest in specific types of companies and privacy violations—that is, how it is interpreting what is "unfair" and "deceptive" in the area of data security

5 Federal Trade Commission, "Stick with Security: A Business Blog Series," *available at* https://www.ftc.gov/tips-advice/business-center/guidance/stick-security-business-blog-series.

and what kinds of companies and violations might be targets. In particular, companies that handle large amounts of consumer data and that make any representations about the security of that data, then arguably—at least in the FTC's view—do not live up to the strength of those representations, will have cause for concern.

III. THE *D-LINK* LITIGATION

In early 2017, the FTC filed a complaint in federal court against the D-Link parent company and a U.S. subsidiary.[6] D-Link manufactures internet routers and Internet-Protocol (IP) cameras and sells those devices in the U.S.

The FTC alleged in its complaint that D-Link failed to conduct software testing and take corrective measures to protect against various security flaws that exposed these products to outside attackers. The FTC's complaint also alleged that D-Link failed to protect adequately the private key for its software—which resulted in exposure of the key on a public website for about six months—and failed to use publicly available software to secure mobile app login credentials.

The FTC claimed that as a result these goods were subject to attacks and were vulnerable to being conscripted into "botnets," or networks of malware-infected computers. Separately, a compromised router could lead to consumers being redirected to malicious websites and thereby providing sensitive information. Conversely, an attacker could obtain sensitive documents stored on devices accessible through the compromised router. Similarly, a compromised IP camera could give an attacker the ability to monitor surreptitiously consumers and their families.[7]

As part of its complaint, the FTC asserted that D-Link made false representations about product security, including after reports of security flaws. These representations included claims that the products incorporated the latest wireless security features and were protected by advanced network security.

The FTC sought injunctive relief against D-Link, with charges based on D-Link's allegedly unfair acts in not securing device software and its allegedly deceptive acts in representing that the devices—including the Graphical User Interface (GUI) through which customers used them—were adequately secured from unauthorized access.

A. D-Link's Challenge to Suit Against the Taiwanese Parent

D-Link first contended, in a motion to dismiss for lack of jurisdiction, that the FTC lacked jurisdiction over the parent corporation located in Taiwan. The parent asserted that it had structured its operations to separate itself from its U.S. operations, which were operated by D-Link Systems, Inc. The parent asserted that it acted only to coordinate

---

6 *D-Link*, No. 17-cv-00039-JD, ECF No. 44 (unredacted complaint filed Mar. 20, 2017).

7 As part of its investigation, the FTC engaged employees to create accounts on a search engine, Shodan, to determine the online presence of devices, including presumably those at issue in this case. *Id.*, ECF No. 108 (FTC's letter brief filed Feb. 15, 2018 to limit D-Link subpoena on Shodan, LLC to protect FTC's work product and statutory rights under the Stored Communications Act, 18 U.S.C. §§ 2701–2712). D-Link contended that the search engine is a controversial tool used by hackers. *Id.*, ECF No. 110 at p. 2 (D-Link opposition letter brief filed Feb. 27, 2018).

between that U.S. subsidiary and third-party vendors based in Asia that manufactured and tested its products.

The FTC in turn asserted that the parent had satisfied the requirements for exercise of personal jurisdiction. A federal court may exercise jurisdiction over a foreign defendant where:

> (1) the defendant either "purposefully direct[s]" its activities or "purposefully avails" itself of the benefits afforded by the forum's laws; (2) the claim "arises out of or relates to the defendant's forum-related activities; and (3) the exercise of jurisdiction [] comport[s] with fair play and substantial justice, i.e. it [is] reasonable."[8]

With regard to the first requirement, the FTC asserted that the D-Link parent purposefully availed itself of the U.S. market through, among other things, finalizing the requirements of its products in coordination with the U.S. subsidiary and by addressing security issues for those products offered for sale in the U.S.[9] Alternatively, the FTC contended that the parent purposefully directed its activities to the U.S. by designing the products, assuming responsibility for their manufacture, and directing the security testing, with the intent to distribute the products in the U.S. through the U.S. subsidiary.[10]

Ultimately, the parties agreed by joint stipulation to an order dismissing the Taiwanese parent without prejudice, with counsel for the U.S. subsidiary agreeing to accept discovery requests on behalf of the parent.[11] Nevertheless, the motion to dismiss for lack of jurisdiction presented an issue likely to arise again with other foreign manufacturers that structure their design, manufacture, and sales operations through separate U.S. subsidiaries. That is particularly true as companies assert that the resolution of these data security-related claims depends on foreign law.

