ADMINISTRATIVE LAW — FEDERAL TRADE COMMISSION ACT — THIRD CIRCUIT FINDS FTC HAS AUTHORITY TO REGULATE DATA SECURITY AND COMPANY HAD FAIR NOTICE OF POTENTIAL LIABILITY. — *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

Many statutes authorizing regulation by executive agencies were written long before modern computer technology was invented, and even longer before hackers began exploiting weaknesses to access personal information. In the last decade, the Federal Trade Commission (FTC) has started to police companies for exposing the data they collect from consumers to the threat of breach. The Commission has primarily based this enforcement on the FTC Act[1] (FTCA), which in 15 U.S.C. § 45(a) prohibits "unfair . . . practices in or affecting commerce."[2] This language has left the Commission vulnerable to challenge based on its scope of authority. Recently, in *FTC v. Wyndham Worldwide Corp.*,[3] the Third Circuit held that certain data security practices could be considered "unfair" under § 45(a), and that the relevant provision provided Wyndham fair notice that its practices opened it up to liability. Based on the procedural posture and facts of the case, the court correctly determined that Wyndham had fair notice of its potential liability under the statute. But the court's statutory fair notice analysis illustrated a tension between effective FTC regulation of data security practices and constitutional notice requirements. Future courts facing more difficult factual circumstances will likely have to grapple with this tension in a way the Third Circuit was able to avoid.

Wyndham Worldwide, a hospitality company that franchises and manages hotels, used a property management system that processed consumer information, including names, addresses, contact information, and credit card information.[4] In 2008 and 2009, Wyndham's network and property management systems were hacked three times.[5] Hackers allegedly accessed unencrypted information for over 619,000 accounts, resulting in approximately $10.6 million in fraud loss.[6]

The FTC filed suit against Wyndham in the U.S. District Court for the District of Arizona in June 2012,[7] claiming that the hacks were the

---

[1] 15 U.S.C. §§ 41–58 (2012).

[2] *Id.* § 45(a).

[3] 799 F.3d 236 (3d Cir. 2015).

[4] *Id.* at 240.

[5] *Id.* at 241–42.

[6] *Id.* at 242.

[7] The Commission can commence civil actions in district court for violations of the FTCA, *see* 15 U.S.C. § 57(b), as an alternative to its own adjudicative process, *id.* § 45(b).

result of unfair and deceptive practices in violation of § 45(a).[8] At Wyndham's request the case was transferred to the U.S. District Court for the District of New Jersey, and Wyndham filed a Rule 12(b)(6) motion to dismiss.[9] Wyndham asserted three claims: the FTC did not have authority to bring a data security unfairness claim, violated fair notice principles by bringing an unfairness claim without first promulgating formal regulations, and insufficiently pleaded its unfairness and deception claims.[10]

The district court denied the motion to dismiss.[11] In response to Wyndham's first claim, the court held that FTC authority over data security could "coexist with the existing data security regulatory scheme"[12] and was not, as Wyndham argued, analogous to the FDA's claim of authority over tobacco rejected in *FDA v. Brown & Williamson Tobacco Corp*.[13] As to Wyndham's second claim, the court noted that agencies generally have the discretion to regulate through adjudication or rulemaking as they see fit.[14] Although the court acknowledged the parties' dispute over the applicable standard of review,[15] it focused instead on the ability of the FTC's public statements, guidance documents, and complaints and consent decrees to provide notice.[16] Moreover, "a statutorily-defined standard exist[ed] for asserting an unfairness claim"[17] — § 45 requires that a practice satisfy a particular cost-benefit balancing test to be declared "unfair."[18] The court also held the FTC did not need to formally promulgate rules because the

---

[8] *Wyndham*, 799 F.3d at 242. These practices included storing credit card information in clear, readable text, using easily guessed passwords for system access, failing to employ firewalls, allowing hotels to connect to the network with out-of-date operating systems, failing to restrict network access of third-party vendors, and failing to take reasonable measures following network intrusions. *Id.* at 240–41.

[9] *Id.* at 242.

[10] FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 607 (D.N.J. 2014).

[11] *Id.*

[12] *Id.* at 613.

[13] 529 U.S. 120, 142–43 (2000) (finding that newly declared FDA authority over tobacco products would require their removal from the market, contradicting Congress's clear intent to the contrary expressed by "a distinct regulatory scheme," *id.* at 155). The district court also found that the data security legislation complemented FTC authority by granting it additional enforcement tools. *Wyndham*, 10 F. Supp. 3d at 613.

