Bloomberg BNA

Privacy and Security Law Report®

The FTC as Data Security Regulator: *FTC v. Wyndham* and Its Implications

BY WOODROW HARTZOG AND DANIEL J. SOLOVE

In the field of data security law, hardly any case has had as much at stake as *Federal Trade Commission v. Wyndham*. The FTC has been the leading regulator of data security for the past 15 years, and the scope of its power had not been challenged until this case. The long-awaited federal district court opinion in *FTC v. Wyndham* has finally been released,[1] and the FTC has emerged the winner of round one. Though this dispute seems far from over, this decision is a big win for the agency as it seeks to protect consumer data.

For more than 15 years, the FTC has regulated data security through its authority to regulate unfair and deceptive trade practices. In the late 1990s, the first complaints were brought under a theory of deception based upon a company's failure to honor its own promises of data security, usually made as part of a privacy policy.

About a decade ago, the FTC also began to allege that inadequate data security was an unfair trade practice regardless of whether good data security was promised. Every complaint filed by the FTC settled. But then, Wyndham Worldwide Corp. refused to settle and challenged the FTC's complaint in federal court. Soon afterwards, LabMD Inc. also pushed back against the FTC.[2]

Wyndham's challenge was quite significant, as it argued that the FTC lacked authority to regulate data security under its unfairness authority and that the FTC has failed to provide fair notice of what constitutes actionable data security practices. If Wyndham were to prevail, the FTC's power to regulate data security would be significantly diminished.

On April 7, the U.S. District Court for the District of New Jersey issued its long-awaited opinion in the case. The court rejected Wyndham's calls to create a data security exception to the FTC's broad authority to regulate unfair practices under Section 5 of the FTC Act. The court also rejected Wyndham's assertion that the FTC must formally promulgate regulations before bringing an unfairness claim as well as Wyndham's argument that the FTC failed to provide fair notice of what constitutes an unfair data security practice.

The implications of this case could not be more important for data security as well as for privacy. Since the late 1990s, the FTC has ascended into its position as the leading regulator of data security and privacy. Case by case, the FTC has been developing a substantial body of jurisprudence around data security and privacy, filling a critical void in U.S. privacy law. More litigation

[1] *FTC v. Wyndham Worldwide Corp.*, No. 2:13-cv-01887-ES-JAD, 2014 BL 94785 (D.N.J. Apr. 7, 2014), *available at* http://www.bloomberglaw.com/public/document/FTC_v_Wyndham_Worldwide_Corp_No_213cv01887ESJAD_2014_BL_94785_DNJ (*see related report*).

[2] *See* Verified Complaint for Declaratory and Injunctive Relief, *LabMD, Inc. v. FTC*, No. 1:14-cv-00810-WSD (N.D. Ga. Mar. 20, 2014) (13 PVLR 513, 3/24/14).

Woodrow Hartzog is an assistant professor at Samford University's Cumberland School of Law and an affiliate scholar at the Center for Internet and Society at Stanford Law School.

Daniel J. Solove is the John Marshall Harlan research professor of law at George Washington University Law School and the chief executive officer of TeachPrivacy, http://teachprivacy.com, a privacy and data security training company. Solove is also a senior policy adviser at Hogan Lovells US LLP.

All the views in this article are the opinions of the authors and should not be attributed to any of the institutions with which the authors are affiliated.

 ISSN 1538-3423

in this case likely remains, so this decision will likely not be the final word. But for now, the FTC has won the initial battle, and has done so in a decisive way.

