FTC v Wyndham: a sea change in regulating cyber security practices

Kurt Wimmer, Partner and co-chair of the global Data Privacy and Cybersecurity practice, and Caleb Skeath, Associate, with Covington & Burling LLP (Washington), examine the significance of the recent decision of the US Third Circuit Court on the FTC's jurisprudence to regulate cyber security practices

In 2008 and 2009, the Wyndham hotel chain was victimized when hackers gained access to Wyndham's internal computer systems. The hackers obtained data from over 600,000 Wyndham customers, and this theft of data led to more than $10 million in fraudulent charges against customer credit cards.

The US Federal Trade Commission (the 'FTC'), the closest analogue the United States has to a data protection authority, began an investigation of the hack. The FTC determined that Wyndham had insufficiently protected its customers' information, and had engaged in unreasonable cybersecurity practices. Unlike some 350 companies that have faced FTC charges of unfair privacy or security practices in the past decade, Wyndham did not agree to settle these charges. Instead it began a frontal challenge against the FTC's authority to regulate cybersecurity practices under the Federal Trade Commission Act (the 'FTC Act').

For the FTC, this was a high-stakes challenge. If it won, the FTC's jurisdiction to regulate cybersecurity practices in the US would be reinforced more strongly than ever before. If it lost, however, it would lose the ability to regulate data security practices.

Following a trial court decision in the FTC's favour, Wyndham appealed the decision to the United States Court of Appeals for the Third Circuit. After months of anticipation, the Third Circuit's decision in *Federal Trade Commission v. Wyndham Worldwide Corp.* provided a ringing and unequivocal endorsement of the authority of the FTC to police data security practices under Section 5 of the FTC Act.

The Third Circuit Court's reasoning

Section 5, a 100-year-old statute, gives the FTC authority to prohibit unfair and deceptive trade practices 'in or affecting commerce,' and the FTC has relied on this general grant of authority to pursue numerous enforcement actions for 'unfair' data security practices over the past decade.

The Third Circuit agreed to hear Wyndham's appeal on two issues: (1) whether the FTC has authority to regulate cybersecurity under the 'unfairness' prong of its Section 5 authority, and (2) if the FTC has such authority, whether Wyndham received fair notice that its cybersecurity practices could fall short of the Section 5 standard.

On the first issue, the Third Circuit rejected Wyndham's arguments that other federal laws regulating narrower areas of privacy could be read to exclude cybersecurity from the reach of the FTC's Section 5 authority. The Third Circuit also rejected Wyndham's contention that the FTC's prior statements disclaimed regulatory authority over cybersecurity practices, finding that these statements acknowledged limitations in the FTC's jurisdiction (such as the inability to regulate what data companies collect) that do not prevent the FTC from regulating cybersecurity practices.

Having concluded that the FTC's Section 5 authority encompasses cybersecurity, the Third Circuit also rejected Wyndham's argument that the FTC's failure to provide 'fair notice' of required cybersecurity practices under Section 5 violated the Due Process Clause of the United States Constitution. The due process clause requires that laws regulating conduct provide 'fair notice' to regulated entities that is at least sufficient for the entities to act in accordance with the law. As part of this argument, Wyndham highlighted the alleged lack of any concrete guidance from the FTC as to what, exactly, constituted 'unfair' cybersecurity practices, and claimed that the FTC failed to define the cybersecurity practices required under Section 5 with 'ascertainable certainty.'

However, the Third Circuit held that Wyndham's 'ascertainable certainty' standard cannot apply if, as in this case, an agency has not issued a relevant 'rule, adjudication, or document' that merits judicial deference. Where no such deference is required, the court can only engage in the 'ordinary judicial interpretation of a civil statute.' Under this standard, the Third Circuit held that Wyndham was not entitled to fair notice of the specific cybersecurity practices required by the FTC under Section 5. Instead, Wyndham was only entitled to fair notice of the general standard that is applicable to all unfairness actions

(Continued on page 4)

(Continued from page 3)

(not just cybersecurity) under the plain text of Section 5. Turning to the second part of the fair notice inquiry, the court held that Wyndham had fair notice that its alleged conduct could 'fall within the meaning of' the text of Section 5. Although it acknowledged that the text of Section 5 is 'far from precise', the court held that the statute provided notice to companies that the 'relevant inquiry here is a cost-benefit analysis...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 would arise from investment in stronger cybersecurity.'

