PILLSBURY WINTHROP SHAW PITTMAN LLP
LAURA C. HURTADO (CSB #267044)
laura.hurtado@pillsburylaw.com
Four Embarcadero Center, 22nd Floor
San Francisco, California 94111
Telephone: (415) 983-1000
Facsimile: (415) 983-1200

CAUSE OF ACTION INSTITUTE
PATRICK J. MASSARI [*pro hac vice* pending] [Lead Counsel]
patrick.massari@causeofaction.org
MICHAEL PEPSON [*pro hac vice* pending]
michael.pepson@causeofaction.org
KARA E. MCKENNA [*pro hac vice* pending]
kara.mckenna@causeofaction.org
1875 Eye Street N.W., Suite 800
Washington, D.C. 20006
Telephone: (202) 422-4332
Facsimile: (202) 330-5842

*Attorneys for Defendant D-Link Systems, Inc.*

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

FEDERAL TRADE COMMISSION,

Plaintiff,

v.

D-LINK CORPORATION

and

D-LINK SYSTEMS, INC.,

Defendants.

No. 3:17-cv-00039-JD

**DEFENDANT D-LINK SYSTEMS, INC.'S NOTICE OF MOTION AND MOTION TO DISMISS COMPLAINT; MEMORANDUM OF POINTS AND AUTHORITIES**

Date: Thursday, March 9, 2017
Time: 10:00 a.m.
Courtroom: 11

Judge: Hon. James Donato

# TABLE OF CONTENTS

**Page**

## TABLE OF AUTHORITIES

**Page(s)**

Cases

Statutes and Codes



Rules and Regulations



Other Authorities

**NOTICE OF MOTION AND MOTION**

TO ALL PARTIES AND THEIR ATTORNEYS OF RECORD:

PLEASE TAKE NOTICE that on March 9, 2017, at 10:00 a.m., or as soon thereafter as this may be heard, in Courtroom 11 of this Court located at 450 Golden Gate Avenue, 19th Floor, San Francisco, CA, before the Honorable James Donato, United States District Judge, defendant D-Link Systems, Inc. ("D-Link Systems") will, and hereby does, move this Court for an Order dismissing Federal Trade Commission's ("FTC" or "Commission") Complaint with prejudice pursuant to Fed. R. Civ. P. 12(b)(6) and 9(b) for failure to state a claim. This Motion is based upon this Notice of Motion and Motion; this Memorandum of Points and Authorities; all pleadings and papers filed in this action; oral argument of counsel; and any other matter properly considered.

**ISSUE TO BE DECIDED**

1. Does the Complaint fail to state a claim upon which relief may be granted pursuant to Federal Rules of Civil Procedure 12(b)(6) and 9(b)?

**MEMORANDUM OF POINTS AND AUTHORITIES**

## I. INTRODUCTION

This is a case of government overreach, without justification or any evidence of consumer injury in violation of D-Link Systems's due process rights, which should be dismissed.

To begin, this action is *ultra vires* because the FTC lacks statutory authority to regulate data security for Internet of Things ("IoT") companies as an "unfair" practice under Section 5.

The FTC further fails to plead the basic elements necessary for a Section 5 "unfairness" violation. Section 5(a) does not empower the FTC to prohibit all business practices—only those that are "unfair."[1] Under Section 5(n), which further limits the FTC's "unfairness" authority, the FTC "shall have no ["unfairness"] authority … *unless* the act or practice *causes or is likely to cause substantial injury* to consumers which *is* not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[2]

Here, the FTC's "unfairness" claim fails federal pleading requirements because it is devoid

[1] *See* 15 U.S.C. § 45(a) ("Section 5(a)").

[2] *See* 15 U.S.C. § 45(n) ("Section 5(n)") (emphasis added).

of well-pleaded *factual* allegations (1) that D-Link Systems engaged in "unfair" conduct; (2) D-Link Systems's alleged data-security practices *currently* harm or are likely to harm consumers; (3) an identifiable data breach resulting in actual harm to identifiable consumers; (4) how the hypothetical alleged past "risk" of harm outweighs the time and monetary costs of implementing whatever data-security practices the FTC apparently ***now*** thinks D-Link Systems should have used and the countervailing benefits to consumers and competition; (5) the alleged *past hypothetical* "risk" of harm was not reasonably avoidable by "consumers"; and (6) the appropriate standard of care at specific points in time and deviations therefrom.

Pleading legal conclusions couched as hypothetical, speculative factual allegations requiring unwarranted deductions, as the FTC has done here, is insufficient.

The FTC's "unfairness" claim independently fails because the FTC's standardless ex post "we know 'unfair' data security when we see it" case-by-case approach to enforcing Section 5 violates D-Link Systems's due process right to fair notice of prohibited or required conduct.

The Complaint's "deception" counts should also be dismissed for failure to meet the heightened pleading standards set by Rule 9(b), which requires such claims to be pled with particularity. At minimum, each "deception" count must be supported by well-pleaded factual allegations establishing the "who, what, when, where, and how." The Complaint fails to do this.

For these reasons, this Court should grant D-Link Systems's Motion in its entirety.

