PRECEDENTIAL

UNITED STATES COURT OF APPEALS
FOR THE THIRD CIRCUIT

No. 14-3514

FEDERAL TRADE COMMISSION

v.

WYNDHAM WORLDWIDE CORPORATION,
a Delaware Corporation
WYNDHAM HOTEL GROUP, LLC,
a Delaware limited liability company;
WYNDHAM HOTELS AND RESORTS, LLC,
a Delaware limited liability company;
WYNDHAM HOTEL MANAGEMENT INCORPORATED,
a Delaware Corporation

Wyndham Hotels and Resorts, LLC,
Appellant

On Appeal from the United States District Court
for the District of New Jersey
(D.C. Civil Action No. 2-13-cv-01887)
District Judge: Honorable Esther Salas

Argued March 3, 2015

Before: AMBRO, SCIRICA, and ROTH, Circuit Judges

(Opinion filed: August 24, 2015)

Kenneth W. Allen, Esquire
Eugene F. Assaf, Esquire (Argued)
Christopher Landau, Esquire
Susan M. Davies, Esquire
Michael W. McConnell, Esquire
Kirkland & Ellis
655 15th Street, N.W., Suite 1200
Washington, DC 20005

David T. Cohen, Esquire
Ropes & Gray
1211 Avenue of the Americas
New York, NY 10036

Douglas H. Meal, Esquire
Ropes & Gray
800 Boylston Street, Prudential Tower
Boston, MA 02199

Jennifer A. Hradil, Esquire
Justin T. Quinn, Esquire
Gibbons
One Gateway Center
Newark, NJ 07102

Counsel for Appellants

Jonathan E. Nuechterlein
General Counsel
David C. Shonka, Sr.
Principal Deputy General Counsel
Joel R. Marcus, Esquire (Argued)
David L. Sieradzki, Esquire
Federal Trade Commission
600 Pennsylvania Avenue, N.W.
Washington, DC 20580

Counsel for Appellee

Sean M. Marotta, Esquire
Catherine E. Stetson, Esquire
Harriet P. Pearson, Esquire
Bret S. Cohen, Esquire
Adam A. Cooke, Esquire
Hogan Lovells US LLP
555 Thirteenth Street, N.W.
Columbia Square
Washington, DC 20004

Kate Comerford Todd, Esquire
Steven P. Lehotsky, Esquire
Sheldon Gilbert, Esquire
U.S. Chamber Litigation Center, Inc.
1615 H Street, N.W.
Washington, DC 20062

Banks Brown, Esquire
McDermott Will & Emery LLP
340 Madison Ave.
New York, NY 10713

Karen R. Harned, Esquire
National Federation of Independent Business
Small Business Legal Center
1201 F Street, N.W., Suite 200
Washington, DC 20004

Counsel for Amicus Appellants
Chamber of Commerce of the USA;
American Hotel & Lodging Association;
National Federation of Independent Business.

Cory L. Andrews, Esquire
Richard A. Samp, Esquire
Washington Legal Foundation
2009 Massachusetts Avenue, N.W.
Washington, DC 20036

John F. Cooney, Esquire
Jeffrey D. Knowles, Esquire
Mitchell Y. Mirviss, Esquire
Leonard L. Gordon, Esquire
Randall K. Miller, Esquire
Venable LLC
575 7th Street, N.W.
Washington, DC 20004

Counsel for Amicus Appellants
Electronic Transactions Association,
Washington Legal Foundation

Scott M. Michelman, Esquire
Jehan A. Patterson, Esquire
Public Citizen Litigation Group

1600 20th Street, N.W.
Washington, DC 20009

Counsel for Amicus Appellees
Public Citizen Inc.; Consumer Action;
Center for Digital Democracy.

Marc Rotenberg, Esquire
Alan Butler, Esquire
Julia Horwitz, Esquire
John Tran, Esquire
Electronic Privacy Information Center
1718 Connecticut Avenue, N.W., Suite 200
Washington, DC 20009

Catherine N. Crump, Esquire
American Civil Liberties Union
125 Broad Street, 18th Floor
New York, NY 10004

Chris Jay Hoofnagle, Esquire
Samuelson Law, Technology & Public Policy Clinic
U.C. Berkeley School of Law
Berkeley, CA 94720

Justin Brookman, Esquire
G.S. Hans, Esquire
Center for Democracy & Technology
1634 I Street N.W. Suite 1100
Washington, DC 20006

Lee Tien, Esquire
Electronic Frontier Foundation

815 Eddy Street
San Francisco, CA 94109

Counsel for Amicus Appellees
Electronic Privacy Information Center,
American Civil Liberties Union,
Samuelson Law, Technology & Public Policy Clinic,
Center for Democracy & Technology,
Electronic Frontier Foundation

OPINION OF THE COURT

AMBRO, Circuit Judge

The Federal Trade Commission Act prohibits "unfair or deceptive acts or practices in or affecting commerce." 15 U.S.C. § 45(a). In 2005 the Federal Trade Commission began bringing administrative actions under this provision against companies with allegedly deficient cybersecurity that failed to protect consumer data against hackers. The vast majority of these cases have ended in settlement.

On three occasions in 2008 and 2009 hackers successfully accessed Wyndham Worldwide Corporation's computer systems. In total, they stole personal and financial information for hundreds of thousands of consumers leading to over $10.6 million dollars in fraudulent charges. The FTC filed suit in federal District Court, alleging that Wyndham's conduct was an unfair practice and that its privacy policy was deceptive. The District Court denied Wyndham's motion to dismiss, and we granted interlocutory appeal on two issues:

whether the FTC has authority to regulate cybersecurity under the unfairness prong of § 45(a); and, if so, whether Wyndham had fair notice its specific cybersecurity practices could fall short of that provision.[1] We affirm the District Court.

I. Background

A. Wyndham's Cybersecurity

Wyndham Worldwide is a hospitality company that franchises and manages hotels and sells timeshares through three subsidiaries.[2] Wyndham licensed its brand name to approximately 90 independently owned hotels. Each Wyndham-branded hotel has a property management system that processes consumer information that includes names, home addresses, email addresses, telephone numbers, payment card account numbers, expiration dates, and security codes. Wyndham "manage[s]" these systems and requires the hotels to "purchase and configure" them to its own specifications. Compl. at ¶ 15, 17. It also operates a computer network in Phoenix, Arizona, that connects its data center with the property management systems of each of the Wyndham-branded hotels.

---

[1] On appeal, Wyndham also argues that the FTC fails the pleading requirements of an unfairness claim. As Wyndham did not request and we did not grant interlocutory appeal on this issue, we decline to address it.

[2] In addition to Wyndham Worldwide, the defendant entities are Wyndham Hotel Group, LLC, Wyndham Hotels and Resorts, LCC, and Wyndham Hotel Management, Inc. For convenience, we refer to all defendants jointly as Wyndham.

The FTC alleges that, at least since April 2008, Wyndham engaged in unfair cybersecurity practices that, "taken together, unreasonably and unnecessarily exposed consumers' personal data to unauthorized access and theft." *Id.* at ¶ 24. This claim is fleshed out as follows.

1. The company allowed Wyndham-branded hotels to store payment card information in clear readable text.

2. Wyndham allowed the use of easily guessed passwords to access the property management systems. For example, to gain "remote access to at least one hotel's system," which was developed by Micros Systems, Inc., the user ID and password were both "micros." *Id.* at ¶ 24(f).

3. Wyndham failed to use "readily available security measures"—such as firewalls—to "limit access between [the] hotels' property management systems, . . . corporate network, and the Internet." *Id.* at ¶ 24(a).

4. Wyndham allowed hotel property management systems to connect to its network without taking appropriate cybersecurity precautions. It did not ensure that the hotels implemented "adequate information security policies and procedures." *Id.* at ¶ 24(c). Also, it knowingly allowed at least one hotel to connect to the Wyndham network with an out-of-date operating system that had not received a security update in over three years. It allowed hotel servers to connect to Wyndham's network even though "default user IDs and passwords were enabled . . . , which were easily available to hackers through simple Internet searches." *Id.* And, because it failed to maintain an "adequate[] inventory [of] computers connected to [Wyndham's] network [to] manage the devices," it was unable to identify the source of at least one of the cybersecurity attacks. *Id.* at ¶ 24(g).

5. Wyndham failed to "adequately restrict" the access of third-party vendors to its network and the servers of Wyndham-branded hotels. *Id.* at ¶ 24(j). For example, it did not "restrict[] connections to specified IP addresses or grant[] temporary, limited access, as necessary." *Id.*

6. It failed to employ "reasonable measures to detect and prevent unauthorized access" to its computer network or to "conduct security investigations." *Id.* at ¶ 24(h).

