Bloomberg BNA

Privacy Law Watch™

Wyndham—Did the Third Circuit Get It Wrong?

CHRISTIN S. MCMELEY

On Aug. 24, the U.S. Court of Appeals for the Third Circuit released its much-anticipated ruling in *Federal Trade Commission v. Wyndham Worldwide Corp.*, unanimously upholding the FTC's authority to regulate companies' data security practices under Section 5 of the Federal Trade Commission Act (FTC Act).[1] In doing so, however, the court also held that Wyndham—and any other entity subject to the FTC's jurisdiction—''was not entitled to know with ascertainable certainty the FTC's interpretation of what cybersecurity practices are required by [Section 5].''[2] This does not, however, resolve the still unanswered question of what constitutes ''reasonable and appropriate'' security practices. Moreover, the court took a novel approach to the due process issue of ''fair notice.'' In the context of understanding an agency's expectations of reasonableness that will prevent future investigations and enforcement actions, this point is critical.

As background, in 2012, the FTC filed a complaint against Wyndham in federal court alleging that Wyndham engaged in unfair and deceptive practices regarding three data breaches in 2008 and 2009 that, ''taken together, unreasonably and unnecessarily exposed [hundreds of thousands of] consumers' personal data to unauthorized access and theft,'' which led to over $10.6 million in fraudulent charges.[3] Wyndham had asked the lower court to dismiss the suit, contending that the FTC is not empowered to police companies' data security practices under its authority to regulate unfair practices pursuant to Section 5.[4] Wyndham also argued that the FTC had not given companies fair notice of the data security standards that the agency would enforce. The

Christin S. McMeley is a partner in Davis Wright Tremaine LLP's Washington office and chair of the firm's privacy and security practice. She advises companies in various industries in privacy compliance, information governance, data security, public policy and regulatory matters. Prior to her work at Davis Wright Tremaine, McMeley was the chief privacy officer and deputy general counsel at Charter Communications Inc.

[1] *FTC v. Wyndham Worldwide Corp.*, No. 14-3514, 2015 BL 271793 (3d Cir. Aug. 24, 2015) [hereinafter ''Order''], *available at* http://www.bloomberglaw.com/public/document/FEDERAL_TRADE_COMMISSION_v_WYNDHAM_WORLDWIDE_CORPORATION_a_Delawa (164 PRA, 8/25/15).

[2] *Id.* at *14.

[3] Complaint at 10, *FTC v. Wyndham Worldwide Corp.*, No. 2:13-cv-01887 (D. Ariz. June 26, 2012) (123 PRA, 6/27/12). Whether Wyndham's security practices—as opposed to the allegations of the complaint (which are assumed to be true on a motion to dismiss)—were consistent with standard industry practices at the time of the alleged violations is beyond the scope of this article.

[4] Motion to Dismiss filed by Wyndham Hotels & Resorts LLC, *FTC v. Wyndham Worldwide Corp.*, No. 2:13-cv-01887 (D.N.J. Apr. 26, 2013) (165 PRA, 8/26/13).

district court denied Wyndham's motion to dismiss but permitted the company to seek an interlocutory appeal, which was accepted by the Third Circuit.[5]

The Third Circuit made short work of Wyndham's argument that the FTC lacked authority to take enforcement action against ''unfair'' cybersecurity practices, finding that Congress purposefully left the term ''unfair'' ambiguous, that it was meant to represent a '' 'flexible concept with evolving content' ''[6] ***to be determined by the commission***.[7] The commission, in turn, has issued evolving policy statements over the years, culminating in the current test for unfairness that was codified by Congress in 1994[8] and which requires an act or practice (1) that causes or is likely to cause substantial injury to consumers, (2) which is not reasonably avoidable by consumers themselves and (3) not outweighed by countervailing benefits to consumers or to competition and (4) which may be determined based on public policy considerations.[9] While not explicitly saying that the FTC's enforcement activities have met this test, the court simply stated that ''[h]aving rejected Wyndham's arguments that its conduct *cannot* be unfair, we assume for the remainder of this opinion that it *was*.''[10]

Once the court made the assumption—not the finding—that Wyndham's cybersecurity practices were unfair, and thus within the FTC's authority to challenge, the court turned to the question of whether Wyndham had fair notice that its conduct was unfair under Section 5, and thus subject to FTC enforcement.