The issue whether exercise of U.S. jurisdiction over a foreign entity is reasonable may depend on:

> (1) the extent of the defendant's purposeful interjection into the forum state, (2) the burden on the defendant in defending in the forum, (3) the extent of the conflict with the sovereignty of the defendant's state, (4) the forum state's interest in adjudicating the dispute, (5) the most efficient judicial resolution of the controversy, (6) the importance of the forum to the plaintiff's interest in convenient and effective relief, and (7) the existence of an alternative forum.[12]

---

8 *Dole Food Co. v. Watts*, 303 F.3d 1104, 1111 (9th Cir. 2002).

9 *Federal Trade Commission v. D-Link Corp.*, No. 3:17-cv-00039-JD (N.D. Cal.), ECF No. 58 at 9:12–18 (FTC opposition filed April 17, 2017 to D-Link's motion to dismiss).

10 *Id.* at 10:1–4.

11 *Id.*, ECF No. 75 (Joint Stipulation and Order Dismissing D-Link Corporation without Prejudice entered May 15, 2017).

12 *Bancroft & Masters, Inc. v. Augusta Nat'l Inc.*, 223 F.3d 1082, 1088 (9th Cir. 2000).

The third and fourth factors, involving foreign sovereignty and a foreign state's interest in the dispute, could become relevant when, for example, manufacturers in China assert conflicting data security obligations in China. That is, a Chinese manufacturer may assert that what a U.S. regulator deems a "vulnerability" is in fact a disclosure or means of access that is necessary to comply with China's Cybersecurity Law. Specifically, the law imposes requirements on manufacturers that certain network products and services must undergo a state security assessment and that network operators cooperate with Chinese public security and state security bureaus.[13] To the extent a foreign jurisdiction has an interest in the future in resolving the issues raised in an FTC complaint, these issues may demonstrate a "conflict with the sovereignty of the defendant's state" or "the forum state's interest in adjudicating the dispute." A foreign company could highlight these conflicts to a court to explain why an FTC action against it should be dismissed.

B. D-Link's Challenge to the FTC's Enforcement Authority Over the Security of Its Devices

D-Link brought a separate motion to dismiss the complaint that challenged the FTC's power to seek injunctive relief, based on what the FTC asserted were inadequately identified risks of harm from the alleged security flaws. D-Link attacked both the FTC's "unfairness" claim and the "deception" claims.

The court dismissed the unfairness claim. The court initially rejected D-Link's claim that the FTC did not have authority under Section 5 of the FTC Act to regulate data security practices, given that Congress deliberately made the provision "open-ended."[14] Interestingly, the court's order did not state that the FTC had articulated what constituted unfairness in the data security context, perhaps in recognition that, at least at this stage, fairness "is a flexible concept with evolving content."[15] Indeed, the court then rejected D-Link's claim that the FTC had not provided fair notice, since, as the court noted, "to require the FTC in all cases to adopt rules or standards before responding to data security issues faced by consumers is impractical and inconsistent with governing law."[16]

But after rejecting these claims, the court addressed the complaint's allegation of the likelihood of substantial injury for the unfairness claim under Section 5(n) of the FTC Act.[17] The court noted that the FTC's claim depended on the allegation that outside hackers could avail themselves of available tools to exploit known vulnerabilities in D-Link devices.[18] The court deemed this allegation to "make out a mere possibility of injury at best."[19] Importantly, the complaint did not allege that anyone had suffered harm

---

13 China Cybersecurity Law, arts. 23, 28.

14 *D-Link*, No. 3:17-cv-00039-JD, ECF No. 90 at 6:6–7:1.

15 *Id.* at 6:22–23 (citing *FTC v. Bunte Bros., Inc.*, 312 U.S. 349, 353 (1941)) (internal quotation marks omitted).

