ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

The Global Impact of FTC v. Wyndham: Another Reason Your Company Should Review Its Privacy and Cybersecurity Programs Right Now

Compliance and Ethics

Technology, Privacy, and eCommerce

CHEAT SHEET

- ***A fuzzy standard.*** The Federal Trade Commission's (FTC) minimum standard of care will likely increase as consumers become even more wary of data security.
- ***Start with security.*** No one can steal what you don't have, so eliminate stockpiles of useless data.
- ***Grant access judiciously.*** Limit internal access to sensitive data to only those who require a connection.
- ***Segment your network.*** Limit damage to your network by maintaining internal barriers to quarantine malicious elements when they appear.

In case there was any doubt, the *FTC v. Wyndham*[1] decision makes clear that there is a new sheriff in town when it comes to holding businesses accountable for cybersecurity breaches that harm consumers. That sheriff is the Federal Trade Commission (FTC).

The FTC is an independent agency within the executive branch of the United States government, but the Commission's activities impact businesses and consumers globally. In recent years, the FTC Bureau of Consumer Protection's Division of Privacy and Identity Theft (Division) has set the standard for regulating the cybersecurity practices of companies conducting business in the United States. The Division has brought more cybersecurity-related privacy enforcement actions against businesses on behalf of consumers and published more guidelines than any other US regulator.

The Division also takes a leading role coordinating with other regulators such as the Department of Health and Human Services Office of Civil Rights, Consumer Financial Protection Bureau and Department of Commerce in an effort to foster consistent approaches to cybersecurity and consumer privacy across industries.[2] For example, recent FTC guidelines incorporate many of the same cybersecurity principles articulated in the voluntary Cybersecurity Framework created by the National Institute of Standards and Technology (NIST).[3] The NIST framework, intended to provide guidance for critical infrastructure organizations, has also become a popular tool for other industries to better manage cyber risk.

Similarly, the FTC has cross-border jurisdictional authority under the US Safe Web Act[4] and works with consumer protection authorities around the world on enforcement and policy matters through informal and formal agreements. The FTC is also responsible for enforcing the recently invalidated EU-US Safe Harbor Agreement that places consumer privacy-based restrictions on the transfer of personal data from Europe to the United States.[5] Simply stated, in-house counsel should understand how the FTC influences cybersecurity standards globally and why the *FTC v. Wyndham* decision will impact the breadth of the FTC's policing authority in the future.

1 *Federal Trade Commission v. Wyndham Worldwide Corp*., 799 F.3d 236, (3d Cir. 2015.

2 The FTC's powers generally do not extend to certain industries such as federally regulated financial institutions or the telecommunications and transportation industries.

3 The U.S. NIST Cybersecurity Framework is a tool to help critical infrastructure industries assess

and improve their current cybersecurity posture in the much like the European Union Directive on Critical Infrastructure.

4 15 U.S.C. § § 41 et seq.

5 At the time of publication, negotiations to replace the invalidated EU-US Safe Harbor Agreement have been ongoing.

Wyndham's surprising response to the FTC's allegations

Playing the role of consumer cybersecurity sheriff is really nothing new for the FTC. Since 2002 the FTC's Bureau of Consumer Protection has secured more than 50 data security settlements against businesses for allegedly deficient cybersecurity practices that failed to protect consumer data against hackers. Alleged lapses have included everything from businesses misrepresenting how consumer data would be used on their websites, to failure to encrypt consumer credit and debit card information. Given the steady rise in cybersecurity related enforcement actions filed by the FTC, most observers were not surprised when the FTC filed a complaint against Wyndham Worldwide Corporation (Wyndham) on behalf of consumers in 2012.

The FTC's complaint alleged that Wyndham engaged in unfair and deceptive cybersecurity practices that "unreasonably and unnecessarily exposed consumers' personal data to unauthorized access and theft."[6] Among other things, alleged exposures included insufficient encryption, the use of weak passwords, and the failure to follow proper incident response procedures. As with other cases, the FTC relied on Section 5 of the FTC Act,[7] which prohibits "unfair or deceptive acts or practices in or affecting commerce" as the legal basis for initiating the action.

