Federal Trade Commission v. Wyndham Worldwide Corporation, et al.

United States District Court for the District of New Jersey (Case No. 2:12-cv-01365-SPL)

The continuing civil action against Wyndham for alleged data security failures has seen Wyndham file a motion to dismiss based on Wyndham's challenge to the FTC's authority to regulate cybersecurity.

Introduction

Over the past decade, the United States Federal Trade Commission (the 'FTC' or 'Commission') has brought cybersecurity enforcement actions against various private companies[1]. Through these actions, the FTC has signaled that it intends to take a lead in setting data security and privacy standards, by imposing tens of millions of dollars in monetary penalties and requiring companies to maintain more stringent data security practices. No company has ever challenged in court the FTC's authority to regulate cybersecurity in this way - until now.

In FTC v. Wyndham Worldwide Corporation, et al.[2], the FTC launched a civil action against the Wyndham parent company and three of its subsidiaries - Wyndham Hotels Group, Wyndham Hotels and Resorts, and Wyndham Hotel Management - for alleged data security failures that the FTC claimed led to three major data breaches in less than two years. Unlike many other data security FTC enforcement actions, in which the defendant chose to cut its losses and settle out of court, Wyndham decided to stand and fight the FTC with a motion to dismiss. The motion is currently pending before Judge Esther Salas of the US District Court for the District of New Jersey. And several major advocacy organisations, including the US Chamber of Commerce, have filed *amicus* briefs to ensure that the Court appreciates the importance of this case of first impression.

Scope of FTC authority

As a general matter, the Commission's stated mission, set forth on www.ftc.gov, is to prevent anticompetitive, unfair, and deceptive business practices while 'enhanc[ing] informed consumer choice and public understanding of the competitive process,' and to 'accomplish this without unduly burdening legitimate business activities.' In support of this mission, the Commission has been bringing data security enforcement actions pursuant to Section 5 of the Federal Trade Commission Act ('FTC Act'), which prohibits 'unfair or deceptive acts or practices in or affecting commerce.' The FTC started regulating cybersecurity in response to certain egregious security lapses. For instance, in 2006 the Commission settled charges against Nations Holding Company based on allegations that - despite its privacy policy promising consumers that it maintained 'physical, electronic and procedural safeguards in compliance with federal standards to protect [their personal] information' - the company tossed consumer home loan applications in an open dumpster.

Noble and valuable as it may be, the FTC's mission is relatively vague and Section 5 of the Act does not offer much in the way of clarity. A wide variety of additional laws have been passed to define (and arguably widen) the scope of the Commission's regulatory authority. Some of these laws - the Gramm-Leach-Bliley Act, the Children's Online Privacy Protection Act, and others - expressly grant the FTC oversight and enforcement authority over data security standards, but these acts confine the Commission's authority to certain industries and situations. According to the Wyndham defendants 'on multiple occasions in the 1990s and early 2000s the FTC publicly acknowledged that it lacked authority to prescribe substantive data-security standards under the [FTC Act]. For that very reason, the FTC has repeatedly asked Congress to enact legislation giving it such authority.' Its congressional lobbying effort notwithstanding, Congress has not granted the Commission broad power to regulate data security.

FTC's case against Wyndham

Although the FTC's authority to bring this suit against the Wyndham defendants is questionable to many, the alleged facts of the case do not seem to cut in the defendants' favour. The Commission's complaint against Wyndham is based on three separate data breaches that occurred between April 2008 and January 2010. Each time, according to the FTC, the hackers were able to gain unauthorised access to the computer networks of Wyndham Hotels and Resorts' and several hotels franchised and managed by Wyndham.

According to the Commission's complaint, Wyndham failed to 'adequately limit access between and among the Wyndham-branded hotels' property management systems, [Wyndham] Hotels and Resorts' corporate network, and the Internet.' The FTC alleges that this failure allowed intruders to use weak access points (e.g., a single hotel's local computer network) to hack into the entire Wyndham Hotels and Resorts' corporate network. From there, the complaint claims, the intruders were able to gain access to the payment management systems of scores of Wyndham-branded hotels.