7. It did not follow "proper incident response procedures." *Id.* at ¶ 24(i). The hackers used similar methods in each attack, and yet Wyndham failed to monitor its network for malware used in the previous intrusions.

Although not before us on appeal, the complaint also raises a deception claim, alleging that since 2008 Wyndham has published a privacy policy on its website that overstates the company's cybersecurity.

> We safeguard our Customers' personally identifiable information by using industry standard practices. Although "guaranteed security" does not exist either on or off the Internet, we make commercially reasonable efforts to make our collection of such [i]nformation consistent with all applicable laws and regulations. Currently, our Web sites utilize a variety of different security measures designed to protect personally identifiable information from unauthorized access by users both inside and outside of our company, including the use of 128-bit encryption based on a Class 3 Digital Certificate issued by Verisign Inc. This allows for utilization of Secure Sockets Layer, which is a method for

> encrypting data. This protects confidential information—such as credit card numbers, online forms, and financial data—from loss, misuse, interception and hacking. We take commercially reasonable efforts to create and maintain "fire walls" and other appropriate safeguards . . . .

Id. at ¶ 21. The FTC alleges that, contrary to this policy, Wyndham did not use encryption, firewalls, and other commercially reasonable methods for protecting consumer data.

B. The Three Cybersecurity Attacks

As noted, on three occasions in 2008 and 2009 hackers accessed Wyndham's network and the property management systems of Wyndham-branded hotels. In April 2008, hackers first broke into the local network of a hotel in Phoenix, Arizona, which was connected to Wyndham's network and the Internet. They then used the brute-force method—repeatedly guessing users' login IDs and passwords—to access an administrator account on Wyndham's network. This enabled them to obtain consumer data on computers throughout the network. In total, the hackers obtained unencrypted information for over 500,000 accounts, which they sent to a domain in Russia.

In March 2009, hackers attacked again, this time by accessing Wyndham's network through an administrative account. The FTC claims that Wyndham was unaware of the attack for two months until consumers filed complaints about fraudulent charges. Wyndham then discovered "memory-scraping malware" used in the previous attack on more than thirty hotels' computer systems. *Id.* at ¶ 34. The FTC asserts that, due to Wyndham's "failure to monitor [the network] for

the malware used in the previous attack, hackers had unauthorized access to [its] network for approximately two months." *Id.* In this second attack, the hackers obtained unencrypted payment card information for approximately 50,000 consumers from the property management systems of 39 hotels.

Hackers in late 2009 breached Wyndham's cybersecurity a third time by accessing an administrator account on one of its networks. Because Wyndham "had still not adequately limited access between . . . the Wyndham-branded hotels' property management systems, [Wyndham's network], and the Internet," the hackers had access to the property management servers of multiple hotels. *Id.* at ¶ 37. Wyndham only learned of the intrusion in January 2010 when a credit card company received complaints from cardholders. In this third attack, hackers obtained payment card information for approximately 69,000 customers from the property management systems of 28 hotels.

The FTC alleges that, in total, the hackers obtained payment card information from over 619,000 consumers, which (as noted) resulted in at least $10.6 million in fraud loss. It further states that consumers suffered financial injury through "unreimbursed fraudulent charges, increased costs, and lost access to funds or credit," *Id.* at ¶ 40, and that they "expended time and money resolving fraudulent charges and mitigating subsequent harm." *Id.*

C. Procedural History

The FTC filed suit in the U.S. District Court for the District of Arizona in June 2012 claiming that Wyndham engaged in "unfair" and "deceptive" practices in violation of § 45(a). At Wyndham's request, the Court transferred the case to the U.S. District Court for the District of New Jersey.

Wyndham then filed a Rule 12(b)(6) motion to dismiss both the unfair practice and deceptive practice claims. The District Court denied the motion but certified its decision on the unfairness claim for interlocutory appeal. We granted Wyndham's application for appeal.

II. Jurisdiction and Standards of Review

The District Court has subject-matter jurisdiction under 28 U.S.C. §§ 1331, 1337(a), and 1345. We have jurisdiction under 28 U.S.C. § 1292(b).

We have plenary review of a district court's ruling on a motion to dismiss for failure to state a claim under Rule 12(b)(6). *Farber v. City of Paterson*, 440 F.3d 131, 134 (3d Cir. 2006). In this review, "we accept all factual allegations as true, construe the complaint in the light most favorable to the plaintiff, and determine whether, under any reasonable reading of the complaint, the plaintiff may be entitled to relief." *Pinker v. Roche Holdings Ltd.*, 292 F.3d 361, 374 n.7 (3d Cir. 2002).

III. FTC's Regulatory Authority Under § 45(a)

A. Legal Background

The Federal Trade Commission Act of 1914 prohibited "unfair methods of competition in commerce." Pub. L. No. 63-203, § 5, 38 Stat. 717, 719 (codified as amended at 15 U.S.C. § 45(a)). Congress "explicitly considered, and rejected, the notion that it reduce the ambiguity of the phrase 'unfair methods of competition' . . . by enumerating the particular practices to which it was intended to apply." *FTC v. Sperry & Hutchinson Co.*, 405 U.S. 233, 239–40 (1972) (citing S. Rep. No. 63-597, at 13 (1914)); *see also* S. Rep. No. 63-597, at 13 ("The committee gave *careful consideration* to

the question as to whether it would attempt to define the many and variable unfair practices which prevail in commerce . . . . It concluded that . . . there were too many unfair practices to define, and after writing 20 of them into the law it would be quite possible to invent others." (emphasis added)). The takeaway is that Congress designed the term as a "flexible concept with evolving content," *FTC v. Bunte Bros.*, 312 U.S. 349, 353 (1941), and "intentionally left [its] development . . . to the Commission," *Atl. Ref. Co. v. FTC*, 381 U.S. 357, 367 (1965).

After several early cases limited "unfair methods of competition" to practices harming competitors and not consumers, *see, e.g.*, *FTC v. Raladam Co.*, 283 U.S. 643 (1931), Congress inserted an additional prohibition in § 45(a) against "unfair or deceptive acts or practices in or affecting commerce," Wheeler-Lea Act, Pub. L. No. 75-447, § 5, 52 Stat. 111, 111 (1938).

For the next few decades, the FTC interpreted the unfair-practices prong primarily through agency adjudication. But in 1964 it issued a "Statement of Basis and Purpose" for unfair or deceptive advertising and labeling of cigarettes, 29 Fed. Reg. 8324, 8355 (July 2, 1964), which explained that the following three factors governed unfairness determinations:

> (1) whether the practice, without necessarily having been previously considered unlawful, offends public policy as it has been established by statutes, the common law, or otherwise—whether, in other words, it is within at least the penumbra of some common-law, statutory or other established concept of unfairness; (2) whether it is immoral, unethical, oppressive, or unscrupulous; [and] (3) whether it causes

> substantial injury to consumers (or competitors or other businessmen).

Id. Almost a decade later, the Supreme Court implicitly approved these factors, apparently acknowledging their applicability to contexts other than cigarette advertising and labeling. *Sperry*, 405 U.S. at 244 n.5. The Court also held that, under the policy statement, the FTC could deem a practice unfair based on the third prong—substantial consumer injury—without finding that at least one of the other two prongs was also satisfied. *Id.*

During the 1970s, the FTC embarked on a controversial campaign to regulate children's advertising through the unfair-practices prong of § 45(a). At the request of Congress, the FTC issued a second policy statement in 1980 that clarified the three factors. FTC Unfairness Policy Statement, Letter from the FTC to Hon. Wendell Ford and Hon. John Danforth, Senate Comm. on Commerce, Sci., and Transp. (Dec. 17, 1980), *appended to Int'l Harvester Co.*, 104 F.T.C. 949, 1070 (1984) [hereinafter 1980 Policy Statement]. It explained that public policy considerations are relevant in determining whether a particular practice causes substantial consumer injury. *Id.* at 1074–76. Next, it "abandoned" the "theory of immoral or unscrupulous conduct . . . altogether" as an "independent" basis for an unfairness claim. *Int'l Harvester Co.*, 104 F.T.C. at 1061 n.43; 1980 Policy Statement, *supra* at 1076 ("The Commission has . . . never relied on [this factor] as an independent basis for a finding of unfairness, and it will act in the future only on the basis of the [other] two."). And finally, the Commission explained that "[u]njustified consumer injury is the primary focus of the FTC Act" and that such an injury "[b]y itself . . . can be sufficient to warrant a finding of unfairness." 1980 Policy Statement, *supra* at 1073. This "does not mean that every consumer injury is legally 'unfair.'" *Id.* Indeed,

> [t]o justify a finding of unfairness the injury must satisfy three tests. [1] It must be substantial; [2] it must not be outweighed by any countervailing benefits to consumers or competition that the practice produces; and [3] it must be an injury that consumers themselves could not reasonably have avoided.