The FTC and Its Role in Data Protection

In our recently published article ''The FTC and the New Common Law of Privacy,''[3] we explain how and why the FTC has become the most influential privacy and data security regulator in the U.S. This is particularly true with respect to data security because there is no one general law mandating that companies have good data security practices regarding the personal data they collect and maintain. While a few specific industries such as finance and health care are obligated to take certain procedural and technical safeguards under rules promulgated according to the Gramm-Leach-Bliley Act and the Health Insurance Portability and Accountability Act, most companies have no federal obligation outside of the FTC's efforts to secure personal data.[4]

The FTC has policed privacy and data security through its broad power under Section 5 of the FTC Act. Under Section 5, ''unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful.''[5] Deceptive trade practices are defined by the FTC as material representations, omissions or practices that are likely to mislead a consumer acting reasonably in the circumstances to the consumer's detriment.[6] Even vague promises of security, such as providing ''reasonable security measures to protect against unauthorized access to or unauthorized alteration, disclosure or destruction of personal information,'' can be the basis of an FTC action.[7]

The FTC defines an ''unfair'' trade practice as one that ''causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and is not outweighed by countervailing benefits to consumers or competition.''[8] This test, codified in Section 5(n) of the FTC Act, has come to be known as the ''three-part test.''

The FTC has refrained from providing a checklist of uniformly acceptable data security practices or focusing on one single practice as actionable. Instead, the FTC has taken a holistic approach and relied upon on industry standards and other norms to identify a particular set of practices that, taken together, constitute adequate security practices for companies collecting personal information.

In evaluating whether a trade practice is unfair, the FTC focuses largely on ''substantial injury to consumers.'' The FTC is not limited to the traditional kinds of injuries cognizable in other areas of law, such as tort or contract. The FTC can remedy not just harm to particular consumers but to society in general. The harm need not be monetary or physical, though such injuries are commonly considered ''substantial.'' Additionally, the harm can consist of a risk rather than an actual loss. Thus, a monetary, health or safety *risk* can be a substantial injury even if that risk has not materialized into an actual injury. A practice need only to be likely to cause substantial injury to consumers.[9]

The FTC views data security as a process that is sensitive to contexts such as ''the particular circumstances of the Web site, including the risks it faces, the costs of protection, and the type of the data it maintains.''[10] The data security complaints filed by the FTC contain common allegations, which include: failure to use readily available security technologies like encryption; failure to train employees in data security and limit employee and third-party vendor access to data; failure to implement measures to assess security risks, detect unauthorized access and remedy vulnerabilities; failure to engage in data minimization practices; and failure to take common security measures, such as changing default settings, installing updates and using sufficiently protective user names and passwords.

The FTC's Allegations Against Wyndham

In its amended complaint, the FTC alleged that Wyndham, a company that manages hotels and sells time-shares, suffered a series of three breaches using similar techniques to access personal information stored on the Wyndham-branded hotels' property management system servers, including ''customers' payment card account numbers, expiration dates, and security codes.''[11]

The FTC claimed that ''[a]fter discovering each of the first two breaches, Defendants failed to take appropriate steps in a reasonable time frame to prevent the further compromise of the Hotels and Resorts' network.''[12] According to the FTC:

> Defendants' failure to implement reasonable and appropriate security measures resulted in the three data breaches described above, the compromise of more than 619,000 consumer payment card account numbers, the exportation of many of those account numbers to a domain registered in Russia, fraudulent charges on many consumers' ac-

---

[3] Daniel J. Solove and Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 Colum. L. Rev. 583 (2014), *available at* http://ssrn.com/abstract=2312913.

[4] A few states have data security laws, the most powerful one being Massachusetts. 201 Mass. Code Regs. § 17.03; *see also* Ark. Code Ann. § 4-110-104(b) (Supp. 2007); 2008 Conn. Acts No. 08-167 (Reg. Sess.); Nev. Rev. Stat. Ann. § 603A.210 (West Supp. 2007); N.C. Gen. Stat. § 75-64(a) (2007); Or. Rev. Stat. Ann. § 646A.622(1) (West Supp. 2008); R.I. Gen. Laws § 11-49.2-2(2) (Supp. 2007); Utah Code Ann. § 13-44-201(1)(a) (Supp. 2007). States have been quick to adopt data security breach notification laws, but they have generally not promulgated laws that directly address data security practices.

[5] 15 U.S.C. § 45(a)(1).