16 *Id.* at 7:17–18.

17 *Id.* at 8:10–9:28.

18 *Id.* at 8:20–23.

19 *Id.* at 8:25–26.

from the alleged security flaws. This was in contrast to other cases that alleged an actual theft of personal information that went along with identified fraudulent activity.[20]

The court noted in passing that the FTC could have based its unfairness claim on representations as to data security that D-Link made to consumers. If the FTC had done so, the alleged purchase of an unsecure device or a device not as secure as advertised "would likely be in the ballpark of a 'substantial injury,' particularly when aggregated across a large group of consumers."[21] But that was not the approach taken by the FTC. Accordingly, the court dismissed the unfairness count.

The court also analyzed the FTC's claims alleging deceptive practices by D-Link with respect to advertising and labeling its products. In particular, the court addressed D-Link's claim that a disclaimer to the consumer in its security policy frustrated the FTC's ability to allege fraud to survive its motion to dismiss.[22] The court rejected this claim, noting that "[d]isclaimers, moreover, do not as a matter of law immunize statements that are otherwise deceptive."[23] The court then pointedly remarked:

> That point is particularly apt here, where the D-Link disclaimer attempts a sweeping abandonment of responsibility that purports to dump on the consumer all of the risk that D-Link may be wrong, reckless or outright lying about its data security features.[24]

While the court rejected this general attack on the deceptive statement counts, the court dismissed some of the complaint's counts involving particular alleged misrepresentations, given that the support for those counts did not contain specific statements that were likely to be misleading to consumers. The only representation was the single word "SECURITY" printed on the brochure, in contrast to exhibits in support of other counts that contained particular statements regarding data security.[25] Nevertheless, the court supported other alleged misrepresentations regarding routers and IP camera GUIs.[26]

This partial defeat for the FTC is instructive in many ways. The court basically concluded that the FTC did not adequately allege that D-Link's security flaws actually led to misuse of data. Without such an allegation, the court found, there was not the requisite element of "substantial injury" needed for the FTC to bring an action on the "unfairness" claim. This ruling should be read together with the Eleventh Circuit's recent rejection of the FTC's data security cease and desist order against LabMD, Inc.[27] After

---

20 *D-Link*, No. 3:17-cv-00039-JD, ECF No. 90 at 8:26–9:12 (citing *FTC v. Wyndham Worldwide*, 799 F.3d 236, 242 (3d Cir. 2015)).

21 *Id.* at 9:22–28 (citation omitted).

22 *Id.* at 5:4–16. D-Link's disclaimer states: "It is up to the reader to determine the suitability of any directions or information in this document." *Id.* at 5:6–7.

23 *Id.* at 5:10–13 (citing *FTC v. Brown & Williamson Tobacco Corp.*, 778 F.2d 35, 42–44 (D.C. Cir. 1985)).

24 *Id.* at 5:13–16.

25 *Id.* at 5:21–6:4.

26 *Id.* at 5:17–20.

27 *LabMD, Inc. v. FTC*, 894 F.3d 1221, 1237 (11th Cir. 2018).

someone installed LimeWire, a file-sharing application, on a computer used by the billing manager at LabMD, a medical laboratory, the FTC filed an enforcement action, asserting that LabMD's data-security program was inadequate and constituted an unfair practice under Section 5(a) of the FTC Act.[28] The FTC's complaint alleged that LabMD failed to employ a variety of security measures, resulting in the improper exposure of consumer data.[29] The Eleventh Circuit held that the order's absence of any prohibitions and lack of instruction to stop specific acts or practices rendered the order unenforceable based on lack of specificity.[30]

In particular, the court disapproved the injunctive provision requiring that LabMD "establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers."[31] In the court's view, this requirement impermissibly exposed LabMD to the prospect of dueling experts who asserted or contested that a particular component "x" was "a necessary component of a reasonably designed data-security program."[32] This effective modification of the injunction at future hearings for an order to show cause would subject LabMD to "micromanaging . . . beyond the scope of court oversight contemplated by injunction law."[33]