Id.

In 1994, Congress codified the 1980 Policy Statement at 15 U.S.C. § 45(n):

> The Commission shall have no authority under this section . . . to declare unlawful an act or practice on the grounds that such act or practice is unfair 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. In determining whether an act or practice is unfair, the Commission may consider established public policies as evidence to be considered with all other evidence. Such public policy considerations may not serve as a primary basis for such determination.

FTC Act Amendments of 1994, Pub. L. No. 103-312, § 9, 108 Stat. 1691, 1695. Like the 1980 Policy Statement, § 45(n) requires substantial injury that is not reasonably avoidable by consumers and that is not outweighed by the benefits to consumers or competition. It also acknowledges the potential significance of public policy and does not expressly require that an unfair practice be immoral, unethical, unscrupulous, or oppressive.

B. Plain Meaning of Unfairness

Wyndham argues (for the first time on appeal) that the three requirements of 15 U.S.C. § 45(n) are necessary but insufficient conditions of an unfair practice and that the plain meaning of the word "unfair" imposes independent requirements that are not met here. Arguably, § 45(n) may not identify all of the requirements for an unfairness claim. (While the provision forbids the FTC from declaring an act unfair "unless" the act satisfies the three specified requirements, it does not answer whether these are the *only* requirements for a finding of unfairness.) Even if so, some of Wyndham's proposed requirements are unpersuasive, and the rest are satisfied by the allegations in the FTC's complaint.

First, citing *FTC v. R.F. Keppel & Brother, Inc.*, 291 U.S. 304 (1934), Wyndham argues that conduct is only unfair when it injures consumers "through unscrupulous or unethical behavior." Wyndham Br. at 20–21. But *Keppel* nowhere says that unfair conduct must be unscrupulous or unethical. Moreover, in *Sperry* the Supreme Court rejected the view that the FTC's 1964 policy statement required unfair conduct to be "unscrupulous" or "unethical." 405 U.S. at 244 n.5.[3]

[3] *Id.* ("[Petitioner] argues that . . . [the 1964 statement] commits the FTC to the view that misconduct in respect of the third of these criteria is not subject to constraint as 'unfair' absent a concomitant showing of misconduct according to the first or second of these criteria. But all the FTC said in the [1964] statement . . . was that '[t]he wide variety of decisions interpreting the elusive concept of unfairness *at least* makes clear that a method of selling violates Section 5 if it is exploitive or inequitable and if, in addition to being morally objectionable, it is seriously

Wyndham points to no subsequent FTC policy statements, adjudications, judicial opinions, or statutes that would suggest any change since *Sperry*.

Next, citing one dictionary, Wyndham argues that a practice is only "unfair" if it is "not equitable" or is "marked by injustice, partiality, or deception." Wyndham Br. at 18–19 (citing *Webster's Ninth New Collegiate Dictionary* (1988)). Whether these are requirements of an unfairness claim makes little difference here. A company does not act equitably when it publishes a privacy policy to attract customers who are concerned about data privacy, fails to make good on that promise by investing inadequate resources in cybersecurity, exposes its unsuspecting customers to substantial financial injury, and retains the profits of their business.

We recognize this analysis of unfairness encompasses some facts relevant to the FTC's deceptive practices claim. But facts relevant to unfairness and deception claims frequently overlap. *See, e.g.*, *Am. Fin. Servs. Ass'n v. FTC*, 767 F.2d 957, 980 n.27 (D.C. Cir. 1985) ("The FTC has determined that . . . making unsubstantiated advertising claims may be both an unfair and a deceptive practice."); *Orkin Exterminating Co. v. FTC*, 849 F.2d 1354, 1367 (11th Cir. 1988) ("[A] practice may be both deceptive and unfair . . . ."). [4] We cannot completely disentangle the two

---

detrimental to consumers or others.'" (emphasis and some alterations in original, citation omitted)).

[4] The FTC has on occasion described deception as a subset of unfairness. *See Int'l Harvester Co.*, 104 F.T.C. at 1060 ("The Commission's unfairness jurisdiction provides a more general basis for action against acts or practices which cause significant consumer injury. This part of our jurisdiction is

theories here. The FTC argued in the District Court that consumers could not reasonably avoid injury by booking with another hotel chain because Wyndham had published a

---

broader than that involving deception, and the standards for its exercise are correspondingly more stringent . . . . [U]nfairness is the set of general principles of which deception is a particularly well-established and streamlined subset."); *Figgie Int'l*, 107 F.T.C. 313, 373 n.5 (1986) ("[U]nfair practices are not always deceptive but deceptive practices are always unfair."); *Orkin Exterminating Co.*, 108 F.T.C. 263, 363 n.78 (1986). So have several FTC staff members. *See, e.g.*, J. Howard Beales, Director of the Bureau of Consumer Protection, FTC, Marketing and Public Policy Conference, The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection (May 30, 2003) ("Although, in the past, they have sometimes been viewed as mutually exclusive legal theories, Commission precedent incorporated in the statutory codification makes clear that deception is properly viewed as a subset of unfairness."); Neil W. Averitt, *The Meaning of "Unfair Acts or Practices" in Section 5 of the Federal Trade Commission Act*, 70 Geo. L.J. 225, 265–66 (1981) ("Although deception is generally regarded as a separate aspect of section 5, in its underlying rationale it is really just one specific form of unfair consumer practice . . . . [For example, the] Commission has held that it is deceptive for a merchant to make an advertising claim for which he lacks a reasonable basis, regardless of whether the claim is eventually proven true or false . . . . Precisely because unsubstantiated ads are deceptive in this manner, . . . they also affect the exercise of consumer sovereignty and thus constitute an unfair act or practice.").

misleading privacy policy that overstated its cybersecurity. Plaintiff's Response in Opposition to the Motion to Dismiss by Defendant at 5, *FTC v. Wyndham Worldwide Corp.*, 10 F. Supp. 3d 602 (D.N.J. 2014) (No. 13-1887) ("Consumers could not take steps to avoid Wyndham's unreasonable data security [before providing their personal information] because Wyndham falsely told consumers that it followed 'industry standard practices.'"); *see* JA 203 ("On the reasonabl[y] avoidable part, . . . consumers certainly would not have known that Wyndham had unreasonable data security practices in this case . . . . We also allege that in [Wyndham's] privacy policy they deceive consumers by saying we do have reasonable security data practices. That is one way consumers couldn't possibly have avoided providing a credit card to a company."). Wyndham did not challenge this argument in the District Court nor does it do so now. If Wyndham's conduct satisfies the reasonably avoidable requirement at least partially because of its privacy policy—an inference we find plausible at this stage of the litigation—then the policy is directly relevant to whether Wyndham's conduct was unfair.[5]

Continuing on, Wyndham asserts that a business "does not treat its customers in an 'unfair' manner when the business *itself* is victimized by criminals." Wyndham Br. at

---

[5] No doubt there is an argument that consumers could not reasonably avoid injury even absent the misleading privacy policy. *See, e.g.*, James P. Nehf, *Shopping for Privacy Online: Consumer Decision-Making Strategies and the Emerging Market for Information Privacy*, 2005 U. Ill. J.L. Tech. & Pol'y. 1 (arguing that consumers may care about data privacy, but be unable to consider it when making credit card purchases). We have no occasion to reach this question, as the parties have not raised it.

21 (emphasis in original). It offers no reasoning or authority for this principle, and we can think of none ourselves. Although unfairness claims "usually involve actual and completed harms," *Int'l Harvester*, 104 F.T.C. at 1061, "they may also be brought on the basis of likely rather than actual injury," *id.* at 1061 n.45. And the FTC Act expressly contemplates the possibility that conduct can be unfair before actual injury occurs. 15 U.S.C. § 45(n) ("[An unfair act or practice] causes or is *likely to cause* substantial injury" (emphasis added)). More importantly, that a company's conduct was not *the most* proximate cause of an injury generally does not immunize liability from foreseeable harms. *See* Restatement (Second) of Torts § 449 (1965) ("If the likelihood that a third person may act in a particular manner is the hazard or one of the hazards which makes the actor negligent, such an act[,] whether innocent, negligent, intentionally tortious, or criminal[,] does not prevent the actor from being liable for harm caused thereby."); *Westfarm Assocs. v. Wash. Suburban Sanitary Comm'n*, 66 F.3d 669, 688 (4th Cir. 1995) ("Proximate cause may be found even where the conduct of the third party is . . . criminal, so long as the conduct was facilitated by the first party and reasonably foreseeable, and some ultimate harm was reasonably foreseeable."). For good reason, Wyndham does not argue that the cybersecurity intrusions were unforeseeable. That would be particularly implausible as to the second and third attacks.

