Journal of Technology Law & Policy

Volume XIV – Spring 2014

ISSN 2164-800X (online)

DOI 10.5195/tlp.2014.149

http://tlp.law.pitt.edu

An Era of Rapid Change: The Abdication of Cash & the FTC's Unfairness Authority

Elie Freedman

An Era of Rapid Change: The Abdication of Cash & the FTC's Unfairness Authority

Elie Freedman*

INTRODUCTION

On June 26, 2012, the Federal Trade Commission ("FTC") filed a complaint against Wyndham Worldwide Corporation ("Wyndham"), a holding company for a group of hotels, claiming that on three separate occasions between 2008 and 2010, Wyndham's failure to maintain reasonable network security measures had resulted in third-party security breaches.[1] The FTC alleged that Wyndham's security failures resulted in $10.6 million in fraud loss, and the theft of more than 200,000 Wyndham customers' personally identifiable account and credit card information.[2] While it has yet to go to trial, *FTC v. Wyndham*[3] is perhaps "the most important case in privacy and data security law,"[4] because it promises to shape the FTC's authority to regulate third-party data breaches through the Federal Trade Commission Act, codified in 15 U.S.C. § 45 (hereinafter referred to interchangeably as either the "FTCA" or "Act"), and consequently, information security and consumer privacy.[5]

* J.D. Candidate, University of Pittsburgh School of Law, 2015; B.A., History, McGill University, 2008. I would like to thank my parents, Marilyn and Norman, and my brother, Shane, for their unwavering love and support. I also thank Professor James Flannery for his invaluable guidance, mentorship, and encouragement. Last, but not least, thank you to all of the editors from the *University of Pittsburgh Journal of Technology, Law & Policy* for your contributions to this article. I could not have done it without you. For comments or to request sources, I may be reached at Elie.Freedman@gmail.com.

[1] First Amended Complaint for Injunctive and Other Equitable Relief at 2, FTC v. Wyndham Worldwide Corp., No. CV 12-1365-PHX-PGR, 2012 WL 3281910 (D. Ariz. Aug. 9, 2012) [hereinafter Wyndham First Amended Complaint].

[2] *Id.*

[3] FTC v. Wyndham Worldwide Corp., No. CV 12-1365-PHX-PGR, 2013 WL 1222491 (D. Ariz. Mar. 25, 2013) (transferring the case to the district court for the District of New Jersey).

[4] Katie W. Johnson, *Impending Wyndham Ruling Leaves Some Questioning FTC's Enforcement Power*, BLOOMBERG BNA PRIVACY & SEC. LAW REPORT (Sept. 2, 2013, 12:00 AM), http://www.bloomberglaw.com/document/X97AK2UO000000.

[5] 15 U.S.C. § 45(a)(1) (2012); *see* Peter S. Frechette, FTC v. LabMD*: FTC Jurisdiction over Information Privacy Is "Plausible," but How Far Can It Go*?, 62 AM. U. L. REV. 1414–15 (2013).

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.149 ● http://tlp.law.pitt.edu

The FTC has been extremely active in regulating third-party data breaches, but its success in data-security enforcement, thus far, is due exclusively to organizational compliance with FTC consent orders.[6] *Wyndham*'s importance comes from the fact that because it is likely to go to trial, *Wyndham* will likely produce the first judicial opinion on FTC regulation in the data-security breach realm.[7] While the FTC has normally required that a private company must provide "reasonable and appropriate security for . . . personal information collected and maintained,"[8] the *Wyndham* case may significantly broaden, or restrict, the scope of this standard. *Wyndham*'s legal conclusions are poised to send shockwaves through the business world, as to whether the FTC may regulate what measures are "reasonable and appropriate."[9] In *Wyndham*'s wake are the concerns of the average consumer: after a business has electronically collected and stored personal consumer information, how far must it go to protect it? This question begs an answer that the United States District Court for the District of New Jersey is bound to address.

Wyndham's potential impact on the business world and consumers is eminently apparent; the result may also affect the practice of law by necessitating new advisement strategies for lawyers working both in-house and as outside counsel for technology companies focused on utilizing personally identifiable consumer information.[10] Advances in computer technology and information storing practices, across industries, have resulted in a significant increase in data security breaches.[11] Data security breaches categorically refer to "an organization's unauthorized or unintentional exposure, disclosure, or loss of sensitive personal information," including personally identifiable information such as Social Security numbers, or financial information such as credit cards and bank account numbers.[12]

---

[6] *See infra* Part II.C.

[7] *See* Johnson, *supra* note 4.

[8] First Amended Complaint for Injunctive and Other Equitable Relief ¶ 24, FTC v. Wyndham Worldwide Corp., No. CV 12-1365-PHX-PGR, 2012 WL 3281910 (D. Ariz. Aug. 9, 2012).

[9] *See* Johnson, *supra* note 4.

[10] *See* David McAuley, *FTC in Cyberspace: Ready, or Not, for Coming Wave of Connected Devices*, BLOOMBERG BNA (Nov. 20, 2013, 12:00 AM), http://www.bna.com/ftc-cyberspace-ready-n17179880248/.

[11] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-14-487T, INFORMATION SECURITY: FEDERAL AGENCIES NEED TO ENHANCE RESPONSES TO DATA BREACHES 1 (2014), *available at* http://www.gao.gov/products/GAO-14-487T?source=ra.

[12] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-07-737, DATA BREACHES ARE FREQUENT, BUT EVIDENCE OF RESULTING IDENTITY THEFT IS LIMITED; HOWEVER, THE FULL EXTENT IS UNKNOWN 1 (2007).

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.149 ● http://tlp.law.pitt.edu

The theft of personally identifiable information and credit card or bank account numbers is more than likely to cause consumer injury, and preventing such injury is a natural objective of the FTC. The abdication of "cash as king" has resulted from the increased use of electronic payment methods by consumers in commercial transactions. Electronic payment methods require the use of personally identifiable consumer information to verify and accept payments. Concomitantly, the technology industry has rapidly developed new and enticing uses for consumer information in business strategies.[13] Consequently, cognizance about the applicability of these developments to clients, and their businesses implies that the legal community should anticipate and recognize its role to provide responsible and sound advice for implementing these strategies reasonably and appropriately.

Nowhere is this development more pertinent than in the city of Pittsburgh, which is home to over 1600 technology companies[14] and the incubator for close to fifty new technology businesses per year.[15] For lawyers in Pittsburgh, especially those working with new and developing companies, data security law promises significant added value for clients. More importantly, this practice area requires attention because of its possible impact on both newly retained and long-standing in-house legal counsel's obligations and due diligence practices.[16] Furthermore, reasonable and appropriate security measures may also become important considerations for lawyers assisting with start-up entity formation and capital investment attraction. FTC suits may result in significant civil liabilities (and consequent monetary penalties), and therefore investors may be deterred from capital contributions to companies without reasonable security measures in place. In light of recent security breaches exposing consumer information at Target, Neiman Marcus, and Kickstarter,[17] to name only a few, Wyndham demands the attention of practitioners. As data security law develops, legal counsel will be

[13] *See, e.g.*, Jason Morris & Ed Lavandera, *Why Big Companies Buy, Sell Your Data*, CNN TECH (Aug. 23, 2012, 3:42 PM), http://www.cnn.com/2012/08/23/tech/web/big-data-acxiom/.

[14] Dan Bobkof, *From Steel To Tech, Pittsburgh Transforms Itself*, NPR (Dec. 16, 2010, 6:57 PM), http://www.npr.org/2010/12/16/131907405/from-steel-to-tech-pittsburgh-transforms-itself.

[15] *Company Creation*, CARNEGIE MELLON UNIV., https://www.cmu.edu/cttec/Spin-Outs/index.html (last visited Mar. 12, 2014).