In light of these rulings, the FTC will need to plead that there has been an actual misuse of data. This may be difficult in many cases, particularly with IoT devices, as discussed below. To the extent allegations of substantial injury depend on theft of personal information, perpetrators of IoT hacks do not necessarily seek the data from the IoT device, nor do they do anything with it if they obtain it. Rather, they simply want the computing power of the device in order to attack others. This suggests, for instance, that the FTC would have a difficult time pursuing a company such as Hangzhou Xiongmai, which manufactured many of the webcams that were used in a notorious botnet that took down a major internet infrastructure service provider in 2016.[34] While the webcams were hijacked so that malicious actors could use their computing power to engage in a Distributed Denial of Service (DDoS) attack, it is highly unlikely that the hackers were interested in any of the data stored and transmitted on the devices. Even if they siphoned off some of the data, given the massive size and geographic spread of the attack, showing (or even alleging) that any of the data was actually misused would be a difficult task.

Nevertheless, at the same time, the *D-Link* court provided insight into its thinking about how the unfairness claim was alleged and what could be done differently in the future. For example, the FTC could tie such claims to the representations underlying the deception claims, which would make the injury allegation more plausible: that is, a

---

28 *Id.* at 1224-25.

29 *Id.* at 1225 n.8, 1229.

30 *Id.* at 1236-37.

31 *Id.* at 1236.

32 *Id.*

33 *Id.* at 1237.

34 Michael Kan, *Chinese firm admits its hacked DVRs, cameras were behind Friday's massive DDOS attack*, PC World, Oct. 23, 2016, *available at* https://www.pcworld.com/article/3134039/hacking/chinese-firm-admits-its-hacked-products-were-behind-fridays-massive-ddos-attack.html.

consumer who purchases a device that is not as secure as advertised is likely to be able to show substantial injury. Hints such as this dicta in the court's order on D-Link's motion to dismiss are likely to guide the FTC's approach going forward, as discussed below, particularly with respect to IoT devices.

IV. IMPLICATIONS FOR FOREIGN IOT MANUFACTURERS

Trial in the *D-Link* case is currently scheduled for January 2019.[35] It is likely that the volume of FTC enforcement activity against overseas IoT manufacturers and distributors will continue to increase. Enforcement could include claims similar to those in *D-Link*, but the FTC has also taken action to enforce the Children's Online Privacy Protection Act of 1998 (COPPA).[36] COPPA generally sets requirements for the collection of information of children under 13 years of age, including providing notice of such collection to the child's parent and obtaining consent from the parent.

This year, the FTC entered into a consent decree with the Hong Kong-based children's electronic learning products manufacturer, VTech Electronics Ltd., and its U.S. subsidiary ("VTech") to enjoin the collection of information in violation of the FTC's own COPPA rule.[37] VTech provided a "Kid Connect" online app on these products, so that child users could communicate with other children and adults who also had the app. The FTC alleged that VTech failed to link its privacy policy to each area of Kid Connect that collected personal information from children. The FTC also alleged VTech failed to develop and implement an adequate information security program and that, in November 2015, VTech learned that a hacker had compromised consumer information, including personal information of children who used Kid Connect.[38]

The consent decree enjoined VTech from violating COPPA, particularly with regard to requiring notice to parents of its data collection practices and obtaining parental consent for that collection. The decree also required VTech to pay a $650,000 judgment, to establish an information security program, and to undergo data security assessments conducted by a qualified third-party professional.[39] State regulators have followed in kind,

---

35 *D-Link*, No. 3:17-cv-00039-JD, ECF No. 149 (amended scheduling order). Each side recently moved for summary judgment. *D-Link*, No. 3:17-cv-00039-JD (N.D. Cal.), ECF Nos. 178 and 183. The FTC argued that D-Link made certain representations regarding the security of its routers and cameras, and that those devices contained serious vulnerabilities, but that D-Link sold the devices anyway. *D-Link*, No. 3:17-cv-00039-JD (N.D. Cal.), ECF No. 178 at 2:1-6. D-Link, for its part, argued that the allegedly deceptive statements were all made in the past, and are no longer being made, while any device vulnerabilities have been resolved, and its current security practices are reasonable. *D-Link*, No. 3:17-cv-00039-JD (N.D. Cal.), ECF No. 183 at 5-11. D-Link also contended that there are "no consumer victims" and that the FTC has failed to present any evidence of any consumers who were actually harmed. *Id.* at 2:9-15. The motions are pending for hearing on November 1, 2018. *Id.* at 1:3.