[14] *Wyndham*, 10 F. Supp. 3d at 617 (citing SEC v. Chenery Corp., 332 U.S. 194, 203 (1947)).

[15] *Id.* at 618. Wyndham claimed that the FTC had to state with "ascertainable certainty" the meaning of its standards, *id.*, while the FTC claimed that its complaints and Business Guide provided adequate notice, *see* Supplemental Memorandum of the FTC at 4 n.2, *Wyndham*, 799 F.3d 236 (No. 14-3514).

[16] *See Wyndham*, 10 F. Supp. 3d at 619–20.

[17] *Id.* at 621.

[18] Section 45(n) states that no act or practice is "unfair" unless (i) it "causes or is likely to cause substantial injury to consumers"; (ii) the injury "is not reasonably avoidable by consumers themselves"; and (iii) the injury is "not outweighed by countervailing benefits to consumers or to competition." 15 U.S.C. § 45(n) (2012).

proscriptions in § 45 are purposefully flexible.[19] It also denied Wyndham's third claim, finding that the agency had adequately alleged substantial consumer injury that was not reasonably avoidable by the consumers themselves.[20]

The Third Circuit granted interlocutory appeal on two questions: (1) whether the FTC had the authority to regulate data security under the unfairness prong of § 45(a), and (2) whether Wyndham had fair notice that its specific practices could run afoul of that provision.[21] The court affirmed the district court and ruled in favor of the FTC on both questions.

Writing for the panel, Judge Ambro[22] first addressed whether the FTC had authority under § 45(a) to regulate the alleged data security practices. The court began by noting that ambiguity and flexibility were purposefully built into the FTCA.[23] The court dismissed Wyndham's argument, first raised on appeal, that the alleged conduct fell outside of the plain meaning of "unfair."[24] The court also substantially reiterated the lower court's analysis of Wyndham's *Brown & Williamson* argument, finding the situations were not analogous.[25]

Having rejected Wyndham's arguments that its conduct could not be unfair,[26] the court turned to Wyndham's argument that the FTC had not provided fair notice of possible liability. To ascertain which legal standard governed Wyndham's claim, the court addressed whether the statute itself could provide notice, or whether the FTC, by issuing an interpretation of the statute, owed Wyndham notice of what conduct was required by its interpretation. If the notice derived from the statute, the relatively "lax" vagueness standard for civil statutes regulating economic activities would apply.[27] On the other hand, when an agency brings an enforcement action based on its interpretation of its organic statute, the regulated party is entitled to have "ascertainable certainty" of what conduct was required or prohibited.[28]

---

[19] *Id.* at 618. The court noted that "the contour of an unfairness claim in the data security context, like any other, is necessarily 'flexible' such that the FTC can apply [§ 45] 'to the facts of particular cases arising out of unprecedented situations.'" *Id.* at 620 (quoting FTC v. Colgate-Palmolive Co., 380 U.S. 374, 385 (1965)).

[20] *Id.* at 621–22. The court also found that the FTC's deception claim had been sufficiently pleaded. *Id.* at 627–28.

[21] *Wyndham*, 799 F.3d at 240.

[22] Judge Ambro was joined by Senior Judge Scirica and Judge Roth.

[23] *Wyndham*, 799 F.3d at 243 (citing FTC v. Bunte Bros., Inc., 312 U.S. 349, 353 (1941)).

[24] *Id.* at 244–47.

[25] *See id.* at 247–49.

[26] For the fair notice analysis, the court assumed without deciding that Wyndham's conduct was unfair. *See id.* at 249.

[27] *Id.* at 250.

[28] *Id.* at 251. As the court explained, the "higher standard of fair notice" in the case of enforcement based on an agency interpretation, *id.* at 251, is justified by the fact that an agency,

To argue that the FTC's view of its authority over data security practices was not owed any deference,[29] Wyndham had consistently asserted that the FTC had not promulgated any binding interpretation of the statute.[30] The court accepted this contention and concluded that the "necessary consequence" was that Wyndham was "only entitled to notice of the meaning of the statute and not to the agency's interpretation of the statute."[31] Therefore, the court considered "whether Wyndham had fair notice that its conduct could fall within the meaning of the statute."[32]

After articulating the applicable legal standard for Wyndham's fair notice claim, the court concluded that the FTC's previous adjudication and interpretive guidance provided the requisite notice to Wyndham that its actions could be considered "unfair" under the FTCA. The court reasoned that Wyndham was entitled to a comparatively low level of statutory notice because no constitutional rights were implicated and because the statute was civil and regulated economic activity.[33] The cost-benefit analysis of § 45(n) provided the relevant statutory language. It informed Wyndham that it should consider the probability and magnitude of harms to consumers caused by its data security practices and whether these costs outweighed any savings from not employing more secure practices.[34] The court noted that Wyndham was hacked three times and that its alleged security practices were specifically counseled against by FTC guidance and complaints.[35] Based on these factors, the court rejected the fair notice claim.[36]