The FTC claimed Wyndham's exposure led to hackers stealing personal and financial information from hundreds of thousands of consumers on three different occasions in 2008 and 2009. They also alleged the theft resulted in fraudulent charges exceeding US$10.6 million dollars. Given the seriousness of the allegations and the fact that defendants in other cases settled with the FTC, many onlookers expected Wyndham to follow suit. But Wyndham responded differently.

Wyndham refused to settle at the administrative proceeding stage and challenged the FTC's Section 5 authority in the US District Court for the District of New Jersey by filing a motion to dismiss the complaint. Although District Judge Esther Salas denied Wyndham's motion to dismiss the complaint, the Third Circuit Court of Appeals granted interlocutory appeal on the following two issues: (1) whether the FTC has authority to regulate cybersecurity under the unfairness prong of Section 5; and, (2) if so, whether Wyndham had fair notice its specific cybersecurity practices could fall short of that provision.

For businesses across many industries, this was the canary in the coal mine they had been waiting for — Wyndham's decision not to settle with the FTC meant the scope of the FTC's Section 5 authority would finally be tested. Many cases before and after Wyndham hinged on the FTC's authority under the "deception" prong of Section 5 and involved companies providing false data security or privacy representations to consumers via their company websites and applications. Since the deceptive nature of these policies was often obvious and businesses often preferred to avoid negative publicity rather than fight, these cases settled.

Contrary to these routine "deception" cases, the FTC's authority to regulate the cybersecurity practices of businesses under Section 5's "unfairness" prong was less clear. The FTC first asserted

"unfair" cybersecurity practices in 2005[8] and like the "deception" cases, the "unfairness" cases settled. Many businesses, including Wyndham, believed the FTC's enforcement activity had exceeded the scope of their regulatory authority under the "unfairness" prong of Section 5. Now Wyndham would have the opportunity to test that theory in court. A victory would weaken the FTC's case and other businesses would reap the benefit of buying more time to review and improve their own cybersecurity programs thanks to Wyndham. A loss, on the other hand, would help validate the FTC's broad interpretation of their authority under Section 5's "unfairness prong" and weaken Wyndham's overall case.

With the stage set, many onlookers anxiously awaited the appellate court's decision and on August 24, 2015, the Third Circuit helped solidify the FTC's expanded Section 5 authority by unanimously rejecting both of Wyndham's arguments on appeal. Following a detailed explanation of the FTC's historical regulatory authority, the appellate court first rejected several of Wyndham's arguments that the "unfairness" prong of Section 5 should be narrowly construed. For example, in response to Wyndham's argument that its conduct did not meet the plain meaning of the word "unfair," the court stated:

> "A company does not act equitably when it publishes a privacy policy to attract customers who are concerned about data privacy, fails to make good on that promise by investing inadequate resources in cybersecurity, exposes its unsuspecting customers to substantial financial injury, and retains the profits of their business."[9]

Next, the court addressed Wyndham's argument that it lacked fair notice. Among other things, Wyndham argued that even if the FTC possessed Section 5 authority to bring an "unfairness" claim, they failed to provide "fair notice" of what was required of Wyndham. In their brief, Wyndham had argued that the FTC had chosen to act as a "roving cybersecurity prosecutor."

> "The commission has simply anointed itself a roving cybersecurity prosecutor — but, unlike other prosecutors, one that seeks to define the offense and to do so after the fact…"[10]

Despite the spirited argument, the Third Circuit rejected the "notice" argument and ruled Wyndham did not prove the FTC failed to provide "fair notice" that their cybersecurity practices were "unfair" under the statute. Among other things, the court cited the FTC's issuance of a guidebook in 2007 titled: *Protecting Personal Information: A Guide for Businesses*, which describes a checklist of practices that form a sound "data security plan," in support of its position.[11]

6 *Id*. at 8

7 codified as 15 U.S.C. § 45(a).

8 See In the Matter of BJ's Wholesales Club, Inc., No. 042-3160 (June 16, 2005) (BJ's settles with FTC based on charges that its failure to take appropriate security measures to protect consumer credit and debit card information resulted in an unfair practice).

9 *Id.* at 17.

10 www.law360.com/articles/585059/wyndham-fires-opening-salvo-in-ftc-data-security-appeal.

11 *Id.* at 41.

What about the LabMD decision?