Finally, Wyndham posits a *reductio ad absurdum*, arguing that if the FTC's unfairness authority extends to Wyndham's conduct, then the FTC also has the authority to "regulate the locks on hotel room doors, . . . to require every store in the land to post an armed guard at the door," Wyndham Br. at 23, and to sue supermarkets that are "sloppy about sweeping up banana peels," Wyndham Reply Br. at 6. The argument is alarmist to say the least. And it invites the

tart retort that, were Wyndham a supermarket, leaving so many banana peels all over the place that 619,000 customers fall hardly suggests it should be immune from liability under § 45(a).

We are therefore not persuaded by Wyndham's arguments that the alleged conduct falls outside the plain meaning of "unfair."

C. Subsequent Congressional Action

Wyndham next argues that, even if cybersecurity were covered by § 45(a) as initially enacted, three legislative acts since the subsection was amended in 1938 have reshaped the provision's meaning to exclude cybersecurity. A recent amendment to the Fair Credit Reporting Act directed the FTC and other agencies to develop regulations for the proper disposal of consumer data. *See* Pub. L. No. 108-159, § 216(a), 117 Stat. 1952, 1985–86 (2003) (codified as amended at 15 U.S.C. § 1681w). The Gramm-Leach-Bliley Act required the FTC to establish standards for financial institutions to protect consumers' personal information. *See* Pub. L. No. 106-102, § 501(b), 113 Stat. 1338, 1436–37 (1999) (codified as amended at 15 U.S.C. § 6801(b)). And the Children's Online Privacy Protection Act ordered the FTC to promulgate regulations requiring children's websites, among other things, to provide notice of "what information is collected from children . . . , how the operator uses such information, and the operator's disclosure practices for such information." Pub. L. No. 105-277, § 1303, 112 Stat. 2681, 2681-730–732 (1998) (codified as amended at 15 U.S.C. § 6502).[6] Wyndham contends these "tailored grants of

[6] Wyndham also points to a variety of cybersecurity bills that Congress has considered and not passed. "[S]ubsequent legislative history . . . is particularly dangerous ground on

substantive authority to the FTC in the cybersecurity field would be inexplicable if the Commission already had general substantive authority over this field." Wyndham Br. at 25. Citing *FDA v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120, 143 (2000), Wyndham concludes that Congress excluded cybersecurity from the FTC's unfairness authority by enacting these measures.

We are not persuaded. The inference to congressional intent based on post-enactment legislative activity in *Brown & Williamson* was far stronger. There, the Food and Drug Administration had repeatedly disclaimed regulatory authority over tobacco products for decades. *Id.* at 144. During that period, Congress enacted six statutes regulating tobacco. *Id.* at 143–44. The FDA later shifted its position, claiming authority over tobacco products. The Supreme Court held that Congress excluded tobacco-related products from the FDA's authority in enacting the statutes. As tobacco products would necessarily be banned if subject to the FDA's regulatory authority, any interpretation to the contrary would contradict congressional intent to regulate rather than ban tobacco products outright. *Id.* 137–39; *Massachusetts v. EPA*, 549 U.S. 497, 530–31 (2007). Wyndham does not argue that recent privacy laws *contradict* reading corporate cybersecurity into § 45(a). Instead, it merely asserts that Congress had no reason to enact them if the FTC could already regulate cybersecurity through that provision. Wyndham Br. at 25–26.

We disagree that Congress lacked reason to pass the recent legislation if the FTC already had regulatory authority over some cybersecurity issues. The Fair Credit Reporting

---

which to rest an interpretation of a prior statute when it concerns . . . a proposal that does not become law." *Pension Benefit Guar. Corp. v. LTV Corp.*, 496 U.S. 633, 650 (1990).

Act requires (rather than authorizes) the FTC to issue regulations, 15 U.S.C. § 1681w ("The Federal Trade Commission . . . *shall* issue final regulations requiring . . . ." (emphasis added)); *id.* § 1681m(e)(1)(B) ("The [FTC and other agencies] *shall* jointly . . . prescribe regulations requiring each financial institution . . . ." (emphasis added)), and expands the scope of the FTC's authority, *id.* § 1681s(a)(1) ("[A] violation of any requirement or prohibition imposed under this subchapter shall constitute an unfair or deceptive act or practice in commerce . . . and shall be subject to enforcement by the [FTC] . . . irrespective of whether that person is engaged in commerce or meets any other jurisdictional tests under the [FTC] Act."). The Gramm-Leach-Bliley Act similarly requires the FTC to promulgate regulations, *id.* § 6801(b) ("[The FTC] shall establish appropriate standards for the financial institutions subject to [its] jurisdiction . . . ."), and relieves some of the burdensome § 45(n) requirements for declaring acts unfair, *id.* § 6801(b) ("[The FTC] shall establish appropriate standards . . . to protect against unauthorized access to or use of . . . records . . . which could result in substantial harm *or inconvenience to any customer*." (emphasis added)). And the Children's Online Privacy Protection Act required the FTC to issue regulations and empowered it to do so under the procedures of the Administrative Procedure Act, *id.* § 6502(b) (citing 5 U.S.C. § 553), rather than the more burdensome Magnuson-Moss procedures under which the FTC must usually issue regulations, 15 U.S.C. § 57a. Thus none of the recent privacy legislation was "inexplicable" if the FTC already had some authority to regulate corporate cybersecurity through § 45(a).

Next, Wyndham claims that the FTC's interpretation of § 45(a) is "inconsistent with its repeated efforts to obtain from Congress the very authority it purports to wield here." Wyndham Br. at 28. Yet again we disagree. In two of the

statements cited by Wyndham, the FTC clearly said that some cybersecurity practices are "unfair" under the statute. *See Consumer Data Protection: Hearing Before the Subcomm. on Commerce, Mfg. & Trade of the H. Comm. on Energy & Commerce*, 2011 WL 2358081, at *6 (June 15, 2011) (statement of Edith Ramirez, Comm'r, FTC) ("[T]he Commission enforces the FTC Act's proscription against unfair . . . acts . . . in cases where a business['s] . . . failure to employ reasonable security measures causes or is likely to cause substantial consumer injury."); *Data Theft Issues: Hearing Before the Subcomm. on Commerce, Mfg. & Trade of the H. Comm. on Energy & Commerce*, 2011 WL 1971214, at *7 (May 4, 2011) (statement of David C. Vladeck, Director, FTC Bureau of Consumer Protection) (same).

In the two other cited statements, given in 1998 and 2000, the FTC only acknowledged that it cannot require companies to adopt "fair information practice policies." *See* FTC, *Privacy Online: Fair Information Practices in the Electronic Marketplace—A Report to Congress* 34 (2000) [hereinafter *Privacy Online*]; *Privacy in Cyberspace: Hearing Before the Subcomm. on Telecomms., Trade & Consumer Prot. of the H. Comm. on Commerce*, 1998 WL 546441 (July 21, 1998) (statement of Robert Pitofsky, Chairman, FTC). These policies would protect consumers from far more than the kind of "substantial injury" typically covered by § 45(a). In addition to imposing some cybersecurity requirements, they would require companies to give notice about what data they collect from consumers, to permit those consumers to decide how the data is used, and to permit them to review and correct inaccuracies. *Privacy Online*, *supra* at 36–37. As the FTC explained in the District Court, the primary concern driving the adoption of these policies in the late 1990s was that "companies . . . were capable of *collecting* enormous amounts of information about consumers, and people were suddenly realizing this." JA 106 (emphasis added). The FTC

thus could not require companies to adopt broad fair information practice policies because they were "just collecting th[e] information, and consumers [were not] injured." *Id.*; *see also* Order Denying Respondent LabMD's Motion to Dismiss, No. 9357, slip op. at 7 (Jan. 16, 2014) [hereinafter *LabMD Order* or *LabMD*] ("[T]he sentences from the 1998 and 2000 reports . . . simply recognize that the Commission's existing authority may not be sufficient to effectively protect consumers with regard to *all* data privacy issues of potential concern (such as aspects of children's online privacy) . . . ." (emphasis in original)). Our conclusion is this: that the FTC later brought unfairness actions against companies whose inadequate cybersecurity resulted in consumer harm is not inconsistent with the agency's earlier position.