Wyndham marked the first time the FTC's authority to regulate data security under the unfairness prong of § 45(a) — and its method for doing so — had been addressed by a court.[37] Given the case the court was presented with, its reasoning that Wyndham had fair notice

---

which is "free to adopt *any reasonable construction*" of its statute, may impose less obvious legal obligations on regulated parties than would be derived from the "*best* or *most reasonable* interpretation" of a statute, *id.* at 252.

[29] Agency interpretations of the scope of their authority under their organic statutes are given *Chevron* deference. *See* City of Arlington v. FCC, 133 S. Ct. 1863, 1868 (2013).

[30] *Wyndham*, 799 F.3d at 253–54.

[31] *Id.* at 255.

[32] *Id.*

[33] *Id.* (citing Village of Hoffman Estates v. Flipside, Hoffman Estates, Inc., 455 U.S. 489, 498–99 (1982)).

[34] *Id.*

[35] *Id.* at 256.

[36] *Id.* at 259.

[37] The Eleventh Circuit found that it did not have subject matter jurisdiction over a company's appeal of the FTC's denial of a motion to dismiss an ongoing Commission adjudication. *See* LabMD, Inc. v. FTC, 776 F.3d 1275 (11th Cir. 2015). All other previous data security complaints brought by the FTC have been settled. *See* FTC, COMMISSION STATEMENT MARKING THE FTC'S 50TH DATA SECURITY SETTLEMENT (2014), https://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf.

of possible liability was appropriate. *Wyndham* highlights the efficacy of the FTC's enforcement scheme in the context of data security but illustrates an inherent tension with traditional precedent on fair notice. This tension will have to be resolved in cases in which the facts and procedural posture do not allow for such a tidy conclusion.

Because the court was reviewing a ruling on a Rule 12(b)(6) motion to dismiss, it accepted the truth of all factual allegations.[38] Wyndham's alleged data security practices, or lack thereof, were egregious. The FTC did not "allege that Wyndham used *weak* firewalls, IP address restrictions, [or] encryption software . . . . Rather, it allege[d] that Wyndham failed to use *any* firewall at critical network points, did not restrict specific IP addresses *at all*, [and] did not use *any* encryption for certain customer files . . . ."[39] Furthermore, the company was not hacked just once, but *three* times, and the second and third hacks occurred after Wyndham had knowledge of the first breach.[40] As the court found, Wyndham could reasonably have anticipated its actions would not pass the cost-benefit analysis of § 45(n),[41] even without FTC interpretation.

In addition, Wyndham tried to argue that the FTC had not interpreted the FTCA but that the company was still entitled to the fair notice standard designated for enforcement based on binding agency interpretations. In arguing that no deference was owed to the FTC's view that it had authority over data security under the unfairness prong of § 45(a), Wyndham asserted that the Commission had not promulgated a binding interpretation of the FTCA in this area.[42] Once the court found the FTC had statutory authority, Wyndham's argument worked against it. The court could "accept Wyndham's forceful contention" that it did not have to address whether the FTC had interpreted the statute and could therefore analyze the fair notice inquiry based on the statute itself.[43] The court contained its inquiry to the statutory language and the lower threshold for notice rather than delving into *Chevron* analysis or concerns regarding retroactive application of agency interpretations.[44]

---

[38] *Wyndham*, 799 F.3d at 242; *see* FED. R. CIV. P. 12(b)(6).

[39] *Wyndham*, 799 F.3d at 256 (citations omitted).

[40] *See* First Amended Complaint for Injunctive and Other Equitable Relief at 12–13, FTC v. Wyndham Worldwide Corp., No. CV 12-1365-PHX (D. Ariz. Aug. 9, 2012). It is unclear from the complaint what remedial steps, if any, Wyndham took after the first breach. According to the complaint, software installed on the Wyndham system in the first attack was used in the second attack. *Id.* at 15–16.

[41] *Wyndham*, 799 F.3d at 256.

[42] *Id.* at 253–54.

[43] *Id.* at 255.