The court immediately acknowledged that ''a higher standard of fair notice'' is required in the context of a regulatory agency acting to interpret a statute for which it has been given primary responsibility for enforcing, or acting to interpret the meaning of its own regulation, than in the typical civil statutory interpretation case ''because agencies engage in interpretation differently than courts.''[11] Indeed, ''[i]n 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.''[12] Therefore, while courts generally must only provide notice under a standard that is ''not so vague as to be 'no rule or standard at all,' ''[13] a party is ''entitled to have 'ascertainable certainty' of what conduct is legally required'' by an agency's regulation or its interpretation of a regulation.[14]

But in determining the appropriate level of notice required, the court relied on Wyndham's repeated contentions that no existing FTC rule or adjudication merited the court's deference, and thus held that it was up to the court to decide in the first instance whether Wyndham's conduct was unfair. However, in almost every instance cited by the court, Wyndham made the deference argument in the context that Congress had not granted the FTC the authority to bring enforcement actions related to a company's cybersecurity practices under the unfairness prong of Section 5. In *that* context, Wyndham argued that the court should not give *Chevron* deference to the commission's own self-proclamations of authority in adjudications administered by the agency itself.[15] Wyndham made the alternative argument that *if* the court found that the agency has the authority to regulate cybersecurity practices, *then* it must find that the agency had not given the constitutionally adequate notice as to what was required.

Instead of answering Wyndham's question of ''[w]hether the FTC has provided constitutionally adequate notice of what are 'reasonable and appropriate' cybersecurity practices,''[16] the court essentially changed Wyndham's inquiry to ask whether the lower standard of judicial notice is applicable if it is up to the court to determine whether cybersecurity practices can be deemed ''unfair'' under Section 5. The inherent problem with this approach is that, under the assumption that cybersecurity practices do fall under the ambit of Section 5's unfairness doctrine, it is left to the commission to interpret the statute and bring subsequent enforcement actions against companies who engage in such ''unfair'' practices. As such, Wyndham and every other entity subject to the FTC's jurisdiction are entitled to fair notice as to the basis for those enforcement actions.

There is no doubt that technology and practices in the cybersecurity arena are evolving, and similarly, there is no doubt that an agency can rely on adjudications rather than rule-makings to ''address problems'' that are so ''varying in nature as to be impossible of capture within the boundaries of a general rule. . . . Thus there is a very definite place for the case-by-case evolution of statutory standards.''[17] However, such case-by-case adjudication must have bounds. ''Regulated parties should know what is required of them so they may act accordingly; and precision and guidance are necessary so that those enforcing the law do not act in an arbitrary or discriminatory way.''[18] In today's regulatory environment where multiple agencies are

---

[5] *FTC v. Wyndham Worldwide Corp.*, 10 F. Supp. 3d 602 (D.N.J. 2014), *available at* http://bit.ly/1L1x2bM (68 PRA, 4/9/14); *FTC v. Wyndham Worldwide Corp.*, No. 14-8091, 2014 BL 216045 (3d Cir. July 29, 2014) (147 PRA, 7/31/14).

[6] Order, 2015 BL 271793 at *5 (quoting *FTC v. Bunte Bros.*, 312 U.S. 349, 353 (1941)).

[7] *Id.*

[8] *Id.* at *6 (citing the FTC Act Amendments of 1994, Pub. L. No. 103-312, § 9, 108 Stat. 1691, 1695 (1994) (current version at 15 U.S.C. § 45(n) (2011)).

[9] 15 U.S.C. § 45(n) (2011).

[10] Order, 2015 BL 271793 at *11 (emphasis added).

[11] *Id.* at *12.

[12] *Id.* (emphasis in original). The court also noted that such agency interpretations may be subject to current political values and associated pressure, making it ''harder to predict how an agency will construe a statute or regulation at some unspecified point in the future.'' *Id.*

[13] *Id.* at *15 (quoting *CMR D.N. Corp. v. City of Phila.*, 703 F.3d 612, 631–32 (3d Cir. 2013)).

[14] *Id.* at *12.

[15] Wyndham's Letter Brief to the Honorable Esther Salas, U.S. District Judge, at 1–2, *FTC v. Wyndham Worldwide Corp.*, No. 13-1887 (D.N.J. Jan. 29, 2014), ECF No. 156; Appellant's Opening Brief and Joint Appendix Vol. 1 at pp. JA1-55, *FTC v. Wyndham Worldwide Corp.*, No. 14-3514 (3d Cir. Aug. 24, 2015) [hereinafter ''Wyndham Opening Brief'']; Appellant's Reply Brief, *FTC v. Wyndham Worldwide Corp.*, No. 14-3514 (3d Cir. Aug. 24, 2015) (02 PRA, 1/5/15).

[16] Wyndham Opening Brief, *supra* note 15, at *7.

[17] *SEC v. Chenery Corp.*, 332 U.S. 194, 202–203 (1947) (citing *Columbia Broadcasting Sys., Inc. v. United States*, 316 U.S. 407, 421 (1942)).

[18] *FCC v. Fox Television Stations, Inc.*, 132 S. Ct. 2307 (2012).