## II. BACKGROUND[3]

As relevant here, two (of three) FTC Commissioners voted to authorize FTC Staff to issue this Complaint; Commissioner Maureen Ohlhausen dissented.[4] On January 5, 2015, the FTC filed this Complaint ("Compl.") (Dkt. No. 1) against Defendants alleging an "unfairness" count (Count I) and five "deception" counts (Counts II-VI) in violation of Section 5.

The Complaint has alleged the following: D-Link routers and IP cameras are sold in the

[3] Under Rule 12(b)(6), certain well-pleaded factual allegations are assumed true solely for purposes of this Motion. *See Ashcroft v. Iqbal*, 556 U.S. 662, 677-79 (2009).

[4] *See* FTC Press Release, "FTC Charges D-Link Put Consumers' Privacy at Risk Due to the Inadequate Security of Its Computer Routers and Cameras" (Jan. 5, 2017) (reporting 2-1 vote), *at* https://www.ftc.gov/news-events/press-releases/2017/01/ftc-charges-d-link-put-consumers-privacy-risk-due-inadequate.

United States. *See* Compl. ¶¶ 6-7, 10-11. D-Link routers, like other routers, are used to join together computers and other Internet-connected devices. *See* Compl. ¶ 13. D-Link IP cameras perform a home-security function and are used "to detect any events that may place the property or its occupants at risk[.]" Compl. ¶ 14. The IP cameras are allegedly "offer[ed] as a means to monitor the security of a home … or to monitor activities within the household." Compl. ¶ 14.

To support its "unfairness" count, the Complaint alleges that at some unspecified point in the past Defendants "failed to take reasonable steps" to secure unspecified routers and IP cameras from alleged "reasonably foreseeable risks of unauthorized access[.]" *See* Compl. ¶ 15. It further alleges that certain unspecified routers and IP cameras were "vulnerable" at some point in the past, creating a past "significant risk" of harm to "consumers" because certain events allegedly "could" hypothetically have occurred. *See* Compl. ¶¶ 16-18. The Complaint does not allege that any of the alleged past data-security practices caused an actual identifiable data breach. Nor does it allege that the alleged *past* data-security practices caused actual harm to any identifiable person. *See* Compl. ¶¶ 16-18. The Complaint does not allege that Defendants are *currently* using allegedly "unreasonable" data-security practices. *See* Compl. ¶ 15. Nor does it allege that Defendants acted recklessly or with any ill intent. *See, e.g.*, Compl. ¶¶ 15, 28.

Based in large part on the alleged *past* failure to take reasonable steps to secure unspecified routers and IP cameras and the *past* "significant risk" of hypothetical harm, *see* Compl. ¶¶ 15-18, 32, 35, 38, 41, 44, the Complaint also alleges various "deceptive" practices. *See* Compl. ¶¶ 31-45. All "deception" counts rely on and incorporate by reference exhibits attached to the Complaint purportedly reflecting *past* representations—most of which appear to have been made between 2010 and 2012; none of which involve express claims about the alleged data-security practices at issue here. *See* Compl. ¶¶ 15, 20-24, 31, 34, 37, 40, 43; PX1-PX11.

## III. ARGUMENT

### A. Standard of Review

"[O]nly a complaint that states a plausible claim for relief survives a motion to dismiss." *Ashcroft v. Iqbal*, 556 U.S. 662, 679 (2009). "Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice." *Id.* at 678; *see Bell Atl. Corp. v.*

*Twombly*, 550 U.S. 544, 555 (2007). "[T]he Court will not treat as fact or accept as true allegations that are bare legal conclusions, recitations of elements, or unwarranted deductions." *Graham v. Wells Fargo Bank, N.A.*, No. 3:15-cv-04220-JD, 2017 U.S. Dist. LEXIS 3598, at *3 (N.D. Cal. Jan. 10, 2017). The Court may also consider documents whose contents are alleged in the complaint or "incorporated into the complaint by reference, and matters of which a court may take judicial notice." *Skilstaf, Inc. v. CVS Caremark Corp.*, 669 F.3d 1005, 1016 n.9 (9th Cir. 2012). Section 5 "deception" claims must meet the heightened pleading requirements of Rule 9(b), *see FTC v. Lights of Am., Inc.*, 760 F. Supp. 2d 848, 853-54 (C.D. Cal. 2010), and particularly allege the "who, what, when, where, and how," *see Brickman v. Fitbit, Inc.*, No. 15-cv-02077-JD, 2016 U.S. Dist. LEXIS 150125, at *4-8 (N.D. Cal. July 15, 2016).

**B. The Count I "Unfairness" Claim Should Be Dismissed**

**1. "Unfairness" Cannot Be Premised on Alleged Past "Vulnerabilities."**

Without exception, *all* of Defendants' allegedly "unreasonable" data-security practices are pleaded in *the past tense*. *See, e.g.*, Compl. ¶¶ 15 ("have failed" and "have stored"), 16 ("have been vulnerable"), 17 ("risk … was significant" and "attackers could use"), 18 ("put consumers at significant risk of harm"). This is fatal to the "unfairness" claim.

