CELEBRATING 125 Years 1890 2015
Pepper Hamilton LLP
Attorneys at Law
Client Alert
March 13, 2015
Berwyn | Boston | Detroit | Harrisburg | Los Angeles | New York | Orange County | Philadelphia | Pittsburgh | Princeton | Silicon Valley | Washington, D.C. | Wilmington

Is the FTC's Authority Over Consumer Privacy About to Be Limited?

Jan P. Levine | levinej@pepperlaw.com, Angelo A. Stio III | stioa@pepperlaw.com
Matthew A. Chiachetti | chiachettim@pepperlaw.com

Historically, the Federal Trade Commission (FTC) has been the most active federal regulator of data privacy and security. Since its creation, it has pursued hundreds of cases against companies that violated privacy statutes or engaged in unfair or deceptive practices that put consumers' personal information at unreasonable risk. In the area of privacy and security, the FTC has asserted seemingly unbridled authority to protect consumer privacy and ensure data security.

The FTC's broad authority, however, is now under scrutiny by the U.S. Court of Appeals for the Third Circuit in *Federal Trade Commission v. Wyndham Worldwide Corporation*, No. 14-3514 (3d Cir. argued Mar. 3, 2015). At issue in *Wyndham* is whether the FTC's Section 5 power to regulate unfair practices includes the authority to scrutinize a commercial entity's cybersecurity practices and enforce specific cybersecurity standards against an entity.[1]

Background

Wyndham arises from three data breaches that affected various entities within the Wyndham family (the Wyndham Companies) between 2008 and 2009. [2] Following those breaches, the FTC sued the Wyndham Companies in federal court, alleging that they failed to employ "reasonable and appropriate" cybersecurity practices.[3] The FTC argued, among other things, that the Wyndham Companies had inadequate data security policies and procedures, utilized outdated systems, and lacked reasonable measures to detect, prevent and investigate unauthorized access to their network.[4]

Based on these failures and inadequacies, the FTC claimed that the Wyndham Companies engaged in (i) deceptive practices under Section 5(a) of the FTC Act (15 U.S.C. § 45(a)) by failing to comply with representations they made to their customers concerning data security practices (the Deception Claim)[5] and (ii) *unfair* practices under Sections 5(a) and 5(n) (15 U.S.C. §§ 45(a), (n)) by failing to employ "reasonable and appropriate measures to protect personal information against unauthorized access" (the Unfairness Claim).[6]

Wyndham Hotels & Resorts LLC (Wyndham), one of the Wyndham Companies, responded to the FTC by filing a motion to dismiss[7] under Section 5 of the FTC Act. Wyndham also claimed that the court should dismiss the Deception Claim because of the FTC's inadequate pleading.

The district court denied Wyndham's motion, concluding that the FTC Act permitted the FTC to regulate cybersecurity practices[8] and that "fair notice" does not "require[] the FTC to formally issue rules and regulations before it can file an unfairness claim in federal district court."[9] Recognizing the evolving landscape of cybersecurity, the court further explained that Section 5's prohibitions are "necessarily flexible" and intended for "cases arising out of unprecedented situations."[10] According to the court, the FTC's complaints, consent decrees and public guidance materials provide sufficient notice to companies about the FTC's standards for reasonable and appropriate cybersecurity practices.[11]

Wyndham moved to certify the district court's order for interlocutory appeal, and the court granted the motion in June. On March 3, 2015, the Third Circuit held oral argument on this appeal, which could alter the cybersecurity regulatory landscape significantly.