Having rejected Wyndham's arguments that its conduct cannot be unfair, we assume for the remainder of this opinion that it was.

IV. Fair Notice

A conviction or punishment violates the Due Process Clause of our Constitution if the statute or regulation under which it is obtained "fails to provide a person of ordinary intelligence fair notice of what is prohibited, or is so standardless that it authorizes or encourages seriously discriminatory enforcement." *FCC v. Fox Television Stations, Inc.*, 132 S. Ct. 2307, 2317 (2012) (internal quotation marks omitted). Wyndham claims that, notwithstanding whether its conduct was unfair under § 45(a),

the FTC failed to give fair notice of the specific cybersecurity standards the company was required to follow.[7]

A. Legal Standard

The level of required notice for a person to be subject to liability varies by circumstance. In *Bouie v. City of Columbia*, the Supreme Court held that a "judicial construction of a criminal statute" violates due process if it is "unexpected and indefensible by reference to the law which had been expressed prior to the conduct in issue." 378 U.S. 347, 354 (1964) (internal quotation marks omitted); *see also Rogers v. Tennessee*, 532 U.S. 451, 457 (2001); *In re Surrick*, 338 F.3d 224, 233–34 (3d Cir. 2003). The precise meaning of "unexpected and indefensible" is not entirely clear, *United States v. Lata*, 415 F.3d 107, 111 (1st Cir. 2005), but we and our sister circuits frequently use language implying that a conviction violates due process if the defendant could not reasonably foresee that a court might adopt the new interpretation of the statute.[8]

---

[7] We do not read Wyndham's briefing as raising a meaningful argument under the "discriminatory enforcement" prong. A few sentences in a reply brief are not enough. *See* Wyndham Reply Br. at 26 ("To provide the notice required by due process, a statement must in some sense declare what conduct the law proscribes and thereby constrain enforcement discretion . . . . Here, the consent decrees at issue . . . do not limit the Commission's enforcement authority in any way." (citation omitted)).

[8] *See Ortiz v. N.Y.S. Parole*, 586 F.3d 149, 159 (2d Cir. 2009) (holding that the "unexpected and indefensible" standard "requires only that the law . . . not lull the potential defendant

The fair notice doctrine extends to civil cases, particularly where a penalty is imposed. *See Fox Television Stations, Inc.*, 132 S. Ct. at 2317–20; *Boutilier v. INS*, 387 U.S. 118, 123 (1967). "Lesser degrees of specificity" are allowed in civil cases because the consequences are smaller than in the criminal context. *San Filippo v. Bongiovanni*, 961 F.2d 1125, 1135 (3d Cir. 1992). The standards are especially lax for civil statutes that regulate economic activities. For those statutes, a party lacks fair notice when the relevant standard is "so vague as to be no rule or standard at all."

---

into a *false sense of security*, giving him *no reason even to suspect* that his conduct *might* be within its scope." (emphases added)); *In re Surrick*, 338 F.3d at 234 ("[We] reject [the] contention that . . . nothing in the history of [the relevant provision] had stated *or even foreshadowed* that reckless conduct *could* violate it. Indeed, in view of the foregoing, the [state court's] decision . . . was neither 'unexpected' nor 'indefensible' by reference to the law which had been expressed prior to the conduct in issue." (emphases added)); *Warner v. Zent*, 997 F.2d 116, 125 (6th Cir. 1993) ("'The underlying principle is that no man shall be held criminally responsible for conduct which *he could not reasonably understand* to be proscribed.'" (emphasis added) (quoting *United States v. Harriss*, 347 U.S. 612, 617 (1954)); *id.* at 127 ("It was *by no means unforeseeable* . . . that the [court] would [construe the statute as it did]." (emphasis added)); *see also Lata*, 415 F.3d at 112 ("[S]omeone in [the defendant's] position *could not reasonably be surprised* by the sentence he eventually received . . . . We reserve for the future the case . . . in which a sentence is imposed . . . that is *higher than any that might realistically have been imagined* at the time of the crime . . . ." (emphases added)).

CMR D.N. Corp. v. City of Phila., 703 F.3d 612, 631–32 (3d Cir. 2013) (internal quotation marks omitted).[9]

A different set of considerations is implicated when agencies are involved in statutory or regulatory interpretation. Broadly speaking, agencies interpret in at least three contexts. One is where an agency administers a statute without any special authority to create new rights or obligations. When disputes arise under this kind of agency interpretation, the courts give respect to the agency's view to the extent it is persuasive, but they retain the primary responsibility for construing the statute.[10] As such, the

---

[9] *See also Bongiovanni*, 961 F.2d at 1138; *Boutilier*, 387 U.S. at 123; *Leib v. Hillsborough Cnty. Pub. Transp. Comm'n*, 558 F.3d 1301, 1310 (11th Cir. 2009); *Ford Motor Co. v. Tex. Dep't of Transp.*, 264 F.3d 493, 507 (5th Cir. 2001); *Columbia Nat'l Res., Inc. v. Tatum*, 58 F.3d 1101, 1108 (6th Cir. 1995).

[10] *See Skidmore v. Swift & Co.*, 323 U.S. 134, 140 (1944) ("[The agency interpretation is] not controlling upon the courts by reason of [its] authority [but is a] body of experience and informed judgment to which courts . . . may properly resort for guidance."); *Christenson v. Harris Cnty.*, 529 U.S. 576, 587 (2000) ("[Agency interpretations are] entitled to respect under [*Skidmore*], but only to the extent that [they] have the power to persuade." (internal quotation marks omitted)); *see also* Peter L. Strauss, *"Deference" is Too Confusing—Let's Call Them "*Chevron *Space" and "*Skidmore *Weight"*, 112 Colum. L. Rev. 1143, 1147 (2012) ("*Skidmore* . . . is grounded in a construct of the agency as responsible expert, arguably possessing special knowledge of

standard of notice afforded to litigants about the meaning of the statute is not dissimilar to the standard of notice for civil statutes generally because the court, not the agency, is the ultimate arbiter of the statute's meaning.

The second context is where an agency exercises its authority to fill gaps in a statutory scheme. There the agency is primarily responsible for interpreting the statute because the courts must defer to any reasonable construction it adopts. *See Chevron, U.S.A., Inc. v. Natural Res. Def. Council, Inc.*, 467 U.S. 837 (1984). Courts appear to apply a more stringent standard of notice to civil regulations than civil statutes: parties are entitled to have "ascertainable certainty" of what conduct is legally required by the regulation. *See Chem. Waste Mgmt., Inc. v. EPA*, 976 F.2d 2, 29 (D.C. Cir. 1992) (*per curiam*) (denying petitioners' challenge that a recently promulgated EPA regulation fails fair notice principles); *Nat'l Oilseed Processors Ass'n. v. OSHA*, 769 F.3d 1173, 1183–84 (D.C. Cir. 2014) (denying petitioners' challenge that a recently promulgated OSHA regulation fails fair notice principles).

The third context is where an agency interprets the meaning of its own regulation. Here also courts typically must defer to the agency's reasonable interpretation.[11] We

---

the statutory meaning a court should consider in *reaching its own judgment*." (emphasis added)).

[11] *See Auer v. Robbins*, 519 U.S. 452, 461 (1997) ("Because the salary-basis test is a creature of the Secretary's own regulations, his interpretation of it is . . . controlling unless plainly erroneous or inconsistent with the regulation." (internal quotation marks omitted)); *Decker v. Nw. Envtl. Def. Ctr.*, 133 S. Ct. 1326, 1337 (2013) ("When an agency

and several of our sister circuits have stated that private parties are entitled to know with "ascertainable certainty" an agency's interpretation of its regulation. *Sec'y of Labor v. Beverly Healthcare-Hillview*, 541 F.3d 193, 202 (3d Cir. 2008); *Dravo Corp. v. Occupational Safety & Health Rev. Comm'n*, 613 F.2d 1227, 1232–33 (3d Cir. 1980).[12] Indeed,

---

interprets its own regulation, the Court, as a general rule, defers to it unless that interpretation is plainly erroneous or inconsistent with the regulation." (internal quotation marks omitted)); *Martin v. Occupational Safety & Health Rev. Comm'n*, 499 U.S. 144, 150–51 (1991) ("In situations in which the meaning of [regulatory] language is not free from doubt, the reviewing court should give effect to the agency's interpretation so long as it is reasonable." (alterations in original, internal quotations omitted)); *Columbia Gas Transp., LLC v. 1.01 Acres, More or Less in Penn Twp.*, 768 F.3d 300, 313 (3d Cir. 2014) ("[A]s an agency interpretation of its own regulation, it is deserving of deference." (citing *Decker*)).