Section 5(n)'s plain language—which, importantly, uses the present tense—limits "unfairness" liability to *current* harmful practices. *See* 15 U.S.C. § 45(n) ("caus*es* or *is* likely to cause" (emphasis added)); *see also* 1 U.S.C. § 1; *Carr v. United States*, 560 U.S. 438, 448 (2010) ("present tense generally does not include the past"); *Bonnichsen v. United States*, 357 F.3d 962, 973 (9th Cir. 2004) (same). Section 5(n)'s undeviating use of the present tense, particularly when juxtaposed with other provisions of Section 5 using the past tense, *see, e.g.*, 15 U.S.C. § 45(b) ("has been"), confirms that liability cannot be based on an alleged past "risk" of harm. *Cf. Gwaltney of Smithfield, Ltd. v. Chesapeake Bay Found., Inc.*, 484 U.S. 49, 59, 63 & n.4 (1987).

"Congress's use of the present tense matters." *United States v. Marsh*, 829 F.3d 705, 709 (D.C. Cir. 2016). "Caus*es*" does not mean "caus*ed*." And "*is* likely" does not mean "*was* likely." *See Guidiville Band of Pomo Indians v. NGV Gaming, LTD.*, 531 F.3d 767, 770 (9th Cir. 2008) ("[T]he word 'is' means just that (in the most basic, present-tense sense of the word)[.]"); *Abdul-*

*Akbar v. McKelvie*, 239 F.3d 307, 313-14 (3d Cir. 2001) (construing "is" to exclude past events); *see also Nichols v. United States*, 136 S. Ct. 1113, 1117-18 (2016); *United States v. Jackson*, 480 F.3d 1014, 1018-21 (9th Cir. 2007) ("travels" does not refer to past travels).

Because the Complaint is devoid of *factual* allegations relating to Defendants' current data security-related practices, Count I fails to state a claim upon which relief may be granted.

**2. Complaint Fails to Plead Section 5(n) Elements.**

**a. Causes or Is Likely to Cause Substantial Injury to Consumers**

The FTC must plead facts plausibly showing that Defendants' data security currently "causes or is likely to cause substantial injury[.]" 15 U.S.C. § 45(n). The FTC has not done so.

Save for a past-tense legal conclusion, *see* Compl. ¶ 29, the Complaint does not contain *any* factual allegations of actual harm to any "consumers," *see* Compl. ¶¶ 15-18, let alone the sort of "substantial" injury required by Section 5(n). *See* 15 U.S.C. § 45(n). The Complaint is devoid of *factual* allegations of an identifiable data breach *involving in any way* D-Link routers and IP cameras, let alone one *causally connected* to D-Link products—and it is equally devoid of allegations of identity theft or fraud causing monetary harm to identifiable consumers.

This alone should be fatal. Without exception, no Article III court has found "unfairness" liability in the absence of actual physical or monetary harms to identifiable "consumers." *See In re LabMD, Inc*., Initial Decision, F.T.C. Docket No. 9357, 2015 FTC LEXIS 272, at *114-*116 (Nov. 13, 2015) ("LabMD Initial Decision"), *vacated by* Opinion of the Commission, 2016 FTC LEXIS 128 (July 29, 2016), *stayed sub nom.*, *LabMD v. FTC*, No. 16-16270-D (11th Cir. Nov. 10, 2016) ("LabMD Stay Order") (attached as Exhibit A to Pepson Decl.). With the sole exception of a controversial (currently stayed) FTC administrative prosecution,[5] *see* LabMD Stay Order at 6-10, 13, the FTC itself has not imposed "unfairness" liability absent evidence of actual monetary or

[5] FTC staff predicated their case against LabMD on false evidence provided to the FTC by a third party. *See* LabMD Initial Decision, 2015 FTC LEXIS 272, at *12-22, *53-72. A congressional investigation ensued, resulting in a 100-page report. *See id.* at *71-72; STAFF OF H. COMM. ON OVERSIGHT AND GOV'T REFORM, 113TH CONG., TIVERSA, INC.: WHITE KNIGHT OR HIGH-TECH PROTECTION RACKET (2015), *available at* https://www.databreaches.net/wp-content/uploads/2015.01.02-Staff-Report-for-Rep.-Issa-re-Tiversa.pdf. The ALJ dismissed the complaint for lack of evidence of harm, *see* LabMD Initial Decision, 2015 FTC LEXIS 272, at *190-201, yet the Commission reversed. The Eleventh Circuit then stayed the case.

physical harm. *See* LabMD Initial Decision, 2015 FTC LEXIS 272, at *114 ("the parties do not cite, and research does not reveal, any case where unfair conduct liability has been imposed without proof of actual harm, on the basis of predicted 'likely' harm alone").

The Complaint does not contain *factual allegations* that even plausibly allege that Defendants' allegedly "unfair" data-security practices are likely to cause harm to consumers, relying instead on, at best, unwarranted deductions based on speculation. *See* Compl. ¶¶ 15-18. The Complaint's conclusory recitation of this element is insufficient. *See* Compl. ¶¶ 29, 46.