[44] A primary concern regarding administrative regulation is that agencies will announce interpretations for the first time in adjudication and retroactively penalize companies for noncompliance. *See* SEC v. Chenery Corp., 332 U.S. 194, 203 (1947); *see also* Matthew C. Stephenson &

The Third Circuit's embrace of Wyndham's argument allowed it to avoid wading into both an ongoing regulatory process[45] and a debate about how the FTC should best regulate this field.[46] Rather than engage in notice-and-comment rulemaking, as some academics have urged,[47] the Commission has focused on adjudication since it began regulating data security practices under its unfairness authority in 2005, primarily settling with companies under consent orders.[48] Using this strategy, the Commission can enforce baseline standards, as it did here, while retaining the intentional flexibility built into its organic statute.[49] Data security is a moving target, with companies constantly using data in new ways and facing myriad potential threats.[50] Specific rules would fail "to offer a touchstone for guiding privacy decisionmaking in new contexts, as new types of products, technologies, and business models evolve."[51] Importantly, the FTC provides guidance in parallel with its enforcement activity. In addition to previous complaints issued as part of consent decrees,[52] the Third Circuit relied on the Commission's guidebook, which detailed specific practices that were not followed by Wyndham.[53] Since Wyndham was first hacked, the FTC has continued hosting conferences, publishing reports, and soliciting public comment on its consent decrees.[54] Fur-

---

Miri Pogoriler, Seminole Rock*'s Domain*, 79 GEO. WASH. L. REV. 1449, 1479–81 (2011); Kieran Ringgenberg, United States v. Chrysler*: The Conflict Between Fair Warning and Adjudicative Retroactivity in D.C. Circuit Administrative Law*, 74 N.Y.U. L. REV. 914 (1999).

[45] *See* LabMD, Inc., No. 9357, 2014 WL 253518 (F.T.C. Jan. 16, 2014).

[46] *See generally* Michael D. Scott, *The FTC, The Unfairness Doctrine, and Data Security Breach Litigation: Has the Commission Gone Too Far?*, 60 ADMIN. L. REV. 127 (2008); Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583 (2014); Gerard M. Stegmaier & Wendell Bartnick, *Psychics, Russian Roulette, and Data Security: The FTC's Hidden Data-Security Requirements*, 20 GEO. MASON L. REV. 673 (2013).

[47] *See, e.g.*, Scott, *supra* note 46, at 171–73; Stegmaier & Bartnick, *supra* note 46.

[48] *See generally* FTC, *supra* note 37.

[49] *See Wyndham*, 799 F.3d at 243.

[50] *See, e.g.*, Donald S. Clark, FTC, Comments of the FTC Before the FCC In the Matter of Cyber Security Certification Program (Sept. 8, 2015), http://www.ftc.gov/sites/default/files/documents/advocacy_documents/ftc-comment-fcc-concerning-proposed-cyber-security-certification-program/101013fcccomment.pdf [http://perma.cc/U89T-4ZQA]; Kim Zetter, *The Biggest Security Threats We'll Face in 2015*, WIRED (Jan. 4, 2015, 6:30 AM), http://www.wired.com/2015/01/security-predictions-2015 [http://perma.cc/LY7E-V9ZZ].

[51] Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 266 (2011); *see also id.* at 273 ("[A] key to the effectiveness of FTC enforcement authority is [its] ability to respond to harmful outcomes by enforcing evolving standards of privacy protection as the market, technology, and consumer expectations change . . . .").

[52] *See, e.g.*, Cardsystems Sols., Inc., No. C-4168, 2006 WL 2709787 (F.T.C. 2006) (decision and order); DSW Inc., 141 F.T.C. 117 (2006) (consent order); BJ's Wholesale Club, Inc., No. C-4148, 2005 WL 2395788 (F.T.C. 2005).

[53] *Wyndham*, 799 F.3d at 256–57.

[54] *See* Solove & Hartzog, *supra* note 46, at 625–26; Stegmaier & Bartnick, *supra* note 46, at 690; Press Release, FTC, FTC Kicks Off "Start With Security" Business Education Initiative

thermore, reflecting the ethos of self-regulation that has characterized this field,[55] industry standards have developed that further inform companies about what practices are considered reasonable.[56] Reliance on informal interpretations allows the FTC to respond to developments in the market, and forces both the Commission and the companies it regulates to focus on what is most important — consumer protection against known and new threats — rather than simple compliance with specified rules. The court's analysis of how Wyndham could have relied on statutory language and interpretive guidance demonstrates how this enforcement approach might work practically for companies.