Third Circuit Appeal

On appeal, the parties primarily focused on the following issues in briefing and at oral argument. First, the parties addressed whether the FTC Act authorized the agency to declare what is and what is not an unfair cybersecurity practice. In this regard, the FTC argued that the FTC Act grants the agency broad and flexible authority to regulate unfair practices.[12] Among its arguments, the FTC maintained that Section 5(n) of the Act defines unfair acts and, therefore, is the only limitation on the scope of the agency's authority.[13] Wyndham responded by claiming that the district court incorrectly considered whether an exception for cybersecurity should be "carved out" from the FTC's broad authority.[14] According to Wyndham, the court should have addressed the inverse question: whether the FTC Act extended such authority to the FTC.[15] Contrary to the FTC's position, Wyndham argued that Section 5(a) limits the scope of the FTC's authority, while Section 5(n) sets the necessary criteria for the FTC to consider when assessing the lawfulness of activity within its Section 5(a) scope of authority.[16] Wyndham further argued that recent legislation authorizing the FTC to regulate specific cybersecurity issues, such as the Fair Credit Reporting Act and the Gramm-Leach-Bliley Act, would be unnecessary if the FTC Act already granted the agency the broad authority that it claims.[17]

Second, the parties addressed whether the FTC places commercial entities on adequate notice of what constitutes "reasonable and appropriate" cybersecurity practices. The FTC claimed that its complaints, consent decrees and published guidance establish a body of standards that place companies on notice of what constitutes unreasonable cybersecurity.[18] The FTC also argued that the standard of care it is enforcing reflects basic negligence principles and that all companies — even without published guidance — are aware that they must follow commercially reasonable standards of care.[19] Wyndham, however, contended that the FTC's complaints and consent decrees provide inadequate notice because they are not the result of adjudications on the merits of the underlying issues.[20] Furthermore, these complaints and consent decrees, like the FTC's brochures and guidance materials, lack sufficient specificity to identify unlawful activity.[21] Wyndham also rejected the FTC's position that requiring companies to "act reasonably" satisfies fair notice requirements.[22]

Third, and directly related to the prior two issues, the parties addressed whether the FTC Act grants the agency the authority to pursue claims against companies for unreasonable cybersecurity practices based on a negligence standard. In support of its authority to pursue negligent acts, the FTC relied on prior adjudications, a policy statement and the FTC Act's lack of a specific exemption for "business[es] that expose [themselves] to harm through negligence at the same time that [they] injure customers."[23] Wyndham, on the other hand, argued that "[w]hatever else the term 'unfair' in Section 5 might mean, it surely cannot mean simple negligence."[24] Wyndham noted that the FTC could not identify any court that "deemed allegedly negligent acts *ipso facto* to be 'unfair' practices."[25] Permitting the FTC to adopt this standard would contradict the majority of cases that deem practices to be "unfair" only when they include unscrupulous or unethical behavior.[26]

Fourth, the parties argued about whether the FTC adequately pled a case for "substantial injury" that is not "reasonably avoidable," as required by Section 5(n). According to the FTC, its allegations that consumers faced "unreimbursed charges" and spent "time and money resolving fraudulent charges and mitigating subsequent harm" are sufficient to sustain the complaint.[27] The FTC maintained that it is reasonable to draw such inferences from the scope of Wyndham's data breaches.[28] Wyndham, however, argued that such inferences do not meet the "plausibility" standard of pleading — particularly considering that federal laws and credit card policies limit customers' fraud exposures and, as discovery has proceeded in this case, the FTC has not yet discovered any individual consumer who suffered unreimbursed loss.[29]

Finally, although not specifically briefed by the parties, the court asked them during oral argument to address whether the issue of unreasonable cybersecurity under Section 5 was properly before the federal court, as opposed to first being addressed through the FTC's administrative procedures (*i.e.*, adjudication or rulemaking). Before concluding the argument, the court instructed the parties to submit supplemental briefs on this issue, which are due the week of March 16. Ultimately, if the court determines that the central issue of the case is not properly in federal court, the parties (and the commercial entities tracking this litigation for guidance) may have to wait for another case to get an appellate opinion about the scope of the FTC's authority.