[16] *Id.* at 51.

[17] Paula Rosenblum, *In Wake of Target Breach, Cash Becoming King Again*, FORBES (Mar. 17, 2014, 5:11 PM), http://www.forbes.com/sites/paularosenblum/2014/03/17/in-wake-of-target-data-breach-cash-becoming-king-again/.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.149 ● http://tlp.law.pitt.edu

required to advise and guide their clients to setup and maintain reasonable and appropriate data security measures for both existing and new ventures.[18]

General consumer ignorance and widespread industry confusion regarding the FTC's unfairness authority belies the import of the *Wyndham* decision. The impact of the FTC's enforcement of the FTCA in the data-security realm, when coupled with a dramatic rise in the severity and frequency of data-breaching attacks against U.S. businesses compels a cogent and fresh examination of the FTC's unfairness authority. This Article has several aims: (1) to provide legal professionals, students, and business operators an understanding of the history of the FTC's unfairness authority; (2) to examine important examples of the FTC's enforcement of the unfairness authority through consent orders, in order to provide the factors, and data security measures that the FTC considers reasonable and appropriate for collecting personally identifiable consumer information; (3) to examine the arguments challenging the FTC's unfairness authority posited in *Wyndham*, and evaluate their strengths; and, (4) most fundamentally, to dispel inapposite and rudimentary characterizations of the FTC's unfairness authority enforcement as irrational, inconsistent or illegitimate. Part I of this Article reviews the FTCA's statutory framework. Part II investigates the current case law and administrative actions that have shaped the FTC's unfairness authority. Part III thoroughly discusses and analyzes the *Wyndham* case, each of the party's arguments in their respective pretrial motions, and the court's recent opinion denying Wyndham's motion to dismiss.

I. THE FTCA STATUTORY FRAMEWORK

The FTCA provides the jurisdictional basis for FTC action over "unlawful" practices.[19] The FTCA explicitly states that the FTC, "is hereby empowered and directed to prevent persons, partnerships, or corporations . . . from using unfair methods of competition in or affecting commerce and *unfair or deceptive* acts or practices in or affecting commerce."[20] In defining an unfair or deceptive labor practice the FTCA further provides that:

> The Commission shall have no authority under this section . . . to declare unlawful an act or practice on the

[18] Michelle Sherman, *Advising Clients on Internet Privacy Policies*, 29 GPSOLO, no. 6, 2012 at 48, 49, *available at* http://www.americanbar.org/publications/gp_solo/2012/november_december2012privacyandconfidentiality/advising_clients_internet_privacy_policies.html.

[19] 15 U.S.C. § 45(a)(2) (2012).

[20] *Id.* (emphasis added).

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.149 ● http://tlp.law.pitt.edu

> grounds that such act or practice is unfair unless the act or practice causes or is likely to cause [1] substantial injury to consumers which is [2] not reasonably avoidable by consumers themselves and [3] not outweighed by countervailing benefits to consumers or to competition. In determining whether an act or practice is unfair, the Commission may consider established public policies as evidence to be considered with all other evidence. Such public policy considerations may not serve as a primary basis for such determination.[21]

Thus, the statutory structure provides two separate bases by which the FTC can claim authority: the FTC may regulate unlawful conduct, categorically, as a deceptive *or* unfair practice.[22] At issue in *Wyndham* is whether the FTC has the jurisdiction to regulate data security breaches via the unfairness basis.[23] In addition to the enforcement jurisdiction contained in § 45, § 57(a)(1)(A) of the Act provides that the FTC may prescribe "interpretive rules and general statements of policy with respect to unfair or deceptive acts or practices in or affecting commerce within the meaning of section 45(a)(1) of [title 15]," subject to the Notice of Proposed Rulemaking procedures under the Administrative Procedure Act.[24] Following this grant of authority, the FTC gives substance to the statutory framework.

---

[21] *Id.* § 45(n).

[22] *Id.* § 45(a)(2).

[23] *Id.* § 45(a)(2); *see also* FTC v. Wyndham Worldwide Corp., No. CV 12-1365-PHX-PGR, 2013 WL 1222491 (D. Ariz. Mar. 25, 2013).

[24] 15 U.S.C. § 57(a)(1)(b), also describes the unfair or deceptive acts or practices rulemaking proceedings offering:

> When prescribing a rule under subsection (a)(1)(B) of this section, the Commission shall proceed in accordance with section 553 of Title 5 (without regard to any reference in such section to sections 556 and 557 of such title), and shall also (A) publish a notice of proposed rulemaking stating with particularity the text of the rule, including any alternatives, which the Commission proposes to promulgate, and the reason for the proposed rule; (B) allow interested persons to submit written data, views, and arguments, and make all such submissions publicly available; (C) provide an opportunity for an informal hearing in accordance with subsection (c) of this section; and (D) promulgate, if appropriate, a final rule based on the matter in the rulemaking record (as defined in subsection (e)(1)(B) of this section), together with a statement of basis and purpose.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.149 ● http://tlp.law.pitt.edu

II. MOLDING THE LIMITS OF "UNFAIR" AND THE FTC'S AUTHORITY

The first substantial test of the FTC's authority to prohibit unfair business practices occurred in 1972, when the Supreme Court of the United States decided *FTC v. Sperry & Hutchinson Co.*, holding that consumers and competitors alike should be protected from unfair practices.[25]

In 1968 the FTC issued a cease and desist order to the Sperry & Hutchinson Company ("S&H"), alleging a violation of § 45(a)(1).[26] Specifically, the FTC claimed that S&H was engaged in unfair practices by improperly regulating trading stamp rates; attempting to suppress other trading stamp exchanges; and colluding with other companies to regulate the rate of stamp dispensation.[27] S&H argued that § 45(a)(1) permitted the FTC to "restrain only such practices as are either in violation of the antitrust laws, deceptive, or repugnant to public morals," and that since S&H engaged in no such activity, the FTC lacked authority in the matter.[28] In promulgating its opinion, the Court considered whether

> [15 U.S.C. § 145(a)(1)] empower[s] the Commission to define and proscribe an unfair competitive practice, even though the practice does not infringe either the letter or the spirit of the antitrust laws? Second, does [15 U.S.C. § 45(a)(1)] . . . empower the Commission to proscribe practices as unfair or deceptive in their effect upon consumers regardless of their nature or quality as competitive practices or their effect on competition?[29]

The Supreme Court held that the statute empowered the FTC to define and proscribe an unfair competitive practice, even if the practice did not infringe on antitrust law, and that the Commission was empowered to proscribe practices as unfair or deceptive in their effect on consumers, regardless of their nature or effect on competition.[30] The Supreme Court reasoned that because Congress explicitly refused to define unfair practices by tying their definitions to statute or common

[25] FTC v. Sperry & Hutchinson Co., 405 U.S. 233, 239 (1972).

[26] *See id.* at 234.

[27] *Id.*

[28] *Id.* at 235.

[29] *Id.* at 239.

[30] *Id.*

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.149 ● http://tlp.law.pitt.edu

law, the determination of what was an unfair practice was the proper domain of the FTC.[31]

A. The Unfairness Statement of 1980

Sperry & Hutchinson gave the FTC tremendous power and flexibility to define unfair practices.[32] In 1980, the FTC issued a letter, now known as the "Unfairness Statement," to the Congressional Subcommittee of the U.S. Senate Committee on Commerce, Science and Transportation, which addressed the palpable limits of the FTC's unfairness authority.[33] In its letter, the FTC identified three standards to be considered in identifying an unfair practice: (1) consumer injury; (2) violation of public policy; and (3) unethical or unscrupulous conduct.[34] The Unfairness Statement factors were codified in an amendment to § 45(n).