Importantly, the Wyndham decision falls short of conclusively validating the scope of the FTC's Section 5 authority under the "unfairness" prong for a number of reasons. First, the case is fact specific and different facts may have supported a different conclusion. Second, the appellate court did not consider all of Wyndham's arguments on appeal.[12] Third, the court hinted that it may entertain a different and better argument in support of Wyndham's position that the FTC failed to provide "fair notice."[13] Fourth, although no appeal has been made yet, Wyndham could appeal the ruling to the US Supreme Court if settlement negotiations with the FTC break down. Lastly, the decision is not binding on other circuits — meaning other courts could rule differently in the future.

In fact, a recent Administrative Law ruling, coming off the heels of the Wyndham decision, may impact Wyndham' restricts the scope of the FTC's "unfairness" authority, albeit on different grounds. Similar to Wyndham, the FTC filed an administrative complaint against LabMD in August 2013, alleging that LabMD was liable for unfair acts or practices in violation of Section 5 of the FTC Act, 15 U.S.C. § 5(a), because it had failed to provide "reasonable and appropriate security" to protect personal information on its computer networks. Chief Administrative Law Judge Chappell dismissed the case on the grounds that the FTC was unable to show by a preponderance of the evidence that LabMD's "alleged unreasonable data security caused, or is likely to cause, substantial consumer injury."[14]

Although the FTC's ability to prove substantial consumer injury was not an issue on appeal in Wyndham, distinguishing the two cases is important. The FTC's claim against LabMD hinged on the alleged exposure of 1,718 pages (1,718 File) of electronic files containing the personal information of approximately 9,300 patients that was posted to a peer to peer sharing network called LimeWire. The 1,718 File was first reported to LabMD by a data security company as part of that company's strategy to secure a contract with LabMD to remediate the apparent security lapse.

The FTC's case began to unravel when a former employee of the security company testified that his company routinely engaged in what amounted to elaborate scams to induce customers like LabMD into believing they had experienced a security breach even when none had occurred. The employee's testimony essentially prevented the FTC from offering reliable evidence to show that any electronic files were unreasonably protected by LabMD, let alone exposed. As a result, Judge Chappell found that the FTC failed to meet the "substantial injury" element for establishing a Section 5 unfairness claim.[15] In doing so, Judge Chappell distinguished LabMD from Wyndham by explaining that unlike LabMD, Wyndham involved "actual harm" resulting from stolen "personal and financial information for hundreds of thousands of consumers leading to over US$10.6 million in fraudulent charges."[16] Although the outcomes are different, the LabMD and Wyndham decisions are consistent and should be read together. Wyndham is the first case to validate the FTC's authority to regulate cybersecurity under Section 5's "unfairness" prong and serves as a strong endorsement of the FTC's expanded role as consumer cybersecurity sheriff moving forward. On the other hand, the LabMD ruling sets a high bar for the FTC to successfully pursue Section 5 "unfairness" claims that are merely "likely" to cause substantial injury to consumers.

More specifically, LabMd requires a showing that substantial injury to consumers is probable, (i.e., likely), not merely possible, when there is no evidence of actual consumer injury. Judge Chappell goes on to explain establishing liability on the basis of "likely" harm is inherently difficult:

> "[i]n light of the inherently speculative nature of predicting "likely" harm, it is unsurprising that, historically, liability for unfair conduct has been imposed only upon proof of actual consumer harm."[17]

The interplay between these two cases begs the question: What are the ramifications for businesses?

12 4 For example, the appellate court did not review Wyndham's argument under the "deception" prong of Section 5 of the FTC Act, but dicta suggests the argument would not have been persuasive.

13 5 The appellate court indicated Wyndham may have an opportunity to argue for the application of a stronger "fair notice" requirement later in the proceedings. However, given the significant increase in settlements, guidelines and public outreach campaigns by the FTC since 2008, future defendants will be hard pressed to persuade courts they lacked "fair notice."

14 *Id.* at 59.

15 Three elements of an unfairness claim are required under Section 5(n). These are that the defendant (1) engaged in acts or practices that caused or were likely to cause substantial injury to consumers, (2) that such injury is not reasonably avoidable by consumers themselves and (3) the injury is not outweighed by countervailing benefits to consumers or to competition. 15 U.S.C. § 45(n).

16 *Id.* at 55.

17 *Id.* at 56.

