AN A.S. PRATT PUBLICATION
NOVEMBER/DECEMBER 2015
VOL. 1 • NO. 3

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Pratt's Privacy & Cybersecurity Law Report

VOLUME 1 NUMBER 3 NOVEMBER/DECEMBER 2015

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at 908-673-3380
Email: ..... Deneil.C.Targowski@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3000
Fax Number .... (518) 487-3584
Customer Service Web site ..... http://www.lexisnexis.com/custserv/
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (518) 487-3000

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [1] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [82] (LexisNexis A.S. Pratt)

An A.S. Pratt™ Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2015–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 718.224.2258. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report,* LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

Federal Trade Commission v. Wyndham Worldwide Corporation: Regulatory Implications for Consumer-Related Data Breaches

By Scott Caplan and Craig A. Newman*

In a closely watched case, the U.S. Court of Appeals for the Third Circuit recently affirmed the Federal Trade Commission's ("FTC") broad enforcement authority in cybersecurity under the unfairness prong of Section 5 of the FTC Act. The authors of this article discuss the decision and the implications for cybersecurity.

The U.S. Court of Appeals for the Third Circuit recently affirmed the Federal Trade Commission's broad enforcement authority in cybersecurity under the unfairness prong of Section 5 of the FTC Act.[1] In the closely watched case, the court held that Wyndham Worldwide Corporation ("Wyndham") was not "entitled to know with ascertainable certainty the cybersecurity standards by which the FTC expected it to conform."[2]

Since 2005, the FTC has been the leading federal agency policing consumer-related data breaches and has instituted more than 50 enforcement actions during that time, almost all of which have resulted in settlements or consent decrees.[3] Wyndham is one of only two companies that have challenged the FTC's authority in this area.

BACKGROUND

By way of background, in June 2012, the FTC sued Wyndham, alleging that its cybersecurity failures constituted both "unfair" and "deceptive" acts and practices within the meaning of the FTC Act, based on three data breaches into Wyndham's reservation systems over a two-year period. The credit card information of more than 600,000 consumers was compromised in those breaches. The FTC's action followed a two-year investigation, during which Wyndham produced more than one million pages of documents.[4] In its lawsuit, the FTC alleged that, as a result of Wyndham's

---

* Scott Caplan is an associate and Craig A. Newman, a member of the Board of Editors of *Pratt's Privacy & Cybersecurity Law Report*, is a partner at Patterson Belknap Webb & Tyler LLP. The authors may be contacted at scaplan@pbwt.com and cnewman@pbwt.com, respectively.

[1] *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 2015 U.S. App. LEXIS 14839 (3d Cir. August 24, 2015).

[2] 2015 U.S. App. LEXIS 14839 at *55.

[3] The FTC's press releases are available at https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/enforcing-privacy-promises. *See also* FTC, *Start with Security: A Guide for Business* (June 2015), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (describing 10 "lessons to learn" from these enforcement actions).

[4] Appellant's Opening Brief at 9, 10, 47, *FTC v. Wyndham Worldwide Corp.*, 2015 U.S. 3d Cir. Briefs LEXIS 308 (3d Cir. Oct. 6, 2014) (No. 14-3514).

lax data security measures, it "unreasonably and unnecessarily exposed consumers' personal data to unauthorized access and theft."[5] Section 5 of the FTC Act – which provides the Commission with its authority over consumer protection – prohibits "unfair or deceptive acts or practices in or affecting commerce."[6] The Act defines "unfair practices" as those that "[1] cause[] or [are] likely to cause substantial injury to consumers [2] which [are] not reasonably avoidable by consumers themselves and [3] not outweighed by countervailing benefits to consumers or to competition."[7]

After transferring the litigation from Arizona to New Jersey federal court, Wyndham moved to dismiss the case for failure to state a claim, arguing that the FTC lacked enforcement authority over data security practices. On April 7, 2014, Judge Esther Salas of the District of New Jersey denied Wyndham's motion.[8] The court granted Wyndham's request for interlocutory appeal on two issues: whether the FTC had authority under the "unfairness" prong of the FTC Act to regulate cybersecurity; and if so, whether Wyndham received fair notice that its practices did not meet the FTC's standard of providing "reasonable" data security protections.