The Commission alleges that Wyndham failed to remedy known security vulnerabilities, employ reasonable measures to detect unauthorised access, and follow proper incident response procedures following the first breach in April 2008. Thus, the corporation remained vulnerable to the attacks that took place the following year. All told, as set forth in the FTC's complaint, the

intruders compromised over 600,000 consumer payment card accounts, exported hundreds of thousands of payment card account numbers to a domain registered in Russia, and used them to make over $10.6 million in fraudulent purchases.

Based on these factual allegations, the Commission's complaint charges that Wyndham's data security practices were both unfair and deceptive in violation of Section 5 of the FTC Act. Specifically, the Commission claims that Wyndham's failure to 'employ reasonable and appropriate measures to protect personal information against unauthorized access' constitutes unfair acts or practices insofar as they 'caused or are likely to cause substantial injury to consumers that consumers cannot reasonably avoid themselves and that is not outweighed by countervailing benefits to consumers or competition.'

Additionally, the Commission argues that, in light of the Wyndham's failures to protect user data, the defendants' privacy policies are false or misleading and therefore violate the FTC Act's prohibition against deceptive acts and practices. The privacy policies that the FTC is referring to were posted on the Wyndham Hotels and Resorts website and stated that they 'safeguard [their] customers' personally identifiable information by using industry standard practices' and they 'make commercially reasonable efforts to make [their] collection of such information consistent with all applicable laws and regulations.'

Wyndham's motion to dismiss

In most instances, companies faced with similar alleged facts have settled with the Commission in order to reduce litigation cost and the public scrutiny that often attends a protracted enforcement action. For instance - in July of this year, the Commission approved a final order settling charges against HTC America Inc. stemming from allegations that the technology company 'failed to take reasonable steps to secure the software it developed for its smartphones and tablet computers.' The order did not include any monetary sanctions; however, it did outline the steps that HTC must take in order to establish a comprehensive data security plan. As such, as some of the *amicus* claim, in the data security space the Commission has been able to engage in 'regulation-by-settlement,' free of the required judicial and congressional checks on its power. The Commission then points to those (essentially uncontested) settlements as proof of its regulatory authority. In August of last year, Wyndham broke that mould by filing a motion to dismiss.

Wyndham opened its motion to dismiss by highlighting the fact that, to its knowledge, the criminals who hacked into its computer network 'were never apprehended by authorities and no hotel guest suffered financial harm as a result of these crimes.' Wyndham also attempted to put the FTC's arguably egregious factual allegations in context by noting that hacking has become an 'endemic problem,' one that has affected even the most sophisticated private companies and government entities: Google, Microsoft, the CIA, NASA, the FBI, and the FTC itself.

The bulk of Wyndham's motion addresses the FTC's 'unfairness' claim, asserting that it is a classic example of agency overreach. As Wyndham sees it, the Commission is attempting to circumvent the legislative process by acting as if 'it has the statutory authority to do that which Congress has refused: establish data-security standards for the private sector and enforce those standards in federal court.' The Wyndham defendants argue that the unfairness claim must be dismissed for four reasons: (i) the FTC's 'unfairness' authority does not extend to data security; (ii) even assuming that it was authorised to regulate data security, any such requirements would have to be established through proper rulemaking; (iii) Section 5 of the FTC Act does not govern the security of payment card data; and (iv) the unfairness count fails federal pleadings requirements.

Then, in comparatively short shrift, Wyndham attempts to dismantle the FTC's deception claim by asserting that 'the FTC fails to recognize the fundamental distinction between the data collected by [Wyndham Hotels and Resorts] itself (to which the privacy policy applies) and data collected by the independently owned Wyndham branded hotels (to which the policy expressly does not apply).' After quoting the language from the Wyndham Hotels and Resorts' privacy policy that expressly disclaims any responsibility over the branded hotels' security practices and procedures, the defendants argue that, taken as a whole, defendants' privacy policy is not deceptive.