Ramifications for businesses

Although the LabMD decision may curtail the number of cases the FTC brings, the scope of the FTC's authority to regulate cybersecurity under the "unfairness" prong of Section 5 has been judicially validated by an appellate court for the first time in Wyndham. This broadened authority is likely to result in more regulatory activity and enforcement action by the FTC despite LabMD's limiting effect. The Wyndham decision is also important because it means FTC guidelines and enforcement activities will continue to define the standard of cybersecurity care required by businesses operating in the United States in lieu of more formal and potentially clearer rules.

Barring a contradictory appellate court ruling,[18] the issuance of formal FTC rules, guidance, or legislation, the minimum standard of cybersecurity care required of businesses will evolve much like common law. That means minimum standards of care are likely to increase over time as cybersecurity awareness increases and new guidelines and case decisions are issued. What the FTC deems as "reasonable and necessary" cyber readiness today could very well be deemed unreasonable in the future. That means in-house counsel must remain diligent when it comes to monitoring new FTC cases and guidelines.

The Wyndham decision may also embolden regulators in other industries to act more aggressively without issuing additional formal rules to guide businesses. Regulators across financial, healthcare, and other sectors have already followed the path blazed by the FTC and stepped up their own enforcement activities. For example, the Consumer Financial Protection Bureau recently ordered an auto finance company to pay consumers US$41.1 million in relief for illegal debt collection practices.

In April, 2015, the Federal Communication Commission reached a US$25 million settlement agreement involving the disclosure of personal information from nearly 300,000 citizens due to an alleged data breach. US regulators are increasingly following the FTC playbook by issuing guidance, bringing enforcement actions, and reaching settlement — a trend that is likely to continue.

Stepped up regulatory activity in the United States is driven in part by ongoing international suspicion directed at US businesses and governments following revelations of government spying by former US defense contractor Edward Snowden. Importantly, FTC guidelines and enforcement activities are increasingly aligning with the privacy, principles Europeans and other regions hold sacred which impacts both consumers and business. On one hand, both foreign and domestic consumers want to make sure their private data is adequately protected. On the other hand, businesses need to be familiar with privacy laws in each country where they do business to assure privacy requirements are met in those jurisdictions. Given the FTC's important influence on both fronts, understanding the standard of cybersecurity and consumer protection care required by the FTC is important for in-house counsel both domestically and internationally.

The relevant standard of care the FTC articulated in Wyndham and other cases require businesses to take "reasonable and necessary measures" to protect consumer data. Although the FTC has not provided bright line rules defining what constitutes "reasonable and necessary measures" for implementing a cybersecurity program, they have provided guidance.

For example, the FTC provides tips and advice for businesses, commission leaders have engaged in public outreach, and settlement agreements are published on the FTC's website. Arguably the most important of all these resources is the FTC's recent publication in June of 2015 titled: *Start with Security, A Guide for Business, Lessons Learned from FTC Cases.* Considering the court in Wyndham relied on the publication of the 2007 guidebook mentioned earlier to support its position that Wyndham had notice of what was required, the importance of the 2015 guide cannot be overemphasized.

The 2015 guide distills important facts from over 50 FTC cases into 10 important lessons that are summarized and expanded upon below. Sharing and collectively discussing these lessons with internal information security, privacy, and legal department stakeholders will go a long way toward helping any business implement "reasonable and necessary" cybersecurity measures to protect sensitive data. Perhaps more importantly, adhering to these standards will help businesses subject to the FTC's jurisdiction avoid an FTC enforcement action even if a data breach or loss occurs.

18 Given that LabMD and Wyndham are distinguishable, it is unlikely that Wyndham will be able to successfully challenge the FTC's showing of an actual or likely substantial consumer injury at this stage in the proceedings.

1. Start with security

Although securing sensitive information is critical, no one can steal what you don't possess. That means organization should limit the collection of personal information from consumers to only what they need. Keeping information longer than necessary and for reasons other than legitimate legal or business purposes makes no sense. Eliminating stockpiles of useless information is the backbone of a good information governance plan and a critical data security factor.