1. Consumer Injury

Fundamentally, the FTC recognized that, consistent with the FTCA, consumer injury, alone, is sufficient to find a practice unfair.[35] A consumer injury sufficient for a finding of an unfair practice must be one that is (1) substantial; (2) not outweighed by any offsetting consumer or competitive benefit; and (3) results in an injury not reasonably avoided by the customer.[36] Substantial consumer injury typically results in monetary harm or produces unwarranted health or safety risks.[37] The second factor, weighing the injury against consumer benefits, requires a balancing test wherein the FTC "will not find that a practice unfairly injures consumers unless it is injurious *in its net effects*."[38] Third, injuries not reasonably avoided by the consumer are defined as those involving "seller behavior that

---

[31] FTC v. Sperry & Hutchinson Co., 405 U.S. 233 at 240.

[32] *Id.* at 244 n.5 (1972) (The Supreme Court identified the FTC's determinative factors for unfairness as (1) whether the practice offends public policy (as established by the common law or statutes) (2) "whether it is immoral, unethical, oppressive, or unscrupulous; [and] (3) whether it causes substantial injury to consumers (or competitors or other businessmen).").

[33] Andrew Serwinal, *The Federal Trade Commission and Privacy: Defining Enforcement and Encouraging the Adoption of Best Practices*, 48 SAN DIEGO L. REV. 809, 828–29 (2011).

[34] The Unfairness Statement was later appended to an FTC decision, *In re* Int'l Harvester Co., 104 FTC 949, 1072 (1984), and will be cited thereto, hereafter. Unethical or unscrupulous conduct had never served as an independent basis for the exercise of the FTC's unfairness authority and, as such, the FTC concluded that it would proceed in the future on basis of the first two categories only. *See* 104 FTC 949, 1076 (1984).

[35] *In re* Int'l Harvester Co., 104 FTC 949, 1073 (1984).

[36] *Id.*

[37] *Id.*

[38] *Id.* (emphasis added).

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.149 ● http://tlp.law.pitt.edu

unreasonably creates or takes advantage of an obstacle to the free exercise of consumer decision[-]making."[39]

2. Violation of Public Policy

The FTC recognized that public policy considerations could be used in two distinct ways.[40] Public policy may be employed by the FTC to "test the validity and strength of the evidence of consumer injury, or, less often, it may be cited for a dispositive legislative or judicial determination that such injury is present."[41] Given the relative importance of public policy in FTC unfairness determinations, the FTC proposed a two pronged test, both necessary to establish a violation of public policy.[42] First, the public policy should be clearly established by and embodied, or declared in judicial decisions, statutes, or the Constitution, as interpreted by the courts.[43] Second, the public policy should be widely shared, and not isolated to a single state or court.[44] If both prongs are met, and convincing independent evidence of the violation is established, the FTC may conclude that the practice is "distorting the operation of the market and thereby causing unjustified consumer injury."[45] Ultimately, the FTCA provides that "[i]n determining whether an act or practice is unfair, the Commission may consider established public policies as evidence to be considered with all other evidence. Such public policy considerations may not serve as a primary basis for such determination."[46]

B. "Unfair Act or Practice" Consent Order Resolutions

Starting in 1999, the FTC sought to cede online consumer protection to industry self-regulation but reversed course within a year. The self-regulation experiment proved to be as unsuccessful as it was short-lived. By 2000, the then new FTC Chairman, Timothy Muris, announced a new policy that the Agency would no longer rely solely on self-regulation, but instead would expand

---

[39] *Id.*

[40] *In re* Int'l Harvester Co., 104 FTC 949, 1074 (1984).

[41] *Id.*

[42] *Id.*

[43] *Id.* at 1076.

[44] *Id.*

[45] *Id.* at 1049.

[46] 15 U.S.C. § 45(n) (2012). For the purposes of brevity, this Article will not examine the public policies courts have considered under the FTCA.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.149 ● http://tlp.law.pitt.edu

enforcement of existing laws rather than pursue new legislation.[47] As part of the expanded enforcement initiative, the FTC began applying the "unfairness" principle to organizational data security breaches.[48] Owing to the ubiquitous use of massive data-gathering practices across a wide spectrum of American businesses and the nearly equally ubiquitous occurrences of data-security breaches, this expanded enforcement initiative had a broad regulatory impact.

In furtherance of this expanded initiative, in May 2000, the FTC issued the *Final Report on Online Access and Security* in which the Agency indicated that 1) security measures are a process and that no single standard can assure adequate security because of the evolution of security threats; 2) each website should have a security program that adequately protects all collected consumer information and is appropriate to the circumstances; and 3) appropriateness would be defined on a case-by-case basis, taking into consideration the risks faced by the domain, the costs of protection, and the type of information the site maintains.[49] While this expanded enforcement policy was not without detractors, armed with the Final Report, and a new and expansive implementation program, the FTC delved into the data-security breach realm, heralding a new era of consumer protection and organizational accountability.

1. In re BJ's Wholesale Club

In re BJ's Wholesale Club, Inc. was the first time that the FTC employed its unfairness authority exclusively for an allegation of privacy and data security misrepresentation.[50] BJ's Wholesale Club, Inc. ("BJ's") operated 150 stores in the United States, and maintained a membership model, allowing, generally, only BJ's members to make purchases.[51] BJ's had eight million members and accepted credit card payments from consumers as part of its regular course of business.[52] In order to authorize the credit card purchases, BJ's would collect personally identifiable information from its customer's credit cards, and transmit that information over its wireless in-store computer network to the card issuer's bank, through BJ's central

---

[47] Michael D. Scott, *The FTC, the Unfairness Doctrine, and Data Security Breach Litigation: Has the Commission Gone Too Far?*, 60 ADMIN. L. REV. 127, 131 (2008).

[48] FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE: A FEDERAL TRADE COMMISSION REPORT TO CONGRESS 42 n.21 (2000).

[49] *See generally* FED. TRADE COMM'N ADVISORY COMM., FINAL REPORT ON ONLINE ACCESS AND SECURITY 19–25 (2000).

[50] Until this point the FTC had coupled the unfairness authority with deceptive practices to enforce § 45 of the FTCA. *See* Serwinal, *supra* note 33, at 840.

[51] Complaint at 466, *In re* BJ's Wholesale Club, Inc., 140 FTC 465 (2005).

[52] *Id.*

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.149 ● http://tlp.law.pitt.edu

datacenter.[53] BJ's also received responses, from the banks, through the same transmission route.[54]

In late 2003 banking institutions started noticing that customers who used their cards at BJ's were subsequently victimized by fraudulent credit card charges.[55] Consumer credit card and banking information, collected by BJ's and stored on BJ's network, were being copied by an unauthorized third party to make fraudulent purchases worth millions of dollars.[56] As a result of the fraud, banks and customers were forced to cancel and reissue thousands of credit and debit cards.[57]

On September 20, 2005, the FTC filed a complaint against BJ's alleging that its failure to "employ reasonable and appropriate security measures to protect personal information and files caused or is likely to cause substantial injury to consumers that is not offset by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers. This practice was an unfair act or practice."[58]

The FTC provided patently clear, but often ignored, reasoning in establishing that BJ's conduct was an unfair consumer practice.[59] The FTC alleged that a *combination* of practices, taken together, constituted unreasonable security for sensitive personal information:

> (1) failing to encrypt information collected in its stores while the information was in transit or stored on BJ's computer networks; (2) storing the information in files that could be accessed anonymously, that is, using a commonly known default user id and password; (3) failing to use readily available security measures to limit access to its networks through wireless access points on the networks; (4) failing to employ measures sufficient to detect unauthorized access to the networks

[53] *Id.*

[54] *Id.*

[55] *Id.* at 467.

[56] Complaint at 466, *In re* BJ's Wholesale Club, Inc., 140 FTC 465 (2005).

[57] *Id.* at 466.

