FTC as Data Security Cop Affirmed

Alysa Z. Hutnik, Dana B. Rosenfeld

August 27, 2015

The U.S. Court of Appeals for the Third Circuit this week affirmed the authority of the Federal Trade Commission ("FTC" or "Commission") to enforce against companies that lack reasonable cybersecurity practices. Prior to this ruling, no federal court had adjudicated whether the FTC had authority under 15 U.S.C. § 45(a) ("Section 45(a)") of the Federal Trade Commission Act to bring actions against companies for allegedly deficient cybersecurity practices. This posting discusses key elements of the decision and its implications going forward.

Summary of Wyndham Case

In June 2012, the FTC filed suit against global hospitality company Wyndham Worldwide Corporation and three of its subsidiaries (collectively, "Wyndham"). The Commission alleged that Wyndham's failure to implement reasonable data security safeguards at its franchisee locations allowed computer hackers to breach – on three separate occasions – franchisee computer systems and the company's centralized property management center. This resulted in the breach of financial account information for more than 600,000 hotel customers and a purported $10.6 million in fraud loss. The FTC alleged the following deficiencies, among others, in the company's cybersecurity practices: (i) storage of payment card information in clear readable text; (ii) failure to require strong passwords to access property management systems; (iii) failure to use "readily available security measures" – such as firewalls – to limit access between the property management systems, the corporate network, and the Internet; (iv) failure to employ reasonable measures to detect and prevent unauthorized access or to conduct security investigations; (v) failure to follow proper incident response procedures; and (iv) failure to adequately restrict the access of third-party vendors to its network and company servers. Given the breadth of alleged deficiencies, the FTC claimed the company's privacy policy deceptively misrepresented the extent to which Wyndham safeguarded consumer data.

Rather than challenge the complaint on the merits, Wyndham filed in New Jersey federal district court a motion to dismiss the FTC's complaint. The company argued dismissal was warranted on a number of grounds, including the following two which were considered by the Third Circuit on interlocutory appeal (click here for more complete discussion on the lower court's ruling): whether the FTC had authority to regulate cybersecurity under the "unfairness" prong of the FTC Act; and if so, whether Wyndham had "fair notice" that its specific cybersecurity practices could fall short of that provision. The district court denied the motion, and interlocutory appeal followed.

Third Circuit's Ruling

A. Unfairness

In challenging the FTC's authority to bring an unfairness action against allegedly deficient

cybersecurity practices, Wyndham advanced a novel theory: the familiar three elements of an unfairness claim that are codified at 15 U.S.C. § 45(n) – (i) substantial injury, (ii) that is not reasonably avoidable by consumers, and (iii) that is not outweighed by the benefits to consumers or to competition – were "necessary but insufficient conditions" of an unfair practice. That is, Wyndham argued the plain meaning of the word "unfair" imposed independent requirements that the FTC had not satisfied. For example, the company argued that conduct could only be unfair when it injured consumers "through unscrupulous or unethical behavior" or was otherwise "marked by injustice, partiality, or deception." Such requirements may have at one point played a role in the historical evolution of the unfairness doctrine, but the Third Circuit denounced their applicability within current FTC jurisprudence.

In rejecting Wyndham's arguments, the court opined that the FTC Act contemplated a theory of liability based on tortious negligence. The FTC Act expressly contemplated the possibility that conduct could be unfair *before* actual injury occurs.[1] Further, "that a company's conduct was not the most proximate cause of an injury generally does not immunize liability from foreseeable harm."[2] Thus, companies may be liable under an unfairness theory for a reasonably foreseeable data breach – without evidence of actual injury.

In the alternative, Wyndham argued that Congress intended to exclude cybersecurity from the FTC's unfairness authority by enacting more "tailored grants" of substantive authority through more targeted federal privacy legislation (*i.e.*, COPPA and Gramm-Leach-Bliley). Again, this novel theory was summarily rejected. The Third Circuit held the various federal privacy laws were enacted to expand the FTC's authority over corporate cybersecurity, not merely to establish the FTC's authority in the first instance.

B. Fair Notice

Wyndham argued that, notwithstanding whether its conduct was unfair under Section 45(a), the Commission failed to give fair notice of the specific cybersecurity standards that the company was required to follow. Wyndham claimed that a court could not defer to an agency's interpretation of its own regulations unless private parties had "ascertainable certainty" as to those interpretations. Because the company was not made aware with "ascertainable certainty" of the specific cybersecurity standards on which it would be held accountable, Wyndham asserted that the FTC's interpretation of what constituted minimum security standards was not entitled to deference.

The court rejected this argument, noting that the FTC was not relying on an agency interpretation, rule, or adjudication of minimum cybersecurity standards under Section 45(a). Rather, no such precedence exists because the FTC had not yet declared that cybersecurity practices could be unfair (i.e., its numerous cybersecurity related administrative settlements could not be considered precedential). Thus, the appellate court held the company was not entitled to "ascertainable certainty" of the FTC's interpretation of the specific cybersecurity practices required by Section 45(a). As a result, the relevant question was not if Wyndham had fair notice of the FTC's *interpretation* of the statute, but whether it had fair notice of what the statute *itself* required.

The Third Circuit concluded that Wyndham did not lack fair notice that cybersecurity practices could, as a general matter, form the basis of an unfair practice under Section 45(a). Further, the company had adequate notice as to the importance of conducting a cost-benefit analysis to determine the sufficiency of its cybersecurity measures, including relevant factors, such as:

The probability and expected size of reasonably unavoidable harms to consumers given a certain level of cybersecurity and the costs to consumers that would arise from investment in stronger

cybersecurity.

The Court concluded that Wyndham's argument failed for not arguing (and demonstrating) that its cybersecurity practice would have survived a reasonable interpretation of the cost-benefit analysis required by Section 45(n).

Implications Going Forward

The Third Circuit's *Wyndham* decision is significant for several reasons. The decision provides some support that companies may be liable under an FTC unfairness theory for deficient cybersecurity measures on the basis of likely -- rather than actual – injury to consumers. Further, the decision underscores that companies have "fair notice" that a cybersecurity program may fall within the FTC's jurisdictional scope of Section 45(a), and whether such program is reasonable will turn on the extent to which the program survives a cost-benefit analysis. Thus, a company's data security practices may be reasonable (even if not perfect, and even within the context of a breach), if the company can demonstrate that the potential costs of more robust data security measures would offset any benefit to consumers in the aggregate and to competition.

It also is noteworthy that one of the main themes of Wyndham's allegations in this case is that the FTC has not provided sufficient guidance to businesses on the particular data security measures that businesses should have in place to avoid FTC scrutiny. Perhaps, in part, in response to this allegation, over the past several years, the FTC has made a more pronounced public stamp on such matters, through updated data security publications, practical guidance on data security through blogs, and data security conferences around the country. While cyber threats will continue to evolve, and thus require continually-updated security programs to match such threats, having more FTC guidance on point is a positive trend, regardless of the outcome of the Third Circuit's decision.

[1] Citing *Int'l Harvester*, 104 F.T.C. 949, 1061 (1984) (holding unfairness claims could be brought on the basis of likely rather than actual injury).

[2] Citing Restatement (Second) of Torts § 449 (1965).