[12] *See also Wis. Res. Prot. Council v. Flambeau Mining Co.*, 727 F.3d 700, 708 (7th Cir. 2013); *AJP Const., Inc. v. Sec'y of Labor*, 357 F.3d 70, 75–76 (D.C. Cir. 2004) (quoting *Gen. Elec. Co. v. EPA*, 53 F.3d 1324, 1329 (D.C. Cir. 1995)); *Tex. Mun. Power Agency v. EPA*, 89 F.3d 858, 872 (D.C. Cir. 1996); *Ga. Pac. Corp. v. Occupational Safety & Health Rev. Comm'n*, 25 F.3d 999, 1005 (11th Cir. 1994); *Diamond Roofing Co. v. Occupational Safety & Health Rev. Comm'n*, 528 F.2d 645, 649 (5th Cir. 1976). In fact, the Supreme Court applied *Skidmore* to an interpretation by an agency of a regulation it adopted instead of deferring to that interpretation because the latter would have "seriously undermine[d] the principle that agencies should provide regulated parties fair

"the due process clause prevents . . . deference from validating the application of a regulation that fails to give fair warning of the conduct it prohibits or requires." *AJP Const., Inc.*, 357 F.3d at 75 (internal quotation marks omitted).

A higher standard of fair notice applies in the second and third contexts than in the typical civil statutory interpretation case because agencies engage in interpretation differently than courts. *See* Frank H. Easterbook, *Judicial Discretion in Statutory Interpretation*, 57 Okla. L. Rev. 1, 3 (2004) ("A judge who announces deference is approving a shift in interpretive method, not just a shift in the identity of the decider, as if a suit were being transferred to a court in a different venue."). In resolving ambiguity in statutes or regulations, courts generally adopt the *best* or *most reasonable* interpretation. But, as the agency is often free to adopt *any reasonable construction*, it may impose higher legal obligations than required by the best interpretation.[13]

---

warning of the conduct [a regulation] prohibits or requires." *Christopher v. SmithKline Beecham Corp.*, 132 S. Ct. 2156, 2167 & n.15 (2012) (second alteration in original, internal quotation marks omitted) (citing *Dravo*, 613 F.2d at 1232–33 and the "ascertainable certainty" standard).

[13] *See Nat'l Cable & Telecomms. Ass'n v. Brand X Internet Servs.*, 545 U.S. 967, 980 (2005) ("If a statute is ambiguous, and if the implementing agency's construction is reasonable, *Chevron* requires a federal court to accept the agency's construction of the statute, even if the agency's reading differs from what the court believes is the best statutory interpretation."); *Decker*, 133 S. Ct. at 1337 ("It is well established that an agency's interpretation need not be the only possible reading of a regulation—or even the best one—

Furthermore, courts generally resolve statutory ambiguity by applying traditional methods of construction. Private parties can reliably predict the court's interpretation by applying the same methods. In contrast, an agency may also rely on technical expertise and political values.[14] It is harder to predict how an agency will construe a statute or regulation at some unspecified point in the future, particularly when that interpretation will depend on the "political views of

---

to prevail. When an agency interprets its own regulation, the Court, as a general rule, defers to it unless that interpretation is plainly erroneous or inconsistent with the regulation." (internal quotation marks omitted)); *Auer*, 519 U.S. at 462–63 ("[The rule that Fair Labor Standards Act] exemptions are to be narrowly construed against . . . employers . . . is a rule governing judicial interpretation of statutes and regulations, not a limitation on the Secretary's power to resolve ambiguities in his own regulations. A rule requiring the Secretary to construe his own regulations narrowly would make little sense, since he is free to write the regulations as broadly as he wishes, subject only to the limits imposed by the statute." (internal quotation marks omitted)).

[14] *See Garfias-Rodriguez v. Holder*, 702 F.3d 504, 518 (9th Cir. 2012) (rejecting the applicability of the judicial retroactivity test to a new Board of Immigration Appeals' interpretation because the "decision fill[ed] a statutory gap and [was] an exercise [of the agency's] policymaking function"); Easterbrook, *supra* at 3 ("Judges in their own work forswear the methods that agencies employ" to interpret statutes, which include relying on "political pressure, the President's view of happy outcomes, cost-benefit studies . . . and the other tools of policy wonks . . . .").

the President in office at [that] time." Strauss, *supra* at 1147.[15]

Wyndham argues it was entitled to "ascertainable certainty" of the FTC's interpretation of what specific cybersecurity practices are required by § 45(a). Yet it has contended repeatedly—no less than seven separate occasions in *this* case—that there is no FTC rule or adjudication about cybersecurity that merits deference here. The necessary implication, one that Wyndham itself has explicitly drawn on two occasions noted below, is that federal courts are to interpret § 45(a) in the first instance to decide whether Wyndham's conduct was unfair.

Wyndham's argument has focused on the FTC's motion to dismiss order in *LabMD*, an administrative case in which the agency is pursuing an unfairness claim based on allegedly inadequate cybersecurity. *LabMD Order*, *supra*. Wyndham first argued in the District Court that the *LabMD Order* does not merit *Chevron* deference because "self-serving, litigation-driven decisions . . . are entitled to no deference at all" and because the opinion adopted an impermissible construction of the statute. Wyndham's

---

[15] *See also Brand X Internet Servs.*, 545 U.S. at 981 ("[T]he agency . . . must consider varying interpretations and the wisdom of its policy on a continuing basis . . . in response to . . . a change in administrations." (internal quotation marks omitted, first omission in original)); *Motor Vehicle Mfrs. Ass'n of U.S., Inc. v. State Farm Mut. Auto. Ins. Co.*, 463 U.S. 29, 59 (1983) (Rehnquist, J., dissenting in part) ("A change in administration brought about by the people casting their votes is a perfectly reasonable basis for an executive agency's reappraisal of the costs and benefits of its . . . regulations.").

January 29, 2014 Letter at 1–2, *FTC v. Wyndham Worldwide Corp.*, 10 F. Supp. 3d 602 (D.N.J. 2014) (No. 13-1887).

Second, Wyndham switched gears in its opening brief on appeal to us, arguing that *LabMD* does not merit *Chevron* deference because courts owe no deference to an agency's interpretation of the "boundaries of Congress' statutory delegation of authority to the agency." Wyndham Br. at 19–20.

Third, in its reply brief it argued again that *LabMD* does not merit *Chevron* deference because it adopted an impermissible construction of the statute. Wyndham Reply Br. at 14.

Fourth, Wyndham switched gears once more in a Rule 28(j) letter, arguing that *LabMD* does not merit *Chevron* deference because the decision was nonfinal. Wyndham's February 6, 2015 Letter (citing *LabMD, Inc. v. FTC*, 776 F.3d 1275 (11th Cir. 2015)).

Fifth, at oral argument we asked Wyndham whether the FTC has decided that cybersecurity practices are unfair. Counsel answered: "No. I don't think consent decrees count, I don't think the 2007 brochure counts, and I don't think *Chevron* deference applies. So are . . . they asking this federal court in the first instance . . . [?] I think the answer to that question is yes . . . ." Oral Arg. Tr. at 19.

Sixth, due to our continuing confusion about the parties' positions on a number of issues in the case, we asked for supplemental briefing on certain questions, including whether the FTC had declared that cybersecurity practices can be unfair. In response, Wyndham asserted that "the FTC has not declared unreasonable cybersecurity practices 'unfair.'" Wyndham's Supp. Memo. at 3. Wyndham

explained further: "It follows from [our] answer to [that] question that the FTC is asking the federal courts to determine in the first instance that unreasonable cybersecurity practices qualify as 'unfair' trade practices under the FTC Act." *Id.* at 4.

Seventh, and most recently, Wyndham submitted a Rule 28(j) letter arguing that *LabMD* does not merit *Chevron* deference because it decided a question of "deep economic and political significance." Wyndham's June 30, 2015 Letter (quoting *King v. Burwell*, 135 S. Ct. 2480 (2015)).

Wyndham's position is unmistakable: the FTC has not yet declared that cybersecurity practices can be unfair; there is no relevant FTC rule, adjudication or document that merits deference; and the FTC is asking the federal courts to interpret § 45(a) in the first instance to decide whether it prohibits the alleged conduct here. The implication of this position is similarly clear: if the federal courts are to decide whether Wyndham's conduct was unfair in the first instance under the statute without deferring to any FTC interpretation, then this case involves ordinary judicial interpretation of a civil statute, and the ascertainable certainty standard does not apply. The relevant question is not whether Wyndham had fair notice of the *FTC's interpretation* of the statute, but whether Wyndham had fair notice of what the *statute itself* requires.