[6] *FTC Policy Statement on Deception*, http://www.ftc.gov/ftc-policy-statement-on-deception.

[7] Complaint, *In re Compete, Inc.*, FTC File No. 102 3155, Docket No. C-4384 (F.T.C. Feb. 20, 2013), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2013/02/130222competecmpt.pdf.

[8] 15 U.S.C. § 45(n).

[9] FTC Act Amendments of 1994, H.R. 2243, *codified at* 15 U.S.C. § 45(n).

[10] FTC, *Privacy Online: Fair Information Practices in the Electronic Marketplace* (May 2000), *available at* http://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf.

[11] First Amended Complaint for Injunctive and Other Equitable Relief at 13, *FTC v. Wyndham Worldwide Corp.*, No. 2:13-cv-01887-ES-SCM, (Aug. 9, 2012), *available at* http://www.bloomberglaw.com/public/document/Federal_Trade_Commission_v_Wyndham_Worldwide_Corporation_et_al_Do/5.

[12] *Id.*

  PVLR ISSN 1538-3423

counts, and more than $10.6 million in fraud loss. Consumers and businesses suffered financial injury, including, but not limited to, unreimbursed fraudulent charges, increased costs, and lost access to funds or credit. Consumers and businesses also expended time and money resolving fraudulent charges and mitigating subsequent harm.[13]

The FTC claimed that Wyndham deceptively stated in its privacy policy that it protected its customers' personal information by using '' 'industry standard practices' '' and '' 'a variety of different security measures designed to protect personally identifiable information from unauthorized access by users both inside and outside of our company, including the use of 128-bit encryption based on a Class 3 Digital Certificate issued by Verisign Inc.' ''[14] Other allegedly deceptive statements included a promise that Wyndham takes '' 'commercially reasonable efforts to create and maintain fire walls and other appropriate safeguards to ensure that to the extent we control the Information, the Information is used only as authorized by us and consistent with this Policy, and that the Information is not improperly altered or destroyed.' ''[15] The FTC alleged that Wyndham actually provided deficient data security practices contrary to their representations of following ''industry standard practices.''

In addition to claiming deceptiveness, the FTC also faulted Wyndham's data security practices on unfairness grounds. Specifically, the FTC identified practices that ''unreasonably and unnecessarily exposed consumers' personal data to unauthorized access and theft.''[16] Among other things, the FTC alleged that Wyndham: failed to use readily available access guards (firewalls); allowed misconfiguration, resulting in the storage of credit card information in clear text; failed to ensure implementation of adequate security policies before connecting to the main network; and failed to remedy known security vulnerabilities (for example, by connecting to insecure servers with outdated operating systems unable to get security patches). Wyndham also allegedly: allowed computers with well-known default user IDs to connect to the network; failed to make passwords hard to guess; failed to inventory networked computers; failed to employ reasonable measures to detect and prevent unauthorized access; failed to follow proper incident response procedures, including monitoring for malware post-breach; and failed to adequately restrict third-party vendor access.

Wyndham's Arguments and the Court's Opinion

Regarding unfairness, Wyndham Hotels and Resorts LLC, a subsidiary of Wyndham Worldwide, made three principal arguments in its motion to dismiss: (1) the FTC unfairness authority does not extend to data security; (2) the FTC has failed to give fair notice of what data security practices are required by law; and (3) Section 5 does not apply to the security of payment card data because there is no possibility for consumer injury.[17]

U.S. District Judge Esther Salas resolved each of these issues in favor of the FTC and denied Wyndham's motion to dismiss.