'Friend of the court' (*amicus*) briefs

The defendant's arguments are strong and persuasive. However, because the scope of the FTC's authority to regulate data security is a matter of first impression before the federal courts, several advocacy organisations have filed *amicus* briefs in support of Wyndham to ensure that the court appreciates the reach of its forthcoming ruling.

In a joint effort, four

membership-based business advocacy organisations - the Chamber of Commerce of the United States, the Retail Litigation Center, the American Hotel & Lodging Association, and the National Federation of Independent Businesses - penned one such brief. In it, they note that this is not the first time that the FTC has attempted to 'advance its consumer protection goals in ways far beyond those envisioned by Congress.' They assert that the FTC's current action against Wyndham is emblematic of the Commission's decade-long endeavour to leverage its enforcement authority under Section 5 to 'extract settlements from businesses that themselves have been victimized by data security breaches' without first giving them formal notice of the standards that they are accused of breaching. These organisations are very critical of what they describe as the Commission's use of 'incremental - and unilateral - regulation-through-settlement,' which 'subjects American businesses to vague, unknowable, and constantly changing data security standards.'

Another *amicus* brief was filed jointly by TechFreedom, the International Center for Law and Economics, and Consumer Protection Scholars. Whereas the Chamber, et al. brief was filed to support the interests of their membership, these organisations' interests in the case stems from broader policy perspectives that have aligned around calling the FTC to task. In their words, the questions they raise 'are not about the adequacy of Wyndham's data security practices in particular, or even whether they could conceivably be declared unfair upon a full analysis of the facts and proper development of limiting principles.' Instead, their brief 'speaks to the fundamental problems of vagueness and due process raised by the FTC's routine enforcement actions prior to any adjudication by any court.' Their approach is twofold. First, they are calling on the court to 'demand that the FTC develop the law of data security through rulemakings, and other forms of guidance to give companies notice of how unfairness applies to them.' Second, they are asking that the court to establish pleading standards as a means of reining in the FTC's 'current model of using conclusory allegations to pressure companies to settle.'

Conclusion

The Wyndham defendants are not arguing that the federal government should not regulate data privacy standards, nor are any of the various organisations filing briefs in support of their motion to dismiss. Instead, they claim that the FTC has attempted to circumvent the legislative and administrative rulemaking process. And their arguments are more specific than a general position that overregulation stymies commerce and trade. These companies and advocates suggest that the FTC's approach is particularly harmful because it does not offer clear guidelines for businesses to follow. If a business cannot be sure that it is operating within the scope of a particular federal guideline, then it cannot be certain how to structure its data security procedures, and has no way to protect itself in the event of government enforcement actions and private lawsuits. If the FTC were to use formal notice and comment rulemaking proceedings, the FTC would propose rules and explain its reasoning and interested parties would have an opportunity to provide comments for the FTC to consider. After consideration, the FTC would publish its findings. For Wyndham and the various 'friends of the court,' this would be a preferred, more transparent and proper way to regulate data security.

If Wyndham prevails, the case could usher in a major reduction in FTC enforcement efforts. However, if the court sides with the FTC, the Commission will be further empowered to regulate data security practices. With such high stakes on both sides, any decision is likely to result in an appeal. In the meantime, companies in various industry sectors that maintain personal consumer information are anxiously awaiting the district court's decision.

Michelle W. Cohen Member and Certified Information Privacy Professional (US)
Casselle A.E. Smith Associate
Ifrah PLLC
michelle@ifrahlaw.com
csmith@ifrahlaw.com

1. http://ftcbeat.com/category/cybersecurity/
2. http://www.ftc.gov/os/caselist/1023142/