[58] *Id.* at 468.

[59] The FTC reasoning in this instance is not only patently clear, but also provides the basis upon which nearly every subsequent data-security enforcement action is based. Shamefully, academics and organizations, alike, either ignore or fail to realize that a combination of individual missteps in data security, taken as a whole, is unreasonable and can lead to FTCA culpability.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.149 ● http://tlp.law.pitt.edu

> or conduct security investigations; and (5) storing information for up to 30 days when BJ's no longer had a business need to keep the information, in violation of bank security rules.[60]

Here, BJ's failed its consumers on a plethora of easily reconciled issues; it does not seem clear that any one violation would have supported the FTC's complaint, but the combination of failures measured up to conduct causing substantial, unavoidable consumer injury. If BJ's had remedied any one of the five specific allegations leveled by the FTC it should have left BJ's more than able to prevent or curtail some of the resulting consumer injury. Furthermore, there is both rhyme and reason to the FTC's rationale. BJ's collected consumer information which it failed to mask or encrypt, and failed to protect stored information by allowing access to the information with generic username and password combinations. BJ's stored the poorly protected information for too long, and provided no notification system to alert it of possible unauthorized access.[61]

Perhaps in recognition of these tremendous oversights, BJ's capitulated to the FTC's claims and signed a consent order to implement appropriate and comprehensive information security measures, to obtain a biannual network security assessment, and to file reports with the FTC until 2025.[62] The FTC subsequently submitted the consent order to Public Notice and Comment, and then approved it.[63]

2. FTC v. LabMD, Inc.

In 2008, the FTC issued a resolution ("the 2008 Resolution") defining agency procedures to investigate consumer privacy violations.[64] The 2008 Resolution established FTC investigatory authority

> [t]o determine whether unnamed persons, partnerships, corporations, or others are engaged in, or may have

---

[60] *In re* BJ's Wholesale Club, Inc., 140 FTC 465, 476 (2005).

[61] *Id.*

[62] *Id.* at 476–77.

[63] *See Announced Actions for September 23, 2005*, FED. TRADE COMM'N (Sept. 23, 2005), http://www.ftc.gov/news-events/press-releases/2005/09/announced-actions-september-23-2005.

[64] Federal Trade Commission, Resolution Directing Use of Compulsory Process in Nonpublic Investigation of Acts and Practices Related to Consumer Privacy and/or Data Security, File No. P954807 (Jan. 3, 2008).

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.149 ● http://tlp.law.pitt.edu

> engaged in, deceptive or unfair acts or practices related to consumer privacy and/or data security, including but not limited to the collection, acquisition, use, disclosure, security, storage, retention, or disposition of consumer information, in or affecting commerce, in violation of Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, as amended. Such investigation shall, in addition, determine whether Commission action to obtain redress of injury to consumers or others would be in the public interest.[65]

In 2009, utilizing authority granted by the 2008 Resolution, the FTC began investigating LabMD, Inc. ("LabMD") and other entities, upon discovering that personally identifiable and sensitive health information belonging to consumers, collected by these organizations, was publicly available on peer-to-peer file sharing networks.[66] Unlike BJ's however, wherein FTC complaints resulted in speedy consent orders, LabMD exercised resistance to the FTC's investigation. LabMD's resistance was significant because it was the first substantial contest mounted against the FTC's enforcement of the unfairness authority over third-party data-security breaches, laying the foundations for the respondent's claims in *Wyndham*.

In the *LabMD* case, the FTC undertook "an inquiry to determine whether disclosures of consumers' sensitive personal information [were] attributable to failures to employ reasonable data security measures[,] in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), or whether they violated any other statutes or regulations enforced by the Commission."[67] The FTC issued Civil Investigative Demands ("CIDs"), to various companies, pursuant to the 2008 Resolution, in order to obtain copies of the electronic files containing sensitive consumer information.[68] In response, the FTC obtained a spreadsheet containing, among many other things, information about 9,000 LabMD customers, including names, social security numbers, health insurance information, and dates of birth.[69] After consulting with law enforcement agencies, the FTC issued a voluntary access request to LabMD to help determine whether LabMD had violated the FTCA in

---

[65] *Id.*

[66] FTC v. LabMD, Inc., No. 1:12-cv-3005-WSD, slip op. at 4 (N.D. Ga. Nov. 26, 2012).

[67] *See id.* at 2.

[68] *Id.*

[69] It is unclear, based on the opinion, whether this spreadsheet was received by the FTC from LabMD, or another entity. What is clear, however, is that this document was provided by a third-party subject to the FTC's 2009 CIDs to various organizations.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.149 ● http://tlp.law.pitt.edu

failing to use reasonable and appropriate security measures to safeguard consumer information.[70] LabMD responded to the access request, but the FTC found the response unsatisfactory.[71]

On December 21, 2011, the FTC issued additional CIDs to LabMD, demanding that, by January 13, 2012, the company consent to the following stipulations: LabMD representatives appear at investigational hearings with FTC staff; LabMD respond to a limited set of interrogatories; LabMD provide documents related to its data security practices not already disclosed by the voluntary access request; and LabMD certify compliance with the CIDs.[72]

LabMD sought to limit and remove the CIDs through the administrative process, but the FTC denied LabMD's administrative petitions.[73] On June 25, 2012, the FTC contacted LabMD to implement compliance with the CIDs, but LabMD, again, responded with objections.[74] In August 2012, after LabMD's continued failure to comply with the CIDs, the FTC filed a petition in court seeking an order requiring LabMD's compliance, pursuant to the FTC's authority under 15 U.S.C. §§ 46, 57b-1 of the FTCA and the 2008 Resolution.[75] The FTC alleged that LabMD's failure to comply with the CIDs hindered the FTC's investigation into possible data-security breaches at LabMD.[76]

In September 2012, the court ordered that the FTC serve LabMD with its petition and that LabMD show cause at a hearing explaining why the CIDs should not be implemented.[77] The court also directed LabMD to file a pleading stating its legal and factual support for failing to comply with the FTC's CIDs.[78] The court further ordered the FTC to file a supplemental pleading to answer several questions, including "[W]hat is the FTC required to show to meet the requirement that the subpoena is issued in an inquiry that is within the authority of the agency?"

---

[70] *LabMD, Inc.*, No. 1:12-cv-3005-WSD at 3.

[71] The opinion provides that "LabMD responded to the voluntary access request, but the FTC was dissatisfied with the scope of materials and information that were provided." *Id.* Presumably the dissatisfaction stemmed from the breadth of LabMD's disclosures, though subsequent CIDs may indicate what the FTC felt LabMD was holding back.

[72] *Id.*

[73] *Id.* at 4.

[74] *Id.*

[75] *Id.*

[76] *LabMD, Inc.*, No. 1:12-cv-3005-WSD at 3.

[77] *Id.* at 4–5.

[78] *Id.*

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.149 ● http://tlp.law.pitt.edu

and "[h]ow does the FTC meet the [']within the authority of the agency standard[']in this case?"[79] LabMD put forward several arguments to invalidate the FTC's CIDs, chief among them that the FTC's claim of authority to regulate data security "is not based on any threat of substantial injury to consumers, but only generalities."[80]

In addressing these arguments, the court noted that in assessing the validity of the FTC's CIDs, it was restricted to consider: "(1) Whether the agency makes a plausible argument in support of its assertion of jurisdiction, and (2) Whether the information sought by the CID is plainly incompetent or irrelevant to any lawful purpose of the FTC."[81] The court held that the CIDs were enforceable because there was a plausible argument for the FTC's statutory authority and jurisdiction over data security and consumer privacy, and that the information sought in the CIDs was reasonably relevant to its investigation of LabMD's data-security practices.[82] The court reasoned that the

> FTC presents a plausible argument for the exercise of its jurisdiction to investigate and enforce in the realm of data security and consumer privacy—which it has done so [sic] in at least forty-four instances since 2000—in light of the threat of substantial consumer harm that occurs when consumers are victims of identity theft.[83]

The court further reasoned that the FTC's argument that poor data security and consumer privacy both facilitate and contribute to "predictable and substantial harm to consumers in violation of Section [45]" was plausible, and therefore "material and relevant to a lawful purpose of the agency."[84] Finally, the court

---

[79] *Id.* at 5.