The FTC solely relies on conclusory and speculative allegations contained in the section of the Complaint titled "Thousands of Consumers at Risk," *see* Compl. ¶¶ 16-18, to meet its burden of pleading "likely" harm. *See* Compl. ¶ 30. Those paragraphs do not contain factual allegations, *see* Compl. ¶¶ 16-18, with the sole exception of a passing reference to "press reports" of alleged past vulnerabilities, *see* Compl. ¶ 16. Instead, the FTC relies on bald speculation divorced from facts, tellingly couched in language such as "*have been* vulnerable"; "significant *risk* of unauthorized access"; "[t]he *risk* ... *was* significant"; "remote attackers *could* take"; "remote attackers *could search* for vulnerable devices"; "[a]lternatively, attackers *could use* readily accessible scanning tools"; "Defendants put consumers at significant risk of harm"; "[a]n attacker *could compromise*" a router; "using a compromised router, an attacker *could re-direct* consumers"; "an attacker *could obtain*"; "an attacker *could* compromise a consumer's IP camera"; "[i]n many instances, attackers *could carry out such exploits covertly*"; "consumers … *were* at *significant risk* of downloading malware." *See* Compl. ¶¶ 16-18 (emphasis added).

Even taking the FTC's bald chains of speculation at face value, the FTC still fails to plead currently "likely" harm. Because Section 5(n) does not define "likely," its plain language should be interpreted based on the normal meaning of its words. *See Schindler Elevator Corp. v. United States ex rel. Kirk*, 563 U.S. 401, 407-08 (2011). The plain meaning of "likely" is "having a high probability of occurring …[,] very probable," or "in all probability." Merriam-Webster Online Dictionary, 2016, http://www.merriam-webster.com/. "Likely" does not mean "possible." *See also Southwest Sunsites v. FTC*, 785 F.2d 1431, 1436 (9th Cir. 1986). Nor does it mean "significant

risk," as defined by the Commission.[6] *See* LabMD Stay Order at 9-10 (rejecting the Commission's interpretation of "likely" to mean "significant risk," reading Section 5(n) "to require a higher threshold than that set by the FTC").

As the FTC's own Chief ALJ has explained: "Fundamental fairness dictates that proof of likely substantial consumer injury under Section 5(n) requires proof of something more than an unspecified and hypothetical 'risk' of future harm[.]" LabMD Initial Decision, 2015 FTC LEXIS 272, at *188-89 (rejecting theory that "unfairness" liability can be "based solely on the risk of a data breach and that proof of an actual data breach is not required").[7] Here, the Complaint, at best, alleges an unspecified, hypothetical "risk" of *past* harm. That is insufficient.

**b. Cost-Benefit Prong**

Under Section 5(n), "unfairness" liability may not be imposed unless the FTC proves that, among other things, the "substantial injury" the alleged practices currently cause or are likely to cause in the future outweigh the countervailing benefits to consumers and competition. 15 U.S.C. § 45(n); *see also* Unfairness Statement, 1984 FTC LEXIS 2, *309 ("[T]he injury must not be outweighed by any offsetting consumer or competitive benefits that the sales practice also produces."). The Commission has said it "will not find that a practice unfairly injures consumers unless it is injurious in its net effects." Unfairness Statement, 1984 FTC LEXIS 2, *309.

Recognizing the required analysis in the data-security context, the Commission has stated that Section 5(n) requires "'a cost-benefit analysis' that 'considers a number of relevant factors, including the probability and expected size of reasonably unavoidable harms to consumers given a

---

[6] We expect the FTC to mistakenly rely on dicta from *FTC v. Neovi, Inc.*, 604 F.3d 1150 (9th Cir. 2010), to claim that a past "significant risk of concrete harm" can be "substantial injury," *cf. id.* at 1157. That argument fails. First, unlike here, *Neovi* involved *actual harm to identifiable consumers. See id.* at 1154 (issuance of fraudulent checks totaling over $4 million); *accord FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 242 (3d Cir. 2015) (alleging actual harm to over 619,000 people and $10.6 million-plus fraud loss). Second, this dicta is based on a *footnote* in a Commission Statement of Policy on the Scope of Consumer Unfairness Jurisdiction (Dec. 17, 1980), appended to *Int'l Harvester Co.*, 104 F.T.C. 949, 1984 FTC LEXIS 2, at *307 n.12 (1984). The "Unfairness Statement" states: "The Commission is not concerned with trivial or merely speculative harms." *Id.* at *308. Thus, in *International Harvester*, liability was based on a product defect causing serious injury or death to identifiable consumers. *See id.* at *227.

[7] Notably, even the Commission has declined to address this novel Staff theory of "unfairness" liability. *See* LabMD Commission Opinion, 2016 FTC LEXIS 128, at *46-47.

certain level of cybersecurity and the costs to consumers that would arise from investment in stronger cybersecurity.'" LabMD Commission Opinion, 2016 FTC LEXIS 128, at *29 (quoting *Wyndham*, 799 F.3d at 255); *see also* Unfairness Statement, 1984 FTC LEXIS 2, at *309 ("The Commission also takes account of the various costs that a remedy would entail.").