THE THIRD CIRCUIT DECISION

A three-judge panel of the Third Circuit unanimously affirmed Judge Salas's ruling, rejecting Wyndham's arguments that: (i) Congress had not delegated cybersecurity enforcement to the FTC; (ii) the FTC had not adequately alleged a consumer injury; and (iii) the FTC had not provided fair notice of what cybersecurity measures are necessary. Wyndham's is one of the first federal-court challenges to the FTC's cybersecurity authority, and the Third Circuit's ruling is the first federal appellate decision ruling on the merits of such a challenge.[9]

The Third Circuit's ruling is significant in the evolving area of data privacy law for a number of reasons. *First*, it validates the FTC's current role as the top federal regulator in connection with consumer-related data breaches. *Second*, it means that the FTC's pronouncements and consent decrees take on added significance for companies evaluating what data security measures will satisfy a Commission inquiry. *Third*, the ruling will likely serve as an invitation for state regulators to assume similar authority under their states' respective consumer protection acts.

---

[5] *FTC v. Wyndham*, 2015 U.S. App. LEXIS 14839, at *5.

[6] 15 U.S.C. § 45(a).

[7] 15 U.S.C. § 45(n). Although this provision is captioned "Definition of unfair acts or practices," Wyndham argued the district court and FTC erroneously treated this provision as a definition instead of a limitation on the FTC's power. The Third Circuit agreed the "three requirements in § 45(n) may be necessary rather than sufficient . . . but [was] not persuaded that any other requirements proposed by Wyndham pose[d] a serious challenge to the FTC's claim here." *FTC v. Wyndham*, at *54.

[8] Appellant's Opening Brief, *supra* note 4, at 10–14. The district court decision is reported at 10 F. Supp. 3d 602 (D.N.J. 2014).

[9] *FTC v. Wyndham*, 2015 U.S. App. LEXIS 14839.

Wyndham's Alleged Data Security Failings

In its case against Wyndham, the FTC alleged that Wyndham's data security practices, taken together, "unreasonably and unnecessarily exposed consumers' personal data," and among other things, that Wyndham permitted its hotels to "store payment card information in clear readable text," failed to maintain an adequate inventory of all computers connected to its network and failed to conduct security investigations to detect unauthorized access.[10]

The FTC alleged that these failures allowed Russian hackers to gain unauthorized access to Wyndham customers' confidential information on three occasions between April 2008 and January 2010, compromising a total of 619,000 payment card accounts and resulting in $10.6 million in fraud losses. According to the FTC's complaint, the hackers used similar methods for each attack, but Wyndham failed to take appropriate corrective measures after the first two attacks to prevent the third. Wyndham was alerted to the third attack by a credit card issuer.[11]

Wyndham's Challenge to the FTC's Enforcement Authority

Wyndham challenged the FTC's jurisdiction to police data security practices on several grounds. First, Wyndham argued there was nothing "unfair" about Wyndham's conduct. Wyndham was the victim, not the perpetrator, of the hacking, and there was no allegation Wyndham had acted unscrupulously. Moreover, Congress's express and specific delegation of cybersecurity enforcement to the FTC in certain targeted statutes, such as the Fair Credit Reporting Act, made little sense if the FTC already had broad authority to regulate in the same domain.[12] Second, Wyndham argued that, even if the Commission did have authority to police cybersecurity matters, it had not provided fair notice to regulated companies as to what the FTC required of them. The FTC's publications and consent agreements on cybersecurity, Wyndham argued, consisted of little more than vague generalities and platitudes, which were not particularly helpful to regulated entities.[13] Finally, Wyndham argued the FTC's complaint failed to state a claim as a technical matter, because it failed to allege a "substantial injury to consumers" which was not "reasonably avoidable by consumers themselves," as required by Section 5(n) of the FTC Act.[14]

The Third Circuit rejected each of these arguments. Tracing the history of the FTC's unfairness authority, the court held that Congress had defined the Commission's authority broadly and flexibly, intentionally leaving the development of an

[10] *Id.* at *5–*7.
[11] *Id.* at *7–*10.
[12] Appellant's Opening Brief, *supra* note 4, at 18–35.
[13] *Id.* at 35–45.
[14] *Id.* at 45–50.

unfairness standard to the Commission itself.[15] Moreover, the Supreme Court had rejected reading into the statute any requirement that unfair conduct be "unscrupulous" or "unethical."[16] Equally unavailing was Wyndham's argument that subsequent, targeted cybersecurity statutes evidenced Congressional understanding that the FTC Act had not given the Commission cybersecurity authority. The court read these statutes as supplementing, not contradicting, the FTC's already broad jurisdiction.[17]