Pepper Points

While commercial entities await the outcome of Wyndham, in-house counsel and corporate privacy officers will be well served to ensure that their data privacy and security practices comply with the privacy policy that is being published to the public. Often, corporate privacy policies and internal practices start on the same page but, with the passage of time and new personnel, diverge from each other. If a corporation is making representations to the public about its data privacy and security policies and is not complying with those representations, it risks exposure to deception claims under Section 5(a) of the FTC Act.

In addition, regardless of how the Third Circuit rules on the Unfairness Claim, in-house counsel and corporate privacy officers should familiarize themselves with FTC complaints, consent decrees and guidance in the area of data privacy and cybersecurity. Doing so will help companies stay current on best practices and reduce the risk that the FTC will challenge their data privacy policies and practices as being inappropriate and unreasonable. Attorneys in Pepper Hamilton's Data Privacy and Security Group can help corporations understand the regulatory environment and reduce the risk of claims that corporate data privacy and security practices are outdated or unreasonable.

Endnotes

1. The FTC's authority to regulate deceptive trade practices under Section 5(a) of the Federal Trade Commission Act (FTC Act) is not at issue in this appeal. The FTC continues to pursue a deception claim against the defendants in district court, and Wyndham has not challenged its legal authority to do so. Wyndham has, however, challenged the deception claim on other grounds. Under its Section 5(a) power to regulate deceptive trade practices, the FTC has pursued claims alleging that entities made representations about their data privacy and security practices and then failed to comply with those representations.
2. *See* First Amended Complaint for Injunctive & Other Equitable Relief ¶¶ 7–11, 26–40, *FTC v. Wyndham Worldwide Corp.*, No. 2:13-cv-01887-ES-JAD (D.N.J. filed Aug. 9, 2012).
3. *See id.* at ¶¶ 44, 47.
4. *See id.* at ¶¶ 24(a)-(j).
5. *See id.* at ¶¶ 44–46.
6. *See id.* at ¶¶ 47–49.
7. Motion to Dismiss by Defendant Wyndham Hotels & Resorts LLC, *FTC v. Wyndham Worldwide Corp.*, No. 2:13-cv-01887-ES-JAD (D.N.J. filed Apr. 26, 2013).
8. *FTC v. Wyndham Worldwide Corp.*, 10 F. Supp. 3d 602, 612–15 (Apr. 7, 2014).
9. *Id.* at 617.
10. *Id.* at 620 (internal quotations omitted).
11. *Id.* at 620–21.
12. *See* Brief for the FTC at 19–20, *FTC v. Wyndham Worldwide Corp.*, No. 14-3514 (3d Cir. filed Nov. 5, 2014).
13. *See id.* at 24–25.
14. *See* Appellant's Opening Brief at 18, *FTC v. Wyndham Worldwide Corp.*, No. 14-3514 (3d Cir. filed Oct. 6, 2014).
15. *See id.*
16. *See id.* at 21–23.
17. *See id.* at 23–28.
18. *See* Brief for the FTC, *supra* note 12, at 44–52.
19. *See id.* at 40–44.
20. *See* Appellant's Opening Brief, *supra* note 14, at 41.
21. *See id.* at 41–45.
22. *See* Appellant's Reply Brief at 19–24, *FTC v. Wyndham Worldwide Corp.*, No. 14-3514 (3d Cir. filed Dec. 8, 2014).
23. *See* Brief for the FTC, *supra* note 12, at 22, 26–27, 29–30.
24. *See* Appellant's Reply Brief, *supra* note 22, at 6.
25. *See id.* at 7.
26. *See id.* at 7–8. Although Wyndham opposes a negligence standard in interpreting Section 5 of the FTC Act, the FTC has explained that the existence of a data breach does not necessarily establish that a company violated the FTC Act. *See* Brief for the FTC, *supra* note 12, at 8, 16. According to the FTC, its action against Wyndham was warranted due to Wyndham's extensive security lapses. *Id.* at 47.
27. *See* Brief for the FTC, *supra* note 12, at 53, 58.
28. *See id.* at 53.
29. *See* Appellant's Reply Brief, *supra* note 22, at 30.