Indeed, at oral argument we asked Wyndham whether the cases cited in its brief that apply the "ascertainable certainty" standard—all of which involve a court reviewing an agency adjudication[16] or at least a court being asked to

[16] *See Fox Television Stations, Inc.*, 132 S. Ct. 2307 (vacating an FCC adjudication for lack of fair notice of an agency interpretation); *PMD Produce Brokerage Corp. v. USDA*, 234

defer to an agency interpretation[17]—apply where the court is to decide the meaning of the statute in the first instance.[18] Wyndham's counsel responded, "I think it would, your Honor. I think if you go to *Ford Motor* [*Co. v. FTC*, 673 F.2d 1008 (9th Cir. 1981)], I think that's what was happening there." Oral Arg. Tr. at 61. But *Ford Motor* is readily distinguishable. Unlike Wyndham, the petitioners there did not bring a fair notice claim under the Due Process Clause. Instead, they argued that, per *NLRB v. Bell Aerospace Co.*, 416 U.S. 267 (1974), the FTC abused its discretion by proceeding through agency adjudication rather than

---

F.3d 48 (D.C. Cir. 2000) (vacating the dismissal of an administrative appeal issued by a Judicial Officer in the Department of Agriculture because the agency's Rules of Practice failed to give fair notice of the deadline for filing an appeal); *Gen. Elec. Co.*, 53 F.3d 1324 (vacating an EPA adjudication for lack of fair notice of the agency's interpretation of a regulation); *FTC v. Colgate-Palmolive Co.*, 380 U.S. 374 (1965) (reviewing an FTC adjudication that found liability).

[17] *See In re Metro-East Mfg. Co.*, 655 F.2d 805, 810–12 (7th Cir. 1981) (declining to defer to an agency's interpretation of its own regulation because the defendant could not have known with ascertainable certainty the agency's interpretation).

[18] We asked, "All of your cases on fair notice pertain to an *agency's interpretation* of its own regulation or the statute that governs that agency. Does this fair notice doctrine apply where it is a *court* announcing an *interpretation* of a *statute in the first instance*?" Oral Arg. Tr. at 60 (emphases added).

rulemaking.[19] More importantly, the Ninth Circuit was reviewing an agency adjudication; it was not interpreting the meaning of the FTC Act in the first instance.

In addition, our understanding of Wyndham's position is consistent with the District Court's opinion, which concluded that the FTC has stated a claim under § 45(a) based on the Court's interpretation of the statute and without any reference to *LabMD* or any other agency adjudication or

---

[19] To the extent Wyndham could have raised this argument, we do not read its briefs to do so. Indeed, its opening brief appears to repudiate the theory. Wyndham Br. at 38–39 ("The district court below framed the fair notice issue here as whether 'the FTC must formally promulgate regulations before bringing its unfairness claim.' With all respect, that characterization of Wyndham's position is a straw man. Wyndham has never disputed the general principle that administrative agencies have discretion to regulate through either rulemaking or adjudication. *See, e.g.*, [*Bell Aerospace Co.*, 416 U.S. at 290–95]. Rather, Wyndham's point is only that, however an agency chooses to proceed, it must provide regulated entities with constitutionally requisite fair notice." (internal citations omitted)). Moreover, the Supreme Court has explained that where "it is doubtful [that] any generalized standard could be framed which would have more than marginal utility[, the agency] has reason to . . . develop[] its standards in a case-by-case manner." *Bell Aerospace Co.*, 416 U.S. at 294. An agency's "judgment that adjudication best serves this purpose is entitled to great weight." *Id.* Wyndham's opening brief acknowledges that the FTC has given this rationale for proceeding by adjudication, Wyndham Br. at 37–38, but, the company offers no ground to challenge it.

regulation. *See FTC v. Wyndham Worldwide Corp.*, 10 F. Supp. 3d 602, 621–26 (D.N.J. 2014).

We thus conclude that Wyndham was not entitled to know with ascertainable certainty the FTC's interpretation of what cybersecurity practices are required by § 45(a). Instead, the relevant question in this appeal is whether Wyndham had fair notice that its conduct could fall within the meaning of the statute. If later proceedings in this case develop such that the proper resolution is to defer to an agency interpretation that gives rise to Wyndham's liability, we leave to that time a fuller exploration of the level of notice required. For now, however, it is enough to say that we accept Wyndham's forceful contention that we are interpreting the FTC Act (as the District Court did). As a necessary consequence, Wyndham is only entitled to notice of the meaning of the statute and not to the agency's interpretation of the statute.

B. Did Wyndham Have Fair Notice of the Meaning of § 45(a)?

Having decided that Wyndham is entitled to notice of the meaning of the statute, we next consider whether the case should be dismissed based on fair notice principles. We do not read Wyndham's briefs as arguing the company lacked fair notice that cybersecurity practices can, as a general matter, form the basis of an unfair practice under § 45(a). Wyndham argues instead it lacked notice of what *specific* cybersecurity practices are necessary to avoid liability. We have little trouble rejecting this claim.

To begin with, Wyndham's briefing focuses on the FTC's failure to give notice of its interpretation of the statute and does not meaningfully argue that the statute itself fails fair notice principles. We think it imprudent to hold a 100-

year-old statute unconstitutional as applied to the facts of this case when we have not expressly been asked to do so.

Moreover, Wyndham is entitled to a relatively low level of statutory notice for several reasons. Subsection 45(a) does not implicate any constitutional rights here. *Vill. of Hoffman Estates v. Flipside, Hoffman Estates, Inc.*, 455 U.S. 489, 499 (1982). It is a civil rather than criminal statute.[20] *Id.* at 498–99. And statutes regulating economic activity receive a "less strict" test because their "subject matter is often more narrow, and because businesses, which face economic demands to plan behavior carefully, can be expected to consult relevant legislation in advance of action." *Id.* at 498.

In this context, the relevant legal rule is not "so vague as to be 'no rule or standard at all.'" *CMR D.N. Corp.*, 703 F.3d at 632 (quoting *Boutilier*, 387 U.S. at 123). Subsection 45(n) asks whether "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." While far from precise, this standard informs parties that the relevant inquiry here is a cost-benefit analysis, *Pa. Funeral Dirs. Ass'n v. FTC*, 41 F.3d 81, 89–92 (3d Cir. 1992); *Am. Fin. Servs. Ass'n*, 767 F.2d at 975, that considers a number of relevant factors, including the probability and expected size of reasonably unavoidable harms to consumers given a certain level of cybersecurity and the costs to consumers that

[20] While civil statutes containing "quasi-criminal penalties may be subject to the more stringent review afforded criminal statutes," *Ford Motor Co.*, 264 F.3d at 508, we do not know what remedy, if any, the District Court will impose. And Wyndham's briefing does not indicate what kinds of remedies it is exposed to in this proceeding.

would arise from investment in stronger cybersecurity. We acknowledge there will be borderline cases where it is unclear if a particular company's conduct falls below the requisite legal threshold. But under a due process analysis a company is not entitled to such precision as would eliminate all close calls. *Cf. Nash v. United States*, 229 U.S. 373, 377 (1913) ("[T]he law is full of instances where a man's fate depends on his estimating rightly, that is, as the jury subsequently estimates it, some matter of degree."). 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.

What appears to us is that Wyndham's fair notice claim must be reviewed as an as-applied challenge. *See United States v. Mazurie*, 419 U.S. 544, 550 (1975); *San Filippo*, 961 F.2d at 1136. Yet Wyndham does not argue that its cybersecurity practices survive a reasonable interpretation of the cost-benefit analysis required by § 45(n). One sentence in Wyndham's reply brief says that its "view of what data-security practices are unreasonable . . . is not necessarily the same as the FTC's." Wyndham Reply Br. at 23. Too little and too late.

Wyndham's as-applied challenge falls well short given the allegations in the FTC's complaint. As the FTC points out in its brief, the complaint does not allege that Wyndham used *weak* firewalls, IP address restrictions, encryption software, and passwords. Rather, it alleges that Wyndham failed to use *any* firewall at critical network points, Compl. at ¶ 24(a), did not restrict specific IP addresses *at all*, *id.* at ¶ 24(j), did not use *any* encryption for certain customer files, *id.* at ¶ 24(b), and did not require some users to change their default or factory-setting passwords *at all*, *id.* at ¶ 24(f). Wyndham did not respond to this argument in its reply brief.