[80] *Id.* at 11.

[81] *Id.* at 7 (internal quotations and citations omitted) (providing that "it is well-settled that the role of a district court in a proceeding to enforce an administrative subpoena is sharply limited; inquiry is appropriate only into whether the evidence sought is material and relevant to a lawful purpose of the agency.").

[82] *LabMD, Inc.*, No. 1:12-cv-3005-WSD at 13–14.

[83] *Id.* at 13.

[84] *Id.* at 17.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.149 ● http://tlp.law.pitt.edu

ordered LabMD to comply with the FTC's CIDs, and granted the FTC's Petition.[85] The FTC's investigation is still on going.[86]

Interestingly, *LabMD* appears, on the surface, both to affirm the FTC's authority to regulate data security and consumer privacy practices, and to confer legitimacy to the FTC's investigatory pursuits. However, due to the limited scope of LabMD's challenge to the FTC, via the legitimacy of the CIDs, *LabMD* does not convey much in the way of judicial guidance for the *Wyndham* case. *LabMD* is the first of only two organizations (the other being Wyndham) to raise a significant challenge to the FTC's authority over data security practices.

C. The FTC's Final Privacy Report of 2012

In March 2012, the FTC issued its final privacy report, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* ("Final Report").[87] The Final Report urged businesses to adopt data security measures based on three principles. First, the report suggests privacy by design, meaning "Companies should incorporate substantive privacy protections into their practices, such as data security, reasonable collection limits, sound retention and disposal practices, and data accuracy," and should maintain comprehensive measures to assess privacy protections throughout the data collection lifecycle.[88] The Final Report expounded on reasonable data collection limits, providing:

> Companies should limit data collection to that which is consistent with the context of a particular transaction or the consumer's relationship with the business, or as required or specifically authorized by law. For any data collection that is inconsistent with these contexts, companies should make appropriate disclosures to consumers at a relevant time and in a prominent manner—outside of a privacy policy or other legal document. This clarification of the collection limitation principle is intended to help companies assess whether

[85] *Id.*

[86] *LabMD, Inc., In the Matter of*, FED. TRADE COMM'N (Mar. 4, 2005), http://www.ftc.gov/enforcement/cases-proceedings/102-3099/labmd-inc-matter.

[87] FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS at iii (2000) [hereinafter FINAL PRIVACY REPORT].

[88] *Id.* at 23.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.149 ● http://tlp.law.pitt.edu

> their data collection is consistent with what a consumer might expect; if it is not, they should provide prominent notice and choice.[89]

Second, the Final Report suggests that companies should simplify consumer choice, by stating that:

> For practices requiring choice, companies should offer the choice at a time and in a context in which the consumer is making a decision about his or her data. Companies should obtain affirmative express consent before (1) using consumer data in a materially different manner than claimed when the data was collected; or (2) collecting sensitive data for certain purposes.[90]

Thirdly, the Final Report urges transparency in privacy and data security practices.[91] In addition to this guidance, the FTC also called for basic data security legislation, and offered to work with Congress and private organizations to develop appropriate statutory provisions.[92]

Most importantly, the FTC asserted that it is "well settled that companies must provide reasonable security for consumer data. The Commission has a long history of enforcing data security obligations under [§ 45] of the FTC Act."[93] The FTC's assertion not only affirms its fundamental belief in its statutory authority to investigate and prohibit unreasonable consumer data practices, but also to continue to do so under § 45. The latter notion underscores the importance of the *Wyndham* case. Currently, the causes of data security and consumer privacy protection have only one voice in the federal government, the FTC. The *Wyndham* court possesses, at least preliminarily, the power to either silence that voice, or enhance the FTC's guardianship.

---

[89] *Id.* at 27.

[90] *Id.* at 60.

[91] *Id.* at 60.

[92] *Id.* at viii.

[93] FINAL PRIVACY REPORT, *supra* note 87, at viii.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.149 ● http://tlp.law.pitt.edu

III. *FTC v. WYNDHAM*

Wyndham teeters on the precipice of the FTC's authority to enforce reasonable data-security measures because to date no court decision has either upheld or rejected the premise that the FTC may regulate third-party data-security practices under § 45. In *Wyndham*, the arguments for and against the FTC's authority to regulate data-security breaches are powerful, and the outcome will have overwhelming significance for the FTC, commercial entities, and consumers alike.

A. The FTC's Allegations

On June 26, 2012, the FTC brought a two-count complaint against Wyndham Hotels and Resorts, Wyndham Worldwide Corporation, Wyndham Hotel Group, and Wyndham Hotel Management (collectively, "Wyndham"), and subsequently amended its complaint on August 8, 2012.[94] The FTC alleges that Wyndham's failure to employ reasonable data-security practices resulted in two violations of § 45. First, the FTC asserts that Wyndham engaged in deceptive business practices by misrepresenting the security measures it undertook to protect consumers' personal information.[95] Second, the FTC asserts that "Wyndham engaged in unfair business practices because its failure to use reasonable methods to safeguard consumers' personal information caused or is likely to cause substantial injury that could not be avoided by consumers and was not outweighed by countervailing benefits."[96] In support of the two counts, the FTC alleges that Wyndham "violated the FTCA in connection with their failure to employ reasonable data security practices, which resulted in three data security breaches in less than two years, the known theft of hundreds of thousands of consumers' payment card account numbers, and millions of dollars in fraud loss."[97]

Wyndham, through its subsidiaries and franchises, manages hotels, sells timeshares, and licenses its brand name to approximately ninety independently owned hotels.[98] For all associated Wyndham locations, Wyndham also creates and

[94] Plaintiff's Response in Opposition to Wyndham Hotels and Resort's Motion to Dismiss at 1, FTC v. Wyndham Worldwide Corp., No. 2:12-cv-01365-PHX-PGR, 2012 WL 4766957 (D. Ariz. Oct. 1, 2012).

[95] This paper will not analyze or discuss the FTC's allegation of deception against Wyndham.

[96] Plaintiff's Response in Opposition to Wyndham Hotels and Resort's Motion to Dismiss at 2, No. 2:12-cv-01365-PHX-PGR.

[97] *Id.*

[98] Wyndham First Amended Complaint, *supra* note 1, at 3.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.149 ● http://tlp.law.pitt.edu

oversees information security policies.[99] As part of its information security policies, Wyndham requires that each Wyndham branded hotel purchase a designated property management system to handle reservations, manage inventory, and to handle payment card transactions.[100] The designated property management systems store consumer information, including names, addresses, email addresses, telephone numbers, payment card account numbers, expiration dates and card security codes.[101] Each property management system is part of Wyndham's computer network, and is linked to Wyndham's central corporate network, much of which in turn, is housed in a Phoenix data center.[102] Wyndham's computer network is managed solely by Wyndham, and Wyndham alone sets all program rules and password requirements granting employee access to the management system.[103] Wyndham franchisee and brand name owners pay Wyndham to support the property management systems, and, in turn, Wyndham employs a technical support team responsible for managing all technical issues.[104]

The FTC alleges that between April 2008 and January 2010, on three separate occasions, third party intruders gained unauthorized access to Wyndham's computer network and property management systems.[105] The first intrusion occurred in April 2008 when intruders executed a brute force attack on a Wyndham administrator account.[106] The brute force attack was eventually successful and with admittance to the administrator account, the intruders were granted unfettered access to the property management system servers for a number of hotels.[107] The compromised property management servers, which were using discontinued security protocols, did not employ any security mechanisms to prevent access to other connected network servers.[108] The intruders then installed memory-scraping malware on the property management systems, which collected payment card

[99] *Id.*

[100] *Id.*

[101] *Id.*

[102] *Id.*

[103] Wyndham First Amended Complaint, *supra* note 1, at 3–4.