36 15 U.S.C. §§ 6501–6506.

37 *United States v. VTech Electronics Ltd.*, No. 18-cv-00114 (N.D. Ill.), ECF No. 2 (FTC motion for entry of stipulated order; attaching FTC COPPA Rule, 16 C.F.R. §§ 312.1–312.13).

38 *Id.*, ECF No. 1, ¶¶ 10–28 (complaint filed Jan. 8, 2018).

39 *Id.*, ECF No. 2-1 at 8–14.

including a recent consent decree that the New Jersey Division of Consumer Affairs entered into with a Chinese mobile app developer, Meitu, Inc.[40]

The more general scrutiny given to IoT and other technology products connected to China by U.S. regulators suggests that similar enforcement actions are forthcoming. For example, the U.S.-China Economic and Security Review Commission recently commissioned a report on the U.S. federal information and communications technology (ICT) supply chain, which identified risks based on China's encouragement of indigenous ICT capacity, as well as pressures on U.S. industry to reveal source code, submit to security audits, and require storage of data in China. As a result, the report's authors recommended a national strategy for supply chain risk management for supply chain vulnerabilities for ICT, with a special emphasis on procurement linked to China.[41]

Similarly, in reviewing foreign acquisitions of U.S. businesses, the Committee on Foreign Investment in the United States (CFIUS) has noted its focus on certain proposed acquisitions of U.S. businesses engaged in "cryptography, data protection, Internet security, and network intrusion detection."[42] It is not too much of a leap to infer that CFIUS may have a similar interest in the ability of a foreign acquirer to secure sensitive personal data of U.S. citizens by way of a transaction, and that CFIUS' scrutiny could hinder the parties' ability to pursue or complete the deal.

V. CONCLUSION

The procedural history thus far in the *D-Link* matter provides two lessons for IoT manufacturers and regulators. First, the scope of the FTC's enforcement activity includes the vigorous exercise of its long-arm power over overseas manufacturers that conduct activity in the U.S. As *D-Link* and some of the other cases discussed here suggest, Asian manufacturers and suppliers have claimed a growing share of the IoT market. With that growth, the FTC has demonstrated an interest in their data security policies and practices. While the D-Link parties avoided a court ruling on the jurisdictional issue over the Taiwanese parent through a stipulation in which the parent agreed to provide discovery in exchange for dismissal, there are likely to be future cases presenting this issue, particularly if the parent conducts its activities in the U.S. through agents or third parties.

Second, as discussed above, an FTC unfairness claim in the context of IoT device vulnerability will likely present disputes as to whether there is a "substantial injury." If the FTC is unable to show anything more than possible unauthorized access to personal information without actual theft, the FTC is left with the dicta in *D-Link* that the deficiency may be cured where the alleged vulnerability is connected to a deceptive representation. The FTC did not allege an actual botnet takeover of D-Link devices. If it

---

40 *In re Meitu, Inc.*, Consent Order, New Jersey Dep't of Law and Public Safety, Division of Consumer Affairs (Apr. 17, 2018), *available at* https://www.njconsumeraffairs.gov/News/PressAttachments/05082018-press-attachment.pdf.

41 Interos Solutions, Inc., Supply Chain Vulnerabilities from China in U.S. Federal Information and Communications Technology (prepared for U.S.-China Economic and Security Review Comm'n), ch. 4 (Apr. 2018), *available at* https://www.uscc.gov/sites/default/files/Research/Interos_Supply%20Chain%20Vulnerabilities%20from%20China%20in%20U.S.%20Federal%20ICT_final.pdf.

42 Guidance Concerning the National Security Review Conducted by the Committee on Foreign Investment in the United States, 73 Fed. Reg. 74567, 74571 (Dec. 8, 2008).

could make that showing, perhaps the court would then confront a different basis to find at least a prima facie showing of a substantial injury. To await such an event, however, is inconsistent with the FTC's enforcement program, which seeks preventative action from IoT manufacturers.