Noting that Wyndham had been hacked three times, the court held that at a minimum, Wyndham was on notice after the second hack that a court could find that its cybersecurity practices failed the cost-benefit analysis under Section 5. The court also noted that the FTC has 'counselled against many of the specific practices alleged here' through its informal guidance as well as its complaints and consent decrees in prior enforcement proceedings raising unfairness claims based on inadequate cybersecurity practices.

The court emphasized the presence of similar allegations in at least five of the FTC's enforcement actions. Even though many of these decisions alleged a collection of violations under Section 5 and did not specify which violations were necessary or sufficient for an unfairness finding, the Third Circuit held that these enforcement actions could help companies gauge the possibility of liability under Section 5.

In addition, the Third Circuit rejected Wyndham's argument that it could not have acted unfairly when it was victimized by hackers, finding that Wyndham's alleged conduct did not fall outside of the 'plain meaning' of 'unfair.'

Notably, the Third Circuit held that an unfairness claim could be brought 'on the basis of likely rather than actual injury.' Although Wyndham's conduct may not have been 'the most proximate cause of an injury' to consumers within the context of the data breaches it suffered, this distinction did not immunise Wyndham from liability for foreseeable harms arising from the breaches.

While the FTC's complaint against Wyndham did allege actual harm to consumers resulting from the breaches in the form of over $10 million in fraudulent charges, this language from the court's decision could allow the FTC to continue bringing enforcement actions where no 'actual' harm to consumers exists.

The impact of the decision on US businesses

The real impact of the *Wyndham* decision lies in its 'fair notice' aspects. By holding that Wyndham had 'fair notice' of the FTC's positions on cybersecurity and data security practices because of (1) public access to prior 'consent orders' settling past FTC data security enforcement cases, and (2) FTC reports on 'best practices' in data security, the Third Circuit endorsed the FTC's efforts to create a body of precedent which it can refer to as a basis for future enforcement actions.

Accordingly, the decision has amplified the importance of these consent orders as data security guidance for US organisations. In light of the decision, FTC publications such as a recently released list of ten 'practical lessons' from its prior enforcement actions, are not just 'best practice' guides but standards which companies might be held to account over.

Conclusion

The question of whether data security practices can constitute an 'unfair trade practice' has been hotly debated for years, and Wyndham is the first decision from a Court of Appeals to hold that the FTC does have this authority. As stated above, the decision's 'fair notice' aspects are extremely significant.

Prior to Wyndham, no Court of Appeals had directly addressed the FTC's authority to regulate data security practices under Section 5 of the FTC Act. Although the Third Circuit has authority only over federal judicial districts in Pennsylvania, New Jersey, Delaware and the Virgin Islands, any decision from a federal Court of Appeals has broad persuasive authority to other US courts.

The decision undoubtedly will have broad influence, and will result in US companies taking a renewed interest in the FTC's published consent orders and reports on cybersecurity.

However, the final word on the *Wyndham* dispute may not yet be written. Wyndham still may petition the United States Supreme Court to review the Third Circuit's decision. Moreover, the Third Circuit's finding also leaves open several avenues for future challenges by other parties to the FTC's data security authority.

Wyndham presented a favourable set of facts for the FTC, as the FTC had previously advised against and pursued enforcement actions on the basis of very similar security issues that it alleged against Wyndham. In a future enforcement proceeding that represents an expansion of the FTC's data security jurisprudence beyond its prior enforcement proceedings and guidance, a company could argue that, unlike Wyndham, it could not have received 'fair notice' from the FTC's prior guidance and enforcement proceedings. While Wyndham solidifies the FTC's authority over data security practices and reaffirms the importance of staying up-to-date on the FTC's data security guidance, it does not foreclose the possibility of other challenges to FTC enforcement actions. Follow-on enforcement actions and litigation will be important to the overall development of the FTC's cybersecurity authority.

Kurt Wimmer and
Caleb Skeath
Covington & Burling LLP
kwimmer@cov.com
cskeath@cov.com