Pleading this element as a legal conclusion, as the FTC has done here, *see* Compl. ¶ 29, is insufficient. With the sole exception of a passing reference to "free software," *see* Compl. ¶ 15(c), the Complaint contains no factual allegations whatsoever regarding the monetary costs, let alone the time- and labor-related costs, of conducting whatever "software testing and remediation measures" and other actions the FTC believes Defendants should have implemented.

This omission is fatal to the "unfairness" claim, *see* Compl. ¶ 15, particularly given the FTC's position that the "cost-benefit inquiry is particularly important in cases where the allegedly unfair practice consists of a party's failure to take actions that would prevent consumer injury or reduce the risk of such injury." LabMD Opinion, 2016 FTC LEXIS 128, at *78.

**c. Reasonable Avoidability Prong**

Section 5(n) also requires the FTC to plead facts sufficient to justify a plausible inference that the alleged "substantial injury" at issue could not reasonably be avoided by consumers. *See* 15 U.S.C. § 45(n). The FTC did not do this here.[8] The Complaint's sole mention of that necessary element of any "unfairness" violation is a passing legal conclusion. *See* Compl. ¶ 29.

**d. Deviations from Applicable Standard of Care**

The Complaint alleges that Defendants at some unidentified point in the past (not the present) "failed to take reasonable steps to protect their routers and IP cameras[.]" Compl. ¶ 15; *see also* Compl. ¶¶ 28, 30. The FTC apparently considers "unreasonableness" an element of an "unfairness" claim. *See* Order Denying Motion to Dismiss ("January 16 Order"), *In re LabMD, Inc.*, FTC No. 9357, 2014 FTC LEXIS 2, *46-48, *52-53 (Jan. 16, 2014). Under this rubric, the FTC must allege, at minimum, (a) what the applicable standard of care required at specific points

[8] Elsewhere, the FTC has recognized steps consumers can take to secure their routers and home networks. *See, e.g.,* FTC Consumer Information, "Securing Your Wireless Network," *at* https://www.consumer.ftc.gov/articles/0013-securing-your-wireless-network#understand.

in time and (b) deviations therefrom. *See also Silverpop Sys. v. Leading Mkt. Techs., Inc.*, 641 F. App'x 849, 852 (11th Cir. 2016) (unpublished). *Cf. S&H Riggers & Erectors, Inc. v. OSHRC*, 659 F.2d 1273, 1282-85 (5th Cir. 1981) (due process may require use of objective industry standard).

The need to identify what *was* allegedly "reasonable" (and *when*) is particularly important in the data-security context, for as the Commission itself has recognized, data "security threats and technology constantly evolve … in this rapidly changing area." January 16 Order, 2014 FTC LEXIS 2, at *40-41. Here, the Complaint does not even generally identify the relevant time period at issue in a term of years,[9] let alone plausibly plead facts showing what the applicable standard of care required when and deviations therefrom at specific points in time.

**3. Failure to Plead Culpability Requirements for "Unfairness" Liability.**

Section 5(a) only declares unlawful practices involving culpable conduct more egregious than mere alleged negligence or "unreasonableness"—that is, "unfair … acts or practices." *See* 15 U.S.C. § 45(a)(1). "The plain meaning of 'unfair' is 'marked by injustice, partiality, or deception.'" *LeBlanc v. Unifund CCR Partners*, 601 F.3d 1185, 1200 (11th Cir. 2010) (quoting Merriam-Webster Online Dictionary (2010)). Thus, in addition to alleging conduct satisfying Section 5(n)'s necessary but not sufficient preconditions for liability, the FTC should be required to allege conduct "marked by injustice, partiality, or deception," such as recklessness or similarly blameworthy behavior, to satisfy the requirements for Section 5(a). *See* 15 U.S.C. § 45(a)(1). *Cf. FTC v. Wyndham Worldwide Corp*., 799 F.3d 236, 259 (3d Cir. 2015) ("§ 45(n) [requirements] may be necessary rather than sufficient conditions"). *But cf. Neovi*, 604 F.3d at 1156-57.

Here, the FTC failed to do that, instead alleging only that "Defendants have failed to take reasonable steps to secure the software for their routers and IP cameras[.]" Compl. ¶ 28.

**4. This Action Violates Due Process for Failure to Give Fair Notice.**

Entities regulated by administrative agencies have a due process right to fair notice of regulators' requirements. *United States v. AMC Entm't, Inc*., 549 F.3d 760, 768-70 (9th Cir. 2008); *see, e.g., Montgomery Ward & Co. v. FTC*, 691 F.2d 1322, 1332 (9th Cir. 1982); *see Christopher v.*

[9] The Complaint contains only three vague references to dates. *See* Compl. ¶¶ 15, 20.