[104] *Id.*

[105] *Id.*

[106] A brute force attack is achieved through guessing multiple use IDs and passwords. Brute force attacks generally trigger account lockouts, which did occur in this instance. Multiple account lockouts typically serve as an indication of an attempted third-party network compromise. Here, Wyndham, because of security failures discussed below, did not discover the breach until four months later. *See id.*

[107] *Id.* at 7.

[108] *Id.*

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.149 ● http://tlp.law.pitt.edu

information, associated with payment authorization transactions.[109] The FTC alleges that this first security breach resulted in the compromise of over 500,000 payment card accounts.[110]

The second breach occurred in March 2009, approximately six months after Wyndham had discovered the first breach.[111] In this instance, the intruders gained unauthorized access to the Wyndham network through a service provider's administrator account in the Phoenix data center.[112] In May 2009, Wyndham consumers complained about fraudulent payment charges after using their payment cards for visits to Wyndham properties.[113] Wyndham then searched their networks for memory-scraping malware, and found malignant programs on over thirty property management systems in their network.[114] The intruders also reconfigured the software to create clear text files containing the payment and personal information of guests using payment cards at the hotels.[115] In this second incident, the intruders were able to access, collect, and use the payment and personal information of more than Wyndham 50,000 consumers.[116]

In late 2009, for the third time, intruders compromised an administrator account on Wyndham's network.[117] Somewhat incredibly, despite the first two breaches, Wyndham still had not successfully limited access on its network. Employing the same technique as before, the intruders were able to access multiple Wyndham property management systems and, similarly, installed memory-scraping malware to access payment card account information on Wyndham's network.[118] As in the second breach, Wyndham discovered the intrusion second-hand.[119] In January 2010, a credit-card issuer notified Wyndham of fraudulent activity using payment cards that were compromised shortly after use at Wyndham properties.[120]

---

[109] Wyndham First Amended Complaint, *supra* note 1.

[110] *Id.*

[111] *Id.*

[112] *Id.*

[113] *Id.*

[114] Wyndham First Amended Complaint, *supra* note 1.

[115] *Id.*

[116] *Id.*

[117] *Id.*

[118] *Id.*

[119] *Id.*

[120] Wyndham First Amended Complaint, *supra* note 1.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.149 ● http://tlp.law.pitt.edu

Twenty-eight property management systems were compromised, and intruders were able to access, collect, and use the payment and personal information of more than 69,000 Wyndham consumers.[121]

The FTC alleges that Wyndham's failure to "implement reasonable and appropriate security measures exposed consumers' personal information to unauthorized access, collection, and use. Such exposure . . . has caused and is likely to cause substantial consumer injury, including financial injury, to consumers and businesses."[122] In totality, the breaches resulted in more than $10.6 million in fraud loss.[123] Both businesses and consumers suffered 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."[124]

As in all the adjudications mentioned above,[125] the FTC noted that no one single practice resulted in culpability. Rather, a combination of practices employed by Wyndham, *taken together*, constituted a failure to "employ reasonable and appropriate measures to protect personal information against unauthorized access," and therefore unfair acts or practices in violation of § 45.[126] In particular, the FTC alleges that Wyndham:

> a. [F]ailed to use readily available security measures to limit access between . . . property management systems, the . . . corporate network, and the Internet, such as by employing firewalls;
> b. [A]llowed software at the Wyndham-branded hotels to be configured inappropriately, resulting in the storage of payment card information in clear readable text;
> c. [F]ailed to ensure the Wyndham-branded hotels implemented adequate information security policies and procedures prior to connecting their local computer networks to Hotels and Resorts' computer network;

[121] *Id.*

[122] Wyndham First Amended Complaint, *supra* note 1.

[123] *Id.* at 8.

[124] *Id.*

[125] *See infra* Part III.B.1–2.

[126] *Id.*

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.149 ● http://tlp.law.pitt.edu

> d. [F]ailed to remedy known security vulnerabilities on Wyndham-branded hotels' servers that were connected to Hotels and Resorts' computer network, thereby putting personal information held by [Wyndham] and the other Wyndham-branded hotels at risk . . . ;
> e. [A]llowed servers to connect to Hotels and Resorts' network, despite the fact that well-known default user IDs and passwords were enabled on the servers, which were easily available to hackers through simple Internet searches;
> f. [F]ailed to employ commonly-used methods to require user IDs and passwords that are difficult for hackers to guess . . . ;
> g. [F]ailed to adequately inventory computers connected to the Hotels and Resorts' network so that [Wyndham] could appropriately manage the devices on its network;
> h. [F]ailed to employ reasonable measures to detect and prevent unauthorized access to [Wyndham's] computer network or to conduct security investigations;
> i. [F]ailed to follow proper incident response procedures, including failing to monitor . . . computer network for malware used in a previous intrusion; and
> j. [F]ailed to adequately restrict third-party vendors' access to [the] network and the Wyndham-branded hotels' property management systems . . . .[127]

The FTC's allegations against Wyndham are almost precisely the same combination of practices, taken together, which the FTC leveled against BJ's and LabMD.[128] Specifically, we see a failure to mask or encrypt consumer information,[129] to limit access to the information by using generic user ID and passwords,[130] and to provide a notification system to alert Wyndham of

[127] *Id.* at 5.

[128] *See infra* Part III.B.1–2 (discussing the BJ's and LabMD adjudications).

[129] *See* Wyndham First Amended Complaint, *supra* note 1, ¶ eb, at 10.

[130] *Id.*

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.149 ● http://tlp.law.pitt.edu

unauthorized access.[131] The failure to limit access to consumer information through inter-network connections is very much in line with the theme of limiting access to consumer information through the use of non-generic ID and password combinations because both issues concern basic systems of access limitation concepts, which should be part of the most basic systems of network security.[132] A disturbingly novel addition to unreasonable practices in the *Wyndham* case is the company's abject failure to mitigate *known* vulnerabilities.[133]

B. Wyndham's Motion to Dismiss

After the FTC filed its complaint, Wyndham, on August 27, 2012, filed a motion to dismiss. In the motion to dismiss, Wyndham argues that "simply put, [§ f4's] prohibition on 'unfair' trade practices does not give the FTC authority to regulate the data-security practices of private companies."[134] Wyndham posits the position that (1) the FTC lacks authority to pursue unfair practices related to data-security, (2) the unfairness actions related to data security require rulemaking, and (3) the injury resulting from these payment card breaches is insufficient to support a claim.

First Wyndham argues that the FTC's unfairness authority does not extend to data security because "nothing in the plain text of Section [45] suggests that Congress gave the FTC authority to regulate data security, which is itself strong evidence that no such authority exists."[135] Specifically, Wyndham argues that the existence of specific statutory authorizations granting the FTC authority to regulate data-security practices preclude an interpretation of § 45 that would grant the FTC jurisdiction to regulate data-security practices outside of those specific

---

[131] *Id.* ¶ dc, g, f, at 10–12.

[132] Advice regarding the use of non-generic passwords, and employing firewalls to protect even personal computers is so ubiquitous that it would be imprudent to call such measures anything other than commonly held knowledge. For example, nearly all network servers employ password configuration operations and firewalls explicitly to prevent unauthorized third-party access. *See* Wes Noonan & Ido Dubrawsky, *Chapter 11: Managing Firewalls*, NETWORK WORLD (Nov. 27, 2007, 2:22 PM), http://www.networkworld.com/subnets/cisco/112707-ch11-managing-firewalls.html.