The court also held that Wyndham had fair notice that its data security practices could give rise to liability. Taking the FTC's allegations as true, the court found that Wyndham was on notice that its alleged lack of cybersecurity protections for consumers could constitute an "unfair" practice within the meaning of Section 5(a) of the FTC Act.[18] The court's conclusion was "reinforce[d]" by the FTC's 2007 guidebook, which "describes a 'checklist[]' of practices that form a 'sound data security plan.' "[19] In a similar vein, while the court agreed with Wyndham's argument that the FTC's previous consent orders were "of little use" in understanding what Section 5(a) requires, they nonetheless "help[] companies with similar practices apprehend the possibility that their cybersecurity could fail as well."[20] The court noted several of the FTC's complaints contained allegations that were similar to those against Wyndham.[21]

Finally, the court rejected Wyndham's argument that the FTC failed to allege an adequate consumer injury, noting the FTC's complaint alleged "unreimbursed fraudulent charges" and that consumers "expended time and money resolving fraudulent

---

[15] *FTC v. Wyndham*, 2015 U.S. App. LEXIS 14839, at *11–*15; *see also FTC v. Sperry & Hutchinson Co.*, 405 U.S. 223, 239–40 (1972) (Congress "explicitly considered, and rejected, the notion that it reduce the ambiguity of the phrase 'unfair methods of competition' . . . by enumerating the particular practices to which it was intended to apply.")

[16] *FTC v. Wyndham*, at *16 (citing *FTC v. Sperry & Hutchinson Co.*, 405 U.S. 223, 224 n.5 (1972)). *Sperry* was decided when the so-called Cigarette Rule, 29 Fed. Reg. 8355 (1964), was still the operative statement of FTC policy. The Cigarette Rule required the FTC to consider factors including whether the conduct in question "is immoral, unethical, oppressive, or unscrupulous." Although the unscrupulousness of conduct was a factor to be considered, it was not a necessary condition of an unfair act or practice. *Sperry*, 405 U.S. at 224 n.5. In adopting its 1980 Unfairness Policy Statement, later codified at 15 U.S.C. § 45(n), the Commission observed that it had never relied on the ethics factor "as an independent basis for a finding of unfairness" and "abandoned the theory of immoral or unscrupulous conduct altogether." *FTC v. Wyndham*, at *13 (quoting *Int'l Harvester Co.*, 104 F.T.C. 949, 1061 n.43, 1076) (internal punctuation and quotation marks omitted).

[17] *FTC v. Wyndham*, at *22–*28 (distinguishing *FDA v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120 (2000)).

[18] *Id.* at *28–*47.

[19] *Id.* at *47 (quoting FTC, *Protecting Personal Information: A Guide for Business* (Nov. 2011), *available at* https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf).

[20] *Id.* at *49 n.22, *52.

[21] *Id.* at *51–*54.

charges and mitigating subsequent harm."[22] Without stating so explicitly, the Third Circuit appears to have accepted these allegations as sufficient to state a claim, at least at the motion to dismiss stage.

IMPLICATIONS FOR CYBERSECURITY

The Third Circuit's *Wyndham* decision answers the threshold question of the FTC's authority to enforce data security standards in consumer-related breaches. Companies should therefore consider carefully the FTC's previous consent orders and publications in formulating their cybersecurity policies, as may be applicable to their specific business and operations. These include the FTC's 2007 guidebook,[23] as well as the FTC's June 2015 publication identifying 10 "lessons to learn" drawn from the FTC's enforcement actions to date.[24]

More than half of the states have enacted so-called "Little FTC Acts" containing broad prohibitions on unfair and deceptive practices similar to the FTC's Section 5. Regulators in these states might now be incentivized to pursue similar enforcement actions when there is a consumer-related data breach. Companies facing such claims should be aware that different states apply different standards to deception and unfairness claims.[25] Even those states that look to FTC and federal court decisional authority to interpret their consumer protection statutes may differ on the applicable standard, depending on when their Little FTC Act was enacted and the applicable federal standard at that time.[26]

---

[22] *Id.* at *10.

[23] FTC, *Protecting Personal Information: A Guide for Business* (Nov. 2011), *available at* https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf.

[24] *Start with Security: A Guide for Business* (June 2015), *supra* note 3.

[25] *See* Jack E. Karn, State Regulation of Deceptive Trade Practices Under "Little FTC Acts": Should Federal Standards Control?, 94 Dick. L. Rev. 373 (1990) (analyzing the standards for unfair and deceptive practices under the Little FTC Acts and comparing them with the federal standards).

[26] *See* David L. Belt, *Should the FTC's Current Criteria for Determining "Unfair Acts or Practices" Be Applied to State "Little FTC Acts"?*, ANTITRUST SOURCE, Feb. 2010, at 7–10, http://www.americanbar.org/content/dam/aba/publishing/antitrust_source/Feb10_Belt2_25f.pdf (noting that a majority of these states still apply some version of the Cigarette Rule).