Wyndham's as-applied challenge is even weaker given it was hacked not one or two, but three, times. At least after the second attack, it should have been painfully clear to Wyndham that a court could find its conduct failed the cost-benefit analysis. That said, we leave for another day whether Wyndham's alleged cybersecurity practices do in fact fail, an issue the parties did not brief. We merely note that certainly after the second time Wyndham was hacked, it was on notice of the possibility that a court *could* find that its practices fail the cost-benefit analysis.

Several other considerations reinforce our conclusion that Wyndham's fair notice challenge fails. In 2007 the FTC issued a guidebook, *Protecting Personal Information: A Guide for Business*, FTC Response Br. Attachment 1 [hereinafter *FTC Guidebook*], which describes a "checklist[]" of practices that form a "sound data security plan." *Id.* at 3. The guidebook does not state that any particular practice is required by § 45(a),[21] but it does counsel against many of the specific practices alleged here. For instance, it recommends that companies "consider encrypting sensitive information that is stored on [a] computer network . . . [, c]heck . . . software vendors' websites regularly for alerts about new vulnerabilities, and implement policies for installing vendor-approved patches." *Id.* at 10. It recommends using "a firewall to protect [a] computer from hacker attacks while it is connected to the Internet," deciding "whether [to] install a 'border' firewall where [a] network connects to the Internet," and setting access controls that "determine who gets through

[21] For this reason, we agree with Wyndham that the guidebook could not, on its own, provide "ascertainable certainty" of the FTC's interpretation of what specific cybersecurity practices fail § 45(n). But as we have already explained, this is not the relevant question.

the firewall and what they will be allowed to see . . . to allow only trusted employees with a legitimate business need to access the network." *Id.* at 14. It recommends "requiring that employees use 'strong' passwords" and cautions that "[h]ackers will first try words like . . . the software's default password[] and other easy-to-guess choices." *Id.* at 12. And it recommends implementing a "breach response plan," *id.* at 16, which includes "[i]nvestigat[ing] security incidents immediately and tak[ing] steps to close off existing vulnerabilities or threats to personal information," *id.* at 23.

As the agency responsible for administering the statute, the FTC's expert views about the characteristics of a "sound data security plan" could certainly have helped Wyndham determine in advance that its conduct might not survive the cost-benefit analysis.

Before the attacks, the FTC also filed complaints and entered into consent decrees in administrative cases raising unfairness claims based on inadequate corporate cybersecurity. FTC Br. at 47 n.16. The agency published these materials on its website and provided notice of proposed consent orders in the Federal Register. Wyndham responds that the complaints cannot satisfy fair notice principles because they are not "adjudications on the merits."[22] Wyndham Br. at 41. But even where the "ascertainable certainty" standard applies to fair notice claims, courts regularly consider materials that are neither regulations nor "adjudications on the merits." *See, e.g.*, *United States v.*

[22] We agree with Wyndham that the consent orders, which admit no liability and which focus on prospective requirements on the defendant, were of little use to it in trying to understand the specific requirements imposed by § 45(a).

Lachman, 387 F.3d 42, 57 (1st Cir. 2004) (noting that fair notice principles can be satisfied even where a regulation is vague if the agency "provide[d] a sufficient, publicly accessible statement" of the agency's interpretation of the regulation); *Beverly Healthcare-Hillview*, 541 F.3d at 202 (citing *Lachman* and treating an OSHA opinion letter as a "sufficient, publicly accessible statement"); *Gen. Elec. Co.*, 53 F.3d at 1329. That the FTC commissioners—who must vote on whether to issue a complaint, 16 C.F.R. § 3.11(a); ABA Section of Antitrust Law, *FTC Practice and Procedure Manual* 160–61 (2007)—believe that alleged cybersecurity practices fail the cost-benefit analysis of § 45(n) certainly helps companies with similar practices apprehend the possibility that their cybersecurity could fail as well.[23]

[23] We recognize it may be unfair to expect private parties back in 2008 to have examined FTC complaints or consent decrees. Indeed, these may not be the kinds of legal documents they typically consulted. At oral argument we asked how private parties in 2008 would have known to consult them. The FTC's only answer was that "if you're a careful general counsel you do pay attention to what the FTC is doing, and you do look at these things." Oral Arg. Tr. at 51. We also asked whether the FTC has "informed the public that it needs to look at complaints and consent decrees for guidance," and the Commission could offer no examples. *Id.* at 52. But Wyndham does not appear to argue it was unaware of the consent decrees and complaints; it claims only that they did not give notice of what the law requires. Wyndham Reply Br. at 25 ("The fact that the FTC publishes these materials on its website and provides notice in the Federal Register, moreover, is immaterial—the problem is not that Wyndham lacked notice *of the consent decrees* [which

Wyndham next contends that the individual allegations in the complaints are too vague to be relevant to the fair notice analysis. Wyndham Br. at 41–42. It does not, however, identify any specific examples. And as the Table below reveals, the individual allegations were specific and similar to those here in at least one of the four or five[24] cybersecurity-related unfair-practice complaints that issued prior to the first attack.

Wyndham also argues that, even if the individual allegations are not vague, the complaints "fail to spell out what specific cybersecurity practices . . . actually triggered the alleged violation, . . . provid[ing] only a . . . description of certain alleged problems that, '*taken together*,'" fail the cost-benefit analysis. Wyndham Br. at 42 (emphasis in original). We part with it on two fronts. First, even if the complaints do not specify which allegations, in the Commission's view, form the necessary and sufficient conditions of the alleged violation, they can still help companies apprehend the possibility of liability under the statute. Second, as the Table below shows, Wyndham cannot argue that the complaints fail to give notice of the necessary and sufficient conditions of an

---

reference the complaints] but that consent decrees [and presumably complaints] by their nature do not give notice *of what Section 5 requires*." (emphases in original, citations and internal quotations omitted)).

[24] The FTC asserts that five such complaints issued prior to the first attack in April 2008. *See* FTC Br. at 47–48 n.16. There is some ambiguity, however, about whether one of them issued several months later. *See* Complaint, *TJX Co.*, No. C-4227 (FTC 2008) (stating that the complaint was issued on July 29, 2008). We note that this complaint also shares significant parallels with the allegations here.

alleged § 45(a) violation when all of the allegations in at least one of the relevant four or five complaints have close corollaries here. *See* Complaint, *CardSystems Solutions, Inc.*, No. C-4168 (FTC 2006) [hereinafter CCS].

Table: Comparing CSS and Wyndham Complaints

	CSS	**Wyndham**
1	Created unnecessary risks to personal information by storing it in a vulnerable format for up to 30 days, CSS at ¶ 6(1).	Allowed software at hotels to store payment card information in clear readable text, Compl. at ¶ 24(b).
2	Did not adequately assess the vulnerability of its web application and computer network to commonly known or reasonably foreseeable attacks; did not implement simple, low-cost and readily available defenses to such attacks, CSS at ¶ 6(2)–(3).	Failed to monitor network for the malware used in a previous intrusion, Compl. at ¶ 24(i), which was then reused by hackers later to access the system again, *id.* at ¶ 34.
3	Failed to use strong passwords to prevent a hacker from gaining control over computers on its computer network and access to personal information stored on the network, CSS at ¶ 6(4).	Did not employ common methods to require user IDs and passwords that are difficult for hackers to guess. *E.g.*, allowed remote access to a hotel's property management system that used default/factory setting passwords, Compl. at ¶ 24(f).

4	Did not use readily available security measures to limit access between computers on its network and between those computers and the Internet, CSS at ¶ 6(5).	Did not use readily available security measures, such as firewalls, to limit access between and among hotels' property management systems, the Wyndham network, and the Internet, Compl. at ¶ 24(a).
5	Failed to employ sufficient measures to detect unauthorized access to personal information or to conduct security investigations, CSS at ¶ 6(6).	Failed to employ reasonable measures to detect and prevent unauthorized access to computer network or to conduct security investigations, Compl. at ¶ 24(h).

In sum, we have little trouble rejecting Wyndham's fair notice claim.

V. Conclusion

The three requirements in § 45(n) may be necessary rather than sufficient conditions of an unfair practice, but we are not persuaded that any other requirements proposed by Wyndham pose a serious challenge to the FTC's claim here. Furthermore, Wyndham repeatedly argued there is no FTC interpretation of § 45(a) or (n) to which the federal courts must defer in this case, and, as a result, the courts must interpret the meaning of the statute as it applies to Wyndham's conduct in the first instance. Thus, Wyndham cannot argue it was entitled to know with ascertainable certainty the cybersecurity standards by which the FTC expected it to conform. Instead, the company can only claim that it lacked fair notice of the meaning of the statute itself—a

theory it did not meaningfully raise and that we strongly suspect would be unpersuasive under the facts of this case.

We thus affirm the District Court's decision.