The FTC's Authority Over Data Security

Regarding the scope of the FTC's Section 5 authority, Wyndham asserted that the ''overall statutory landscape'' made it clear that unfairness authority does not extend to data security.[18] For example, Wyndham noted that Congress has enacted targeted data security legislation elsewhere yet failed to create a statute explicitly authorizing the FTC to regulate data security. Relying on *Food and Drug Admin. v. Brown & Williamson Tobacco Corp.*, Wyndham argued that these targeted statutes demonstrated that the FTC lacked broader authority to regulate in this area.[19]

Judge Salas rejected Wyndham's argument and concluded that the FTC has broad power under Section 5 to support its exercise of authority, and the context-specific data security statutes simply enhance data security authority in certain contexts by removing consumer injury requirements, granting the FTC additional enforcement powers that it otherwise lacks and affirmatively compelling (rather than merely authorizing) the FTC to use its authority in particular ways.

Judge Salas wrote that Wyndham ''fails to explain how the FTC's unfairness authority over data security would lead to a result that is incompatible with more recent legislation and thus would 'plainly *contradict* congressional policy.' ''[20] In other words, because Congress's actions all seem to complement, not preclude, the FTC's authority over data security, this dispute is not similar to the FDA's repudiated authority over tobacco products at issue in *Brown & Williamson*.

Wyndham also argued that, like the FDA in *Brown & Williamson*, the FTC disclaimed authority to regulate data security under Section 5's unfairness prong. Judge Salas, however, rejected the comparison: ''[T]he Court is not convinced that these statements, made within a three-year period, equate to a resolute, unequivocal position under *Brown & Williamson* that the FTC has *no* authority to bring *any* unfairness claim involving data security.''[21] The court noted that the FTC actually ''brought unfairness claims in the data-security context shortly after these representations. And the FTC's subsequent representations confirm its authority in this arena, not deny it.''[22]

Fair Notice

Regarding fair notice, Wyndham argued that the FTC ''has not published any rules or regulations that might provide the business community with ex ante notice of

[13] *Id.* at 17–18.
[14] *Id.* at 9.
[15] *Id.* at 9–10.
[16] *Id.* at 10.

[17] Motion to Dismiss by Defendant Wyndham Hotels & Resorts LLC, *FTC v. Wyndham Worldwide Corp.*, No. 2:13-cv-01887-ES-JAD, 2014 BL 94785 (D.N.J. Apr. 7, 2014), *available at* http://www.bloomberglaw.com/public/document/Federal_Trade_Commission_v_Wyndham_Worldwide_Corporation_et_al_Do/9 (12 PVLR 1465, 9/2/13).
[18] *Id.* at 14.
[19] *Id.* (citing *FDA v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120 (2000)).
[20] *Wyndham Worldwide*, 2014 BL 94785, at *6 (quoting *Brown & Williamson*, 529 U.S. at 139) (emphasis in original).
[21] *Id.* at *8 (emphasis in original).
[22] *Id.*

what data-security protections a company must employ to comply with Section 5.''[23] The company also argued that the FTC failed to articulate exactly what the vague standards created by use of the terms ''reasonable,'' ''adequate,'' or ''proper'' require.

The FTC disagreed with Wyndham's argument that rulemaking is the only proper way for the FTC to regulate data security. According to the FTC, rulemaking would be inappropriate because data security is highly contextual and always changing. Regarding defining what ''reasonable'' security is, the FTC argued that companies can look to a few things for guidance: ''(1) industry guidance sources that [Wyndham] itself seems to measure its own data-security practices against; and (2) the FTC's business guidance brochure and consent orders from previous FTC enforcement actions.''[24]

The FTC also asserted that data security standards can be enforced in an industry-specific, case-by-case way, analogizing its strategy in regulating data security with the approach of other agencies who bring actions without ''particularized prohibitions,'' such as the National Labor Relations Board (NLRB) and the Occupational Safety and Health Administration (OSHA).[25]

The court agreed with the FTC, noting that ''Circuit Courts of Appeal have affirmed FTC unfairness actions in a variety of contexts *without* preexisting rules or regulations specifically addressing the conduct-at-issue.''[26] Although the court agreed that laws must give fair notice of conduct that is forbidden or required, it was not convinced that regulations are the only means of providing sufficient fair notice. Judge Salas seemed to understand that the rapidly evolving nature of data security made the FTC's analogies to the NLRB and OSHA as models of bringing enforcement actions without issuing particularized prohibitions persuasive.