*SmithKline Beecham Corp.*, 132 S. Ct. 2156, 2167 (2012) (agencies should provide regulated entities fair warning of prohibited or required conduct). "To provide sufficient notice, a statute or regulation must 'give the person of ordinary intelligence a reasonable opportunity to know what is prohibited so that he may act accordingly.'" *United States v. Approximately 64,695 Pounds of Shark Fins*, 520 F.3d 976, 980 (9th Cir. 2008) (quoting *Grayned v. City of Rockford*, 408 U.S. 104, 108 (1972)). The responsibility to promulgate clear, unambiguous standards is upon the agency. *See United States v. Trident Seafoods Corp.*, 60 F.3d 556, 559 (9th Cir. 1995); *Marshall v. Anaconda Co.*, 596 F.2d 370, 377 n.6 (9th Cir. 1979); *see also Ga. Pac. Corp. v. OSHRC*, 25 F.3d 999, 1005-06 (11th Cir. 1994) (ascertainable certainty standard); *Gen. Elec. Co. v. EPA*, 53 F.3d 1324, 1329 (D.C. Cir. 1995) (same).

The FTC has not done so, as a U.S. District Judge explained to the FTC in 2014: "I think that you will admit that there are no security standards from the FTC." Preliminary Injunction Hearing Tr., *LabMD v. FTC*, 1:14-cv-810-WSD, at 94:14-15 (May 7, 2014) (Duffey, J.). *See generally* Gus Horowitz, *Data Security and the FTC's UnCommon Law*, 101 IOWA L. REV. 955, 959-60, 973-80 (2016) (noting and echoing Judge Duffey's concerns). The FTC's standardless Section 5 "unfairness" data security regulation violates due process for failure to give fair notice of prohibited or required conduct, *see Connally v. Gen. Constr. Co.*, 269 U.S. 385, 391 (1926), and by authorizing and encouraging seriously discriminatory enforcement, *see FCC v. Fox TV Stations, Inc.*, 132 S. Ct. 2307, 2317 (2012); *Giaccio v. Penn.*, 382 U.S. 399, 402-03 (1966) (due process violated if "judges and jurors [are] free to decide, without any legally fixed standards, what is prohibited and what is not in each particular case"). *Cf. United States v. Jimenez*, No. 15-cr-00372-JD-1, 2016 U.S. Dist. LEXIS 91337, at *5-*18 (N.D. Cal. June 6, 2016) (dismissing indictment to the extent the prosecution was based on a theory that the Defendant possessed a "receiver," within the meaning of a regulation, because Government failed to give fair notice of its interpretation).

The FTC's lack of standards, as applied here, violates due process because the FTC has failed to provide IoT businesses like D-Link Systems fair notice (1) that, as a general matter, the FTC believes that selling IoT products that do not meet its subjective after-the-fact case-by-case benchmark for "reasonable" data security can be "unfair"; and (2) what data-security practices for

routers and IP cameras the FTC believes Section 5 to prohibit or to require, and when.

Even the FTC acknowledges that the *first* FTC *settlement* with an IoT company via a "consent order" was announced in September 2013.[10] *See In the Matter of TRENDnet, Inc*., FTC No. C-4426 (Jan. 16, 2014) (consent order). Consent orders "do[] not establish illegal conduct," *Intergraph Corp. v. Intel Corp*., 253 F.3d 695, 698 (Fed. Cir. 2001), and are "only binding upon the parties to the agreement," *Altria Grp., Inc. v. Good*, 555 U.S. 70, 89 n.13 (2008). Consent orders cannot provide fair notice because, among other things, they are fact-specific and involve no admission of liability. *See Wyndham*, 799 F.3d at 257 n.22. But even assuming arguendo that a consent order could provide such notice, if anything, *TRENDnet* suggests that no "unfairness" liability lies absent an identifiable data breach causing actual harm. *See* Compl., ¶¶ 9-11 ("Respondent's Breach"), *In the Matter of TRENDnet, Inc*., FTC No. C-4426 (Jan. 16, 2014).

The majority of this Complaint's allegations appear to relate to purported conduct allegedly occurring in 2010-2012. But even according to the FTC, it did not issue what it now calls "guidance" (FTC Staff's "Internet of Things" Report) until January 2015.[11] This FTC "Internet of Things" Report relates to a November 2013 FTC "workshop" and purportedly "summarizes the workshop and provides staff's recommendations in this area." Internet of Things Report at i. The Report only purports to "provide[] recommendations for best practices for companies," *id.* at 27, as opposed to what IoT data-security practices the FTC believes "unfair." Even if, counterfactually, the Report provided fair notice as of January 2015, it cannot provide fair warning for conduct

---

[10] The FTC publicly acknowledges that TRENDnet is the first such FTC enforcement action. *See* FTC Staff Report, Internet of Things: Privacy & Security in a Connected World ("Internet of Things Report") 32 (Jan. 2015) (describing "TRENDnet" as "the Commission's first case involving an Internet-connected device"), *available at* https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