However, elements of the statutory fair notice analysis highlight the tension between the FTC's enforcement and the traditional notice requirements to which agencies are held. In particular, the court pointed out that economic statutes "receive a 'less strict' test because their 'subject matter is often more narrow, and because businesses . . . can be expected to consult relevant legislation in advance of action.'"[57] Decades of FTC enforcement have demonstrated that the FTCA does not in fact have a narrow reach.[58] And while the court found that Wyndham could have foreseen that its actions would be considered unfair under the § 45(n) cost-benefit analysis,[59] companies challenging FTC action in the future are more likely to present borderline cases dealing with less obviously reckless practices that do not so clearly fall within the statute and available (nonbinding) FTC interpretations.

It is these cases that present the problem.[60] In most of the cases that have addressed fair notice challenges to administrative actions,

---

(June 30, 2015), http://www.ftc.gov/news-events/press-releases/2015/06/ftc-kicks-start-security-business-education-initiative [http://perma.cc/5BST-DWMC].

55 *See* Kenneth A. Bamberger, *Regulation as Delegation: Private Firms, Decisionmaking, and Accountability in the Administrative State*, 56 DUKE L.J. 377, 385–92 (2006); Solove & Hartzog, *supra* note 46, at 592–94, 598.

56 *See, e.g.*, Brief of Amicus Curiae Electronic Privacy Information Center (EPIC) & Thirty-Three Technical Experts & Legal Scholars in Support of Respondent at 23–29, *Wyndham*, 799 F.3d 236 (No. 14-3514); NAT'L INST. OF STDS. & TECH., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY (2014), http://nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf [http://perma.cc/A84F-VFKF]; Bamberger & Mulligan, *supra* note 51, at 286. In fact, Wyndham's privacy policy — although not at issue here — claimed that it made "commercially reasonable efforts" to secure its customers' personal data. *Wyndham*, 799 F.3d at 241.

57 *Wyndham*, 799 F.3d at 255 (quoting Village of Hoffman Estates v. Flipside, Hoffman Estates, Inc., 455 U.S. 489, 498 (1982)).

58 *See, e.g.*, Am. Fin. Servs. Ass'n v. FTC, 767 F.2d 957, 965–68 (D.C. Cir. 1985) (discussing the Commission's broad discretionary authority).

59 *Wyndham*, 799 F.3d at 256.

60 *See, e.g.*, Stegmaier & Bartnick, *supra* note 46, at 689 ("[E]ntities do not likely need more notice that a complete lack of data security may be 'unfair,' [but] what data security is necessary to make it 'fair' is unknown.").

such as environmental or vehicle-safety regulation,[61] the agency could promulgate rules without fear of the rules becoming immediately outdated.[62] In contrast, fair notice is particularly thorny for the FTC in the data security context. If the FTC were to promulgate rules flexible enough for changing circumstances, these rules would necessarily be so vague as to not give significantly more notice than the status quo. Alternatively, if the FTC were to promulgate specific rules, those rules would likely not adequately address the full array of practices companies must implement to effectively secure consumer data. Therefore, the "ascertainable certainty" for regulated entities that courts might require could be incompatible with effective FTC policing of data security practices.[63]

The Third Circuit was able to avoid the problems that may arise in marginal cases because its role in this case was confined to the facts as alleged and the arguments as presented. The court's analysis shows that the statute, supplemented by persuasive guidance from the FTC, provides sufficient notice in easy cases where companies' data security practices are clearly unreasonable. However, FTC enforcement of less obviously unreasonable practices, which could not rest on statutory notice alone, will require future courts to address how the agency can continue its consumer-protection-focused enforcement while giving companies the necessary notice of the standards to which they will be held.

---

[61] *See, e.g.*, United States v. Chrysler Corp., 158 F.3d 1350 (D.C. Cir. 1998); Chem. Waste Mgmt. Inc. v. EPA, 976 F.2d 2 (D.C. Cir. 1992).

[62] *See* Solove & Hartzog, *supra* note 46, at 620 n.176 (discussing the burdensome nature of the FTC's rulemaking authority).

[63] Not all circuits use this standard. *See generally* Albert C. Lin, *Refining Fair Notice Doctrine: What Notice is Required of Civil Regulations?*, 55 BAYLOR L. REV. 991 (2003). Additionally, it is possible that under a recent Supreme Court decision, the ascertainable certainty standard could be considered to go beyond constitutional requirements of notice and therefore be invalid judicial procedural lawmaking. *See* Perez v. Mortg. Bankers Ass'n, 135 S. Ct. 1199, 1203 (2015) (holding that a D.C. Circuit doctrine requiring agencies to go through notice and comment before significantly revising any interpretative rule improperly imposed an obligation on agencies beyond the requirements of the Administrative Procedure Act); *see also* Vt. Yankee Nuclear Power Corp. v. Nat. Res. Def. Council, Inc., 435 U.S. 519, 525 (1978).