[133] This new allegation raises the idea of negligence, and possibly recklessness on the part of organizations who fail to remedy known data-security vulnerabilities. Though negligence and recklessness are not elements of an unfair practice under § 45, negligence and recklessness do play a role in limited instances of calculating the nature of consumer injury. *See, e.g.*, Motion to Dismiss by Defendant Wyndham Hotels & Resorts LLC at 7, FTC v. Wyndham Worldwide Corp., No. CV 12-1365-PHX-PGR, 2012 WL 3916987 (D. Ariz. Aug. 27, 2012) (arguing that under state unfair practice statutes a practice is unfair only when "egregious or 'reckless' in nature.") [hereinafter Wyndham's Motion to Dismiss].

[134] *Id.* at 3.

[135] *Id.* at 4.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.149 ● http://tlp.law.pitt.edu

delegations.[136] Wyndham notes that the FTC's action here is analogous to the FDA's attempt to regulate tobacco products that was the focus of *FDA v. Brown & Williamson*.[137]

In *Brown & Williamson*, tobacco manufacturers, advertisers and retailers brought an action against the Federal Drug Administration ("FDA") in response to the FDA's attempted regulation over tobacco products under The Food, Drug and Cosmetic Act ("FDCA").[138] Owing to the structure of the FDCA, and to the fact that the "fundamental precept of the FDCA is that any product regulated by the FDA that remains on the market must be safe and effective for its intended use,"[139] the FDA's proposed regulation over tobacco would statutorily mandate the ban of tobacco products.[140] In evaluating the FDA's statutory authority, the Court looked to whether Congress had "directly spoken to the precise question at issue. If so, the court must give effect to Congress' unambiguously expressed intent."[141] The Court held that because Congress had enacted regulation dealing specifically with tobacco products, Congress thereby "foreclosed the removal of tobacco products from the market."[142] The Court reasoned that:

> Congress' decisions to regulate labeling and advertising and to adopt the express policy of protecting "commerce and the national economy . . . to the maximum extent" *reveal its intent that tobacco products remain on the market*. Indeed, the collective premise of these statutes is that cigarettes and smokeless tobacco will continue to be sold in the United States. *A ban of tobacco products by the FDA would therefore plainly contradict congressional policy*.[143]

---

[136] *Id.* at 4–5 (referencing The Fair Credit Reporting Act ("FCRA"), The Gramm-Leach-Biley Act ("GLBA"), The Children's Online Privacy Protection Act ("COPPA"), The Health Insurance Portability and Accountability Act of 1996, The Health Information Technology for Economic and Clinical Health Act, and The Cable Television Consumer Protection and Competition Act ("CTCPC").).

[137] FDA v. Brown & Williamson Tobacco Corp., 529 U.S. 120, 120 (2000).

[138] *Id.*

[139] *Id.* at 121.

[140] *Id.* at 137.

[141] *Id.* at 121 (internal citations and quotations omitted).

[142] *Id.* at 137.

[143] FDA v. Brown & Williamson Tobacco Corp., 529 U.S. 120 at 139 (emphasis added).

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.149 ● http://tlp.law.pitt.edu

The Supreme Court rejected the FDA's position because Congress had subsequently enacted tobacco-specific legislation.[144] Similar to the reasoning in *Brown*, Wyndham argues that the establishment of substantive data-security standards for private companies has been a contested topic in Congress. Wyndham suggests that the proposal, and failure, of eight data-security bills deem the notion of Congress delegating such an authority to the FTC offensive to common sense.[145]

Second, Wyndham argues that even assuming the FTC was authorized to regulate data security, any regulations require establishment through administrative rulemaking.[146] Wyndham suggests that the FTC has mandated data-security standards, *ex post*, through selective enforcement actions, and that any imposition of such standards on Wyndham would raise "serious constitutional questions of fair notice and due process."[147]

Third, Wyndham argues that even if § 45 could be construed to grant the FTC's authority over data-security practices, the nature of the consumer injury raised in Wyndham is unique, and therefore not subject to protection by the FTC.[148] Wyndham argues that the injury of payment card account theft is always avoidable and never substantial because "[f]ederal law places a $50 limit on the amount for which a consumer can be liable for the unauthorized use of a payment card. And all major card brands . . . waive liability for that small amount."[149]

C. The FTC's Response

On October 1, 2012, the FTC filed a response in opposition to Wyndham's motion to dismiss.[150] Taking an opportunity to respond to Wyndham's claims, the FTC asserts that the FTC has authority to enforce the FTCA against entities for unfair practices related to data-security based on § 45(n), and the FTC is not required to address data security through rulemaking because the unfairness

[144] *Id.*

[145] Wyndham's Motion to Dismiss, *supra* note 133.

[146] *Id.* at 5–6.

[147] *Id.* at 6.

[148] *Id.* at 7.

[149] *Id.*

[150] Plaintiff's Response in Opposition to Wyndham Hotels and Resorts' Motion to Dismiss, FTC v. Wyndham Worldwide Corp., No. CV 12-1365-PHX-PGR, 2012 WL 4766957 (D. Ariz. Oct. 1, 2012) [hereinafter The FTC's Response in Opposition to Motion to Dismiss].

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.149 ● http://tlp.law.pitt.edu

authority is well established, and case by case adjudication is a discretionary power granted to all administrative agencies.[151]

In support of its position the FTC advances several points. First, the FTC argues that § 45 prohibits unfair acts or practices in, or affecting, commerce and that the sector-specific exclusions do not apply to Wyndham.[152] The FTC suggests that Congress purposefully delegated broad power to the FTC, in order to address unanticipated unfair practices, and that, as suggested in *Sperry & Hutchinson*, defining an unfair act or practice is the explicit purview of the FTC.[153] Further, the FTC suggests that the authority to regulate an unfair act or practice are limited to those consumer injuries that are substantial, not reasonably avoided by the consumer, and which are not outweighed by countervailing benefits to consumers or to competition.[154]

Next the FTC suggests that enumerated data security statutes do not preclude or foreclose the FTC from authority over data security because none of the statutes expressly, or impliedly, restrict the FTC's unfairness authority over data security.[155] Rather, the FTC alleges that the statutes "enhance the FTC's legal tools beyond the FTC Act by giving the FTC either civil penalty or rulemaking authority in specific circumstances."[156] In response to Wyndham's reliance of *Brown & Williamson*, the FTC distinguishes its authority over data security from the FDA's authority over tobacco, arguing that in *Brown & Williamson*, the FDA's "subsequent assertion of authority regarding tobacco 'would require the agency to ban' tobacco products under the FDCA, a result that would have mooted the congressionally-authorized regulatory regime."[157]

The Court's reasoning in *Brown & Williamson* is at the epicenter of both Wyndham's and the FTC's interpretation of the unfairness authority, in light of subsequent data-security specific legislation enacted by Congress. Wyndham has suggested that the existence of data-security specific legislation, enacted subsequent to § 45's unfairness authority, preclude the FTC regulation in the data

[151] *Id.* at 12.

[152] *Id.* at 5–6.

[153] *Id.* at 3.

[154] *Id.* at 6.

[155] *Id.* at 8–9.

[156] The FTC's Response in Opposition to Motion to Dismiss, *supra* note 150, at 8.

[157] *Id.* at 6 (internal citations and quotations omitted).