[11] The FTC's press release about this case claims that "[t]he FTC has provided **guidance to IoT companies**" like D-Link Systems. FTC Press Release, FTC Charges D-Link Put Consumers' Privacy at Risk Due to the Inadequate Security of Its Computer Routers and Cameras" (Jan. 5, 2017) (emphasis added), *at* https://www.ftc.gov/news-events/press-releases/2017/01/ftc-charges-d-link-put-consumers-privacy-risk-due-inadequate. The bolded language in that press release hyperlinks to a ***January 27, 2015***, FTC press release regarding a FTC Staff Report on the "Internet of Things." *See* FTC Press Release, "FTC Report on Internet of Things Urges Companies to Adopt Best Practices to Address Consumer Privacy and Security Risks" (Jan. 25, 2015), *at* https://www.ftc.gov/news-events/press-releases/2015/01/ftc-report-internet-things-urges-companies-adopt-best-practices.

occurring before then. *See, e.g., Wilson v. Frito-Lay N. Am.*, 961 F. Supp. 2d 1134, 1147 (N.D. Cal. 2013). "Retroactivity—in particular, a new agency interpretation that is retroactively applied to proscribe past conduct—contravenes the bedrock due process principle that the people should have fair notice of what conduct is prohibited." *PHH Corp. v. Consumer Fin. Prot. Bureau*, 839 F.3d 1, 46 (D.C. Cir. 2016). So too here.

Finally, the Commission itself has previously taken the position that Section 5(n), standing alone, provides constitutionally adequate fair notice. *See* January 16 Order, 2014 FTC LEXIS 2, at *46. But even if Section 5(n)'s text *could* provide constitutionally adequate notice that cybersecurity practices resulting in an actual data breach causing monetary and identity theft harms to identifiable consumers may be "unfair" (it cannot), the Complaint here does not allege this. *See* Compl. ¶¶ 16-18 ("Thousands of Consumers At Risk"). *Cf. Wyndham*, 799 F.3d at 256 (after *second* hack and data breach, Wyndham had notice practices might fail Section 5(n)).

Here, the Complaint does not allege an actual identifiable data breach, let alone actual monetary or identity theft harm to identifiable consumers. Therefore, as applied here, Section 5(n) cannot provide fair notice. *Cf.* LabMD Initial Decision, 2015 FTC LEXIS 272, at *188 ("If unfair conduct liability can be premised on 'unreasonable' data security alone, … then … [Section 5(n)] would not provide the required constitutional notice of what is prohibited."); *Wyndham*, 799 F.3d at 256 ("Fair notice is satisfied here as long as the company can reasonably foresee that a court could construe its conduct as falling within the meaning of the statute.").

**5. The FTC's "Unfairness" Authority Does Not Extend to Data Security.**

Because Congress has not conferred power upon the FTC to regulate IoT data security, the FTC lacks authority to do so. *See La. Pub. Serv. Comm'n. v. FCC*, 476 U.S. 355, 374 (1986); *ABA v. FTC*, 430 F.3d 457, 468-69 (D.C. Cir. 2005). Section 5 says nothing about data security, silently refuting the FTC's newfound "unfairness" power claims, which should be greeted skeptically. *See Util. Air Regulatory Grp. (UARG) v. EPA*, 134 S. Ct. 2427, 2444 (2014); *FDA v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120, 159 (2000). If Congress wanted the FTC to regulate data security for the entire economy, it would have clearly said so. *See UARG*, 134 S. Ct. at 2444. Congress, however, did the opposite, last amending Section 5 to *limit* the FTC's

"unfairness" authority. *See* H.R. Conf. Rep. 103-617, 11-12, 1994 WL 385368, *11-12 (1994); S. Rep. 103-130, 1993 WL 322671 (1993). Congress did not give the FTC IoT data-security authority through an amendment specifically intended to narrow the FTC's powers. *See Whitman v. Am. Trucking Ass'ns., Inc.*, 531 U.S. 457, 468 (2001). The FTC's power grab should be rejected. *Cf. FTC v. AT&T Mobility LLC*, 835 F.3d 993, 1003 (9th Cir. 2016).

**C. The "Deception" Claims Fail as a Matter of Law.**

The FTC's "deception" claims (Counts II-VI) are subject to Rule 9(b) and must identify (1) a representation; that (2) is "likely to mislead consumers acting reasonably under the circumstances"; that (3) is "material." *FTC v. Stefanchik*, 559 F.3d 924, 928 (9th Cir. 2009). *See generally* FTC Policy Statement on Deception (appended to *Cliffdale Assocs.*, 103 F.T.C. 110, 1984 FTC LEXIS 71, *167, *170-71, *188 (1984)). "Each advertisement must stand on its own merits[.]" *Removatron Int'l Corp. v. FTC*, 884 F.2d 1489, 1496 (1st Cir. 1989).

**1. Count II Fails to State a Claim**

The Complaint specifically links Count II to alleged representations occurring between December 2013 and September 2015. *See* Compl. ¶¶ 20, 31. Count II then incorporates by reference Paragraph 15-18 of the Complaint to claim that "Defendants did not take reasonable steps to secure" unspecified D-Link products at some unspecified time in the past. *See* Compl. ¶ 32. That alone is fatal because Paragraphs 15-18 do not allege with particularity that D-Link Systems products were not reasonably secure between December 2013 and September 2015, let alone which products. Nor does the Complaint allege that a reasonable consumer would in any way base a decision to purchase a D-Link product on isolated language at the bottom of a webpage that is not an advertisement at all (instead titled "Security Event Response Policy"). *See* PX1. Indeed, immediately following the language the FTC highlights as the gravamen of this "deception" count, PX1 states: "It is up to the reader to determine the suitability of any directions or information in this document." *See* PX1. Therefore, Count II should be dismissed.