Perhaps more importantly, the court noted that ''the contour of an unfairness claim in the data-security context, like any other, is necessarily 'flexible' such that the FTC can apply Section 5 'to the facts of particular cases arising out of unprecedented situations.' ''[27] The court validated a reasonableness approach built upon industry standards and shaped by administrative actions. The court quoted *Gen. Elec. Co. v. Gilbert*, which declared that '' 'the rulings, interpretations and opinions of the Administrator under this Act, while not controlling upon the courts by reason of their authority, do constitute a body of experience and informed judgment *to which courts and litigants may properly resort for guidance*.' ''[28]

The court stated that Wyndham's argument regarding the intolerable vagueness of Section 5 unfairness ''ignores that, in addition to various sources of guidance for measuring reasonableness, a statutorily-defined standard exists for asserting an unfairness claim.''[29] The court also noted the illogical and unacceptable practical consequences of a mandate for specific rules before bringing a complaint, stating ''the FTC would have to cease bringing *all* unfairness actions without first proscribing particularized prohibitions—a result that is in direct contradiction with the flexibility necessarily inherent in Section 5 of the FTC Act.''[30]

Our article, ''The FTC and the New Common Law of Privacy'' demonstrates the validity of the court's conclusion that the FTC's interpretations of the FTC Act provide sufficient guidance. For example, at the time we wrote the article, there were over 40 FTC complaints and consent decrees regarding data security, and we reviewed all of them. When reviewed in their totality, far from being vague and arbitrary, we were able to compile a list of specific security practices that the FTC has deemed as inadequate.[31] Moreover, most of these bad practices are ones that clearly run afoul of industry standards or other regulation.

Sufficient Pleading of Unavoidable Consumer Injury

Regarding injury, Wyndham argued that federal statutes and card brand rules eliminate the possibility that consumers can suffer financial injury from the theft of payment card data. Wyndham also rejected the notion that ''incidental injuries that consumers suffered,'' such as the cost of remedial finance monitoring, was insufficient to constitute a ''substantial injury.''[32] Wyndham rejected the FTC's interpretation that consumer injury can include the aggravation, time and effort associated with obtaining reimbursement from card issuers and otherwise responding to a data breach.

The court recognized that the complaint facially alleged financial injury, including unreimbursed fraudulent charges, increased costs and lost access to funds or credit. The FTC also alleged that consumers and businesses expended time and money mitigating subsequent harm from the breaches. The court held that at this stage in litigation, the FTC's allegations of harm were sufficient to defeat a motion to dismiss.

In a remarkable footnote recognizing the dispute over whether nonmonetary injuries are cognizable under Section 5, the court seemed amendable to recognizing nonmonetary harm: ''Although the court is not convinced that non-monetary harm is, as a matter of law, unsustainable under Section 5 of the FTC Act, the Court need not reach this issue given the substantial analysis of the substantial harm element above.''[33]

Deceptiveness

Regarding the FTC's deceptiveness allegation, Wyndham argued that the claim must fail because Wyndham expressly disclaimed any representations about the state of data security at the Wyndham-branded hotels.

---

[23] Motion to Dismiss, *supra* note 17, at 10.

[24] *Wyndham Worldwide*, 2014 BL 94785, at *10.

[25] Plaintiff's Response in Opposition to the Motion to Dismiss by Defendant Wyndham Hotels & Resorts LLC at 29, *FTC v. Wyndham Worldwide Corp.*, No. 2:13-cv-01887-ES-JAD, 2014 BL 94785 (D.N.J. Apr. 7, 2014), *available at* http://www.bloomberglaw.com/public/document/Federal_Trade_Commission_v_Wyndham_Worldwide_Corporation_et_al_Do/1.

[26] *Wyndham Worldwide*, 2014 BL 94785, at *11 (citing *FTC v. Neovi, Inc.*, 604 F.3d 1150, 1153, 1155–59 (9th Cir. 2010); *FTC v. Accusearch Inc.*, 570 F.3d 1187, 1191, 1193–95 (10th Cir. 2009)).