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.149 ● http://tlp.law.pitt.edu

security realm.[158] Characterized as such, Wyndham's argument appears well grounded. However, the Court's reasoning in *Brown & Williamson* explicitly imparts that congressional intent is of paramount importance.[159] On deeper consideration, because the attempted FDA regulation over tobacco products, and requisite product removal, stood in stark contrast to congressional intent to keep tobacco products on the market, the Court found Congress precluded FDA's authority.[160] Congressional intent to keep tobacco on the market was embodied in legislation enacted subsequent to the FDCA, which would have precluded any tobacco product ban.[161] Thus, it appears that subsequent statutes, which more specifically address the topic at hand, are not preclusive, as Wyndham suggests, *unless* that subsequent statute embodies congressional intent precluding an Agency's statutory enforcement construction. The FTC advances this position by asserting that because Congress has enacted no inconsistent or irreconcilable legislation against the FTC's authority over data-security, that the FTC's interpretation of § 45 to regulate unfair data security practices is properly founded.[162]

The FTC also argues that it is authorized to announce new principles through adjudication, and further, that the principle at force in the *Wyndham* complaint is not a new principle at all. The FTC asserts that the action against Wyndham is "simply a standard application of this authority against an entity that failed to undertake reasonable measures to protect information that it collected about consumers."[163] Furthermore, the FTC defends its enforcement history by noting that the decision to enforce § 45 on a case-by-case is a discretionary power granted administrative agencies. In particular, the FTC notes that it would be impossible "to set forth the type of particularized guidelines that Wyndham suggests would be appropriate for rulemaking," owing to continually developing industry standards.[164] Further, the FTC notes that its reasonableness inquiry is perfectly suited to the ever-evolving landscape of data types and security vulnerabilities—a standard which courts are equipped to navigate.[165] Additionally, the FTC emphasizes that it

---

[158] Wyndham's Motion to Dismiss, *supra* note 133.

[159] FDA v. Brown & Williamson Tobacco Corp., 529 U.S. 120, 120 (2000).

[160] *Id*.

[161] *Id*.

[162] The FTC's Response in Opposition to Motion to Dismiss, *supra* note 150, at 8.

[163] *Id.* at 12.

[164] *Id.*

[165] *Id.* at 13.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.149 ● http://tlp.law.pitt.edu

has been "investigating, testifying about, and providing public guidance on companies' data security obligations under the [FTCA] for more than a decade, and so is not moving in a new direction through the instant action."[166]

Finally, the FTC argues that consumers suffered a substantial injury as a result of Wyndham's data-security practices (or lack thereof). The FTC argues that the injury suffered by Wyndham consumers is exactly the type of injury the FTC is tasked to remedy—small harms to large numbers of consumers.[167] The FTC further posits that, whether or not the injury is reimbursed is not a consideration for whether an injury is avoidable, and that even if reimbursed, the injury is not fully mitigated.[168] As to Wyndham's argument that the standard of liability for failing to adequately protect consumer data should correspond to the small risk of injury posed by the theft of consumer information, the FTC argues that "the only balancing contemplated by the FTCA is weighing the benefit to consumers of inferior information security against the injury to consumers of the resulting potential exposure of their information."[169]

D. Wyndham's Motion to Dismiss Denied

On April 7, 2014, the court issued an opinion denying Wyndham's motion to dismiss pursuant to Federal Rule of Civil Procedure 12(b)(6).[170] In rejecting the arguments raised by Wyndham's motion, the court found: (1) Wyndham's challenge to the FTC's authority to assert an unfairness claim in the data-security is not preempted by the *Brown & Williamson* precedent because, in this instance, the circumstances differ;[171] (2) even absent formally promulgated regulations, the FTC does not violate fair notice principles because precedent provides that "agencies like the FTC need not formally issue regulations,"[172] and; (3) the FTC's allegations were sufficiently pled to support the unfairness and deception claims, and to survive a motion to dismiss.[173] The court denied the motion on all counts, finding that Wyndham's "motion to dismiss demands that this court carve out a data security exception to the FTC's authority and that the FTC publish regulations

---

[166] *Id.*

[167] The FTC's Response in Opposition to Motion to Dismiss, *supra* note 150.

[168] *Id.* at 14.

[169] *Id.* at 7.

[170] FTC v. Wyndham Worldwide Corp., No. 13-1887(ES), 2014 WL 1349019, at *1 (D.N.J. Apr. 7, 2014).

[171] *Id.*

[172] *Id.*

[173] *Id.*

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.149 ● http://tlp.law.pitt.edu

before filing an unfairness claim in federal court. These demands are, in fact, what bring us to uncharted territory."[174]

1. FTC's Authority to Assert Unfairness Claim Not Preempted by Brown & Williamson

First, the court rejected Wyndham's invitation to carve out a data-security exception to the FTC's unfairness authority based on *Brown & Williamson*, because Wyndham failed to explain how the FTC's unfairness authority "would lead to a result that is incompatible with more recent legislation and thus would plainly *contradict* congressional policy."[175] Importantly, the court noted that subsequent data-security legislation is not at odds with the FTC's unfairness authority, but rather, complementary.[176] The court reasoned that because subsequent statutes like the FCRA, GLBA and COPPA set forth different standards for consumer injury based on specified circumstances, these statutes provide the FTC with additional enforcement tools.[177]

2. FTC Authorized to Bring Unfairness Claims Absent Formal Rules

The court considered whether the FTC must promulgate rules and regulations to satisfy fair notice requirements.[178] The court rejected Wyndham's argument that the FTC cannot bring an enforcement action under the unfairness authority without first formally publishing rules and regulations.[179] The court held that fair notice of forbidden or required conduct does not require the FTC to formally issue rules and regulations before it can file an unfairness claim.[180] Section 45 proscriptions are flexible and "to be defined with particularity by the myriad of cases from the field of business . . . Accordingly, Circuit Courts of appeal have affirmed FTC unfairness actions in a variety of contexts *without* preexisting rules or regulations

---

[174] *Id.* at 4.

[175] *Id.* at 6 (internal quotations and citations removed); *see also* FDA v. Brown & Williamson Tobacco Corp., 529 U.S. 120, 139 (2000).

[176] FTC v. Wyndham Worldwide Corp., No. 13-1887(ES), 2014 WL 1349019, at *7 (D.N.J. Apr. 7, 2014). *See also* discussion *supra* Part III.C.

[177] *Id.* at 7. The court also rejected arguments pertaining to alleged representations by the FTC disclaiming authority over data discussion. *See id.* at 7–9 (providing that "the public record here is unlike the lengthy, forceful history of [the FDA's] repeated and consistent disavowals in *Brown & Williamson*.").

[178] *See* discussion *supra* Part III.B–C.

[179] Wyndham Worldwide Corp., No. 13-1887(ES), 2014 WL 1349019, at *12–13.

[180] *Id.* at 11–12.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.149 ● http://tlp.law.pitt.edu

specifically addressing the conduct-at-issue."[181] The court concluded that especially given the rapidly-evolving nature of data security, Wyndham's argument is untenable because "the consequence of accepting [Wyndham's] proposal: 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 [§ i45] of the [FTCA]."[182]

3. FTC Sufficiently Pled Substantial, Unavoidable Consumer Injury

Next, the court considered whether the FTC alleged substantial, unavoidable consumer injury and otherwise satisfied federal pleading requirements.[183] Here again, the court rejected Wyndham's argument, and held that under the Federal Rule of Civil Procedure 8(a), the FTC sufficiently pled an unfairness claim under the FTCA.[184] In deciding this issue, the court emphasized its standard of review on the motion to dismiss, and provided that "all allegations in the complaint must be taken as true, and the plaintiff must be given the benefit of every favorable inference to be drawn therefrom."[185] Comporting with this standard, the court reasoned that the FTC sufficiently pled that Wyndham's data security practices were unfair.[186] The FTC showed that Wyndham caused substantial injury to consumers, which were not reasonably avoidable by the consumers themselves, and which were not outweighed by countervailing benefits to consumers or competition.[187] The court found that