**2. Count III Fails to State a Claim**

Count III is based on a diffuse collection of stale D-Link Systems advertisements regarding different products from about five to seven years ago. *See* Compl. ¶¶ 21, 34 & PX2-5. The alleged

implied representations, *see* Compl. ¶¶ 21, 34, were apparently made in 2010 (PX3), 2011 (PX2, PX5), or 2012 (PX4), and solely relate to four specific router models: the 2011 D-Link® Wireless N 300 Router (DIR-615) (PX2); the 2010 D-Link® Mobile Wireless Router (DIR-412) (PX3); the 2012 D-Link® Wireless N Dual Band Router (DIR-815) (PX4); and the 2011 D-Link® Whole Home Router 1000 (DIR-645) (PX5). *See* Compl. ¶¶ 21, 34.

Count III incorporates by reference Paragraph 15-18 of the Complaint to claim that unspecified models of D-Link Systems routers "were not secure from authorized access and control" at some unspecified time in the past. *See* Compl. ¶ 35. The Complaint's exclusive reliance on Paragraphs 15-18 to show that the above-described representations were not only "misleading to reasonable consumers" but "material," standing alone, is fatal.[12] This is because Paragraphs 15-18 say nothing about *which* D-Link Systems router models were allegedly insecure, *when*, *where*, and *how*. *See* Compl. ¶¶ 15-18. Nor does the Complaint allege *facts* supporting a plausible inference that the alleged representations on which Count III is based are not literally true. *See* Compl. ¶¶ 15-18, 21 & PX2-5. Count III should therefore be dismissed.

**3. Count IV Fails to State a Claim**

Count IV should be dismissed because the FTC does not plead *which, when, where, and how* of the alleged deception. *See* Compl. ¶¶ 22, 37. For instance, the Complaint does not allege whether PX7 correlates to a product actually sold in the United States and, if so, when. Nor does it explain why the "Security" language in PX6 (a 2010 advertisement for a "Surveillance" camera designed to address home security threats like burglars) can plausibly be interpreted as relating in any way to data security. IP cameras are not advertised to perform the same data-security functions as products like computer anti-virus programs. The Complaint itself alleges that IP cameras "play a key security role for consumers" as surveillance devices allowing "consumers" to "monitor the security of their homes or the safety of young children" and "detect any events that may place the property or its occupants at risk." *See* Compl. ¶ 14.

[12] Nor does the Complaint allege facts supporting a plausible inference that any "reasonable" consumer would have viewed all such advertisements at the same time.

### 4. Counts V and VI Fail to State a Claim

Count V essentially alleges "deception" because the "GUI" (i.e., "graphic user interface") for the D-Link DIR-412 and other unspecified routers—which "consumers" would only see after purchase—stated at unspecified points in time "[t]o secure your new networking device, please set and verify a password" (PX8); "[i]t is highly recommended that you create a password to keep your router secure" (PX9); and "Helpful Hints … For security reasons it is recommended you change the password" (PX9). *See* Compl. ¶¶ 23, 40 & PX8-PX9. The FTC is claiming that the foregoing language in PX8 and PX9 probably misled reasonable consumers in a way likely to affect purchasing decisions and how D-Link routers were used. That strains credulity.[13]

PX10 and PX11 (dated 2012) illustrate why Count VI should be dismissed. Count VI, reduced to its essence, *see* Compl. ¶¶ 24, 43, alleges "deception" because the GUI for an IP camera used for surveillance and *home security* purposes (that is, protecting against security threats like burglars) says, unsurprisingly, "SECURICAM Network" (next to a picture of a lock) and states "[s]et up an Admin ID and Password to secure your camera. Click Next to continue," (PX10); and a "DCS-2310L Setup Wizard" from 2012 says "[e]nter a password to secure your camera, (PX11).[14] That is it. Count VI therefore fails for the same reason as Count V.

## IV. CONCLUSION

For the foregoing reasons, the Complaint should be dismissed with prejudice.

Dated: January 31, 2017

Respectfully submitted,
PILLSBURY WINTHROP SHAW PITTMAN LLP

By: /s/ Laura C. Hurtado
LAURA C. HURTADO (CSB#267044)

*Attorneys for Defendant D-Link Systems, Inc.*
*(Additional counsel listed on caption page)*

[13] The FTC makes the same representations: "Secure Your Router … Change your router's pre-set password(s)." FTC Consumer Information, "Securing Your Wireless Network," at https://www.consumer.ftc.gov/articles/0013-securing-your-wireless-network#secure.

[14] The FTC *currently* tells "consumers" to do this: "Using Security Features … Once you've bought your IP camera, set it up with security in mind. Here's how: … Check your camera's password settings. … Use a strong password." FTC Consumer Information, "Using IP Cameras Safely," *at* https://www.consumer.ftc.gov/articles/0382-using-ip-cameras-safely.