  PRA ISSN 0000-0000

bringing the weight of their enforcement ability to bear on businesses that become victims of cybersecurity attacks, this understanding becomes even more important.[19]

The fact that a violation of the FTC Act does not carry criminal penalties does not make this any less important. In its opinion, the court attempted to assuage concerns about applying the lower standard in this context because the statute is civil, rather than criminal, and because it was not clear what remedy, if any, the district court would impose.[20] This type of reasoning has already been rejected by the U.S. Supreme Court. In 2006, the Federal Communications Commission (FCC) issued an order against Fox Television Stations Inc. for airing programs with fleeting expletives, and the Supreme Court ultimately found that the FCC failed to provide Fox adequate notice of its interpretation of the applicable indecency statute. The FCC argued, however, that such notice was not required because the FCC did not impose a sanction against Fox. The Supreme Court rejected the FCC's argument, finding that even though the FCC claimed it would not consider the violation in other contexts, it still had the statutory right to do so, and that even without monetary sanctions, Fox could suffer reputational harm.[21]

Similar to the FCC enforcement actions, an FTC enforcement action carries the potential for reputational harm.[22] Additionally, when parties enter into consent decrees with the FTC, they often agree to monetary penalties if they engage in similar ''violations'' in the future. If a party decides not to enter a consent decree, with the FTC or any other agency, then it must incur significant costs associated with litigating with the agency.[23] For all of these reasons, it is imperative for agencies to provide businesses sufficient notice of the practices that will be called into question. In this instance, the court indicated that if it had applied the ''ascertainable certainty'' standard, it may have actually found the FTC's notice to be lacking. The court found that the guidebook relied upon by the FTC and endorsed by the district court did not actually counsel against many of the specific practices alleged in this case, and therefore the court agreed with Wyndham that ''the guidebook could not, on its own, provide 'ascertainable certainty' of the FTC's interpretation of what cybersecurity practices fail § 45(n).''[24] Moreover, the court agreed with Wyndham that ''the consent orders, which admit no liability and which focus on prospective requirements on the defendant, were of little use to [Wyndham] in trying to understand the specific requirements imposed by § 45(n).''[25] Finally, the court recognized that it ''may be unfair to expect private parties back in 2008 to have examined FTC complaints or consent decrees.''[26]

Whether the notice in the Wyndham case was adequate or not, agencies have provided the required fair notice in the past, such as through the FTC policy statements that were cited by the court in this case. The fact that cybersecurity involves rapidly changing technologies does not preclude finding a balance between flexible standards with adequate notice of how such standards will be enforced. And while the FTC has said that it does not require companies to have ''perfect security,'' there is quite a bit of latitude between perfect security, reasonable security and lax security, especially when agencies are enforcing with hindsight. So far, the FTC appears to be taking the most egregious cases to make examples of bad practices. But when do political pressures dictate that other, more borderline cases, be taken on by the FTC or another agency? When does one banana peel become more than negligent, but unreasonable, and thus unfair or unjust?

It remains to be seen whether Wyndham will seek further review of this decision, whether it will now move on to defending the merits of the case, or whether it will enter into settlement discussions with the FTC. In any event, for now, the threshold issue of the FTC's authority to police and enforce companies' cybersecurity policies and practices under the unfairness doctrine appears to be established. Take notice.

---

[19] With the reclassification of Internet access service as a ''telecommunications service'' subject to Section 222 of the Communications Act, the Federal Communications Commission has affirmatively stated that it will require providers to maintain ''reasonable'' security in the absence of FCC rules and has recently changed its enforcement policy under existing rules. *In re Protecting and Promoting the Open Internet*, Final Rule, 30 FCC Rcd 5601 (Mar. 12, 2015), *available at* https://www.fcc.gov/document/fcc-releases-open-internet-order (50 PRA, 3/16/15). Similarly, the Consumer Financial Protection Bureau has outlined guiding principles for protecting consumers ''as the private sector develops new faster payment systems'' that contain data security guidance. CFPB, *Consumer Protection Principles: CFPB's Vision of Consumer Protection in New Faster Payment Systems* (July 9, 2015), *available at* http://files.consumerfinance.gov/f/201507_cfpb_consumer-protection-principles.pdf (133 PRA, 7/13/15). The CFPB will ostensibly attempt to enforce these principles pursuant to its authority under Section 1031 of the Dodd-Frank Act. 12 U.S.C. § 5531 (2011).

[20] Order, 2015 BL 271793 at *15.

[21] *Fox Television Stations*, 132 S. Ct. at 2318–19.

[22] The FTC also has the ability to obtain redress for consumers, whereas the FCC has the ability to issue fines and penalties under certain circumstances.

[23] *See* Appellant's Supplemental Memorandum at *2, 11, *FTC v. Wyndham Worldwide Corp.*, No. 14-3514 (3d Cir. Aug. 24, 2015), where Wyndham highlighted the substantial expenses it has incurred over the course of the FTC's two-year investigation and nearly three years of litigation, stating that ''[r]esponding to the FTC's wide-ranging discovery has cost Wyndham millions of dollars and required untold hours of work from lawyers and employees within the company.''

[24] Order, 2015 BL 271793 at *16 n.21.

[25] *Id.* at *16 n.22.

[26] *Id.* at *17 n.23.