2. Control access to data sensibly

If there is a legitimate legal or business purpose for holding sensitive data, reasonable steps should be taken to secure that data. That not only means protecting data from outsiders, but also limiting access to data internally to only those who require access. Training employees and segregating sensitive data can go a long way toward controlling data access. However, the risk of loss and theft can be further reduced and streamlined with data loss prevention technology that can automatically prevent unauthorized access to data designated as sensitive or confidential.

3. Require secure passwords and authentication

Requiring employees and customers to use complex and different passwords is a critical data protection step that is commonly overlooked. Passwords like “admin” or “1234” are nearly equivalent to not using a password. Similarly, storing password credentials securely is necessary to prevent bad guys from accessing your password piggy bank. Pass phrases that include numbers and unique characters are stronger and far less likely to become compromised and the use of two factor authentication adds an even stronger layer of security.

4. Store sensitive personal information securely and protect it during transmission

Data doesn’t stay in one place, but sensitive data should be secured at all times. If transmitting information is necessary for your business, the data should be encrypted and secured during the transmission using industry tested standards and reliable technology. Remember, technology is not enough. Make sure encryption technologies are properly configured, deployed and updated or they may not be effective.

5. Segment your network and try to monitor who is trying to get in and out

Firewall tools are an important way to segregate your network and to prevent the spread of digital diseases like viruses and malware across the organization. Similarly, intrusion detection and prevention monitoring tools may be able to prevent unauthorized access or at least limit damage if the network is penetrated. Tools and services exist to help monitor for malicious activity. Failure to use them may be a red flag for the FTC.

6. Secure remote access to your network

If employees, clients, or service providers are given remote access, steps should be taken to secure remote access to the network. Limiting what can be remotely accessed in your network and using firewalls is a logical first step. However, securing the computers and other devices used to remotely access the network with anti-malware software and other endpoint protection software is equally important.

7. Apply sound security practices when developing new products

If you plan to ship the hottest new “app” or software product, have you thought about whether customers will use your solution to store or send personal data? If they will, then you need to make sure the data is secure. That means training engineers to use secure coding practices that prevent or reduce the risk of introducing security flaws during product design. Following platform guidelines when writing code along with testing and verifying privacy features prior to deployment are important steps that can help reduce security risk.

8. Make sure your service providers implement reasonable security measures

Implementing reasonable security within your organization alone is not enough. Third party service providers and business partners should be required to sign written agreements to provide appropriate security. However, the FTC has also indicated written contracts might not be enough because security can't be "a take our word for it" thing. Additional steps should be taken to actually verify that service providers and business partners are complying with your company's reasonable security standards.

9. Put procedures in place to keep your security current and address vulnerabilities that may arise

Securing software and networks is an ongoing process that requires continuous monitoring and remediation. At a minimum, that means third party software must be updated regularly to patch vulnerabilities. Similarly, companies developing their own commercially available software should also have a process in place for reporting and addressing security vulnerabilities. Simple steps like regularly updating security software and establishing a routine reporting and correction procedure are fundamental components of a reasonable security strategy.

10. Secure paper, physical media, and devices

Sensitive information can easily be exposed when not properly secured regardless of whether it exists in paper or electronic format. Important paperwork should be maintained in secure locations and deleted when it is no longer needed. Similarly, media such as laptops, hard drives, flash drives, and mobile phones should be properly secured so information can be protected if those devices are lost are stolen. Wiping decommissioned hard drives, and devices, utilizing mobile management software, and shredding unneeded paper documents helps eliminate downstream security risks.

Conclusion

The importance of the *FTC v. Wyndham* decision cannot be understated. The FTC was established on September 24, 1914, to protect consumers and promote competition. Although the identity and privacy threats facing consumers have evolved significantly over the past 100 years, there is no doubt the FTC intends to broadly regulate the cybersecurity practices of businesses in today's modern landscape. The Wyndham decision validates this broadened authority and puts companies on notice that FTC guidelines and cases form the standard of care for defining what constitutes "reasonable and necessary" security practices when it comes to consumer privacy. Although the FTC might not be a "new" sheriff, there is little doubt that the sheriff's authority and global impact are far reaching and important in the realm of consumer privacy and cybersecurity regulation.

Matthew Nelson

Attorney

Symantec’s corporate strategy department

He monitors privacy and data security policy developments important to Symantec’s global business strategy. Nelson also serves as the company information governance champion and is membership chair of ACC’s Information Governance Committee.