[27] *Id.* at *14 (citing *FTC v. Colgate-Palmolive Co.*, 38 U.S. 374, 384–85 (1965)).

[28] *Id.* (citing *Gen. Elec. Co. v. Gilbert*, 429 U.S. 125, 141–42 (1976)) (emphasis in original).

[29] *Id.*

[30] *Id.* (emphasis in original).

[31] Solove & Hartzog, *supra* note 3, at 651–55.

[32] Motion to Dismiss, *supra* note 17, at 26–27.

[33] *Wyndham Worldwide*, 2014 BL 94785, at *16, n.15.

   ISSN 1538-3423

The court was unpersuaded by Wyndham's arguments, finding that the FTC's allegations were sufficient even under a heightened pleading standard. According to the court, not only did the FTC allege that the defendant directly failed to provide promised data security procedures such as a failure to adequately inventory computers connected to the Wyndham network, but that the supposed disclaimer of liability regarding Wyndham branded hotels is not effective because it is in stark contradiction to other express promises of privacy that include actions taken by Wyndham branded hotels.

For example, the court noted that Wyndham's privacy policy:

> also recognizes ''the important of protecting the privacy of individual-specific (personally identifiable) information collected about guests'' and states that it 'applies to residents of the United States, *hotels of our Brands located in the United States* . . . .' . . . And it also states that '[w]e take commercially reasonable efforts to create and maintain 'fire walls' and other appropriate safeguards to ensure that to the extent we *control* the Information, the Information is used only as authorized by us and consistent with this Policy.'[34]

The court observed that, in short, ''it is reasonable to infer the exact opposite of what [Wyndham] posits: that a reasonable customer would have understood that the policy makes statements about data-security practices at [both Wyndham and Wyndham-branded hotels] to the extent that [Wyndham] *controls* personally identifiable information.''[35]

As a result, the court dismissed Wyndham's arguments.

Implications

The *FTC v. Wyndham* decision is significant for a number of reasons, both large and small. At the doctrinal level, this opinion affirms long-developing patterns such as incremental harms to significant populations and deceptiveness based upon consumer expectations. It also bolsters the FTC's reasonableness approach to data security based upon industry standards and legitimizes the approach so that it can fit comfortably next to other contexts in which the FTC is taking a similar strategy. But there are larger implications to this decision as well, including a solidification of the FTC as the national data security regulator, bolstering the FTC's flexibility in data protection, and, perhaps most directly, the authorization of the FTC setting of baseline standards for data security.

The *Wyndham* case also implicates the future scope of FTC power. The FTC's jurisdiction over privacy has been expanding, and the FTC has been developing its jurisprudence incrementally.

The FTC could push in bolder and more aggressive directions. As we argued in our article, there is a foundation for the FTC to develop an even more robust enforcement of privacy.[36] In other words, there is a lot of room of the FTC to grow, and it has been developing in a very measured and modest way. With the recognition that the FTC is properly within its power to regulate in these areas, the FTC might put its foot on the pedal a little more.

---

[34] *Id.* at *23 (quoting Ex. A to Hradil Decl. at 1) (emphasis in original).

[35] *Id.*

[36] Solove & Hartzog, *supra* note 3, at 583.

NEW PORTFOLIOS & TREATISES NOW AVAILABLE

SAFE DATA & SOUND SOLUTIONS

Privacy & Data Security Law Resource Center™

Unparalleled news. Expert analysis from the new Privacy & Data Security Portfolio Practice Series. Comprehensive new treatises. Proprietary practice tools. State, federal, and international primary sources. The all-in-one research solution that today's professionals trust to navigate and stay in compliance with the maze of evolving privacy and data security laws.

TO START YOUR FREE TRIAL CALL 800.372.1033 OR GO TO www.bna.com/privacy-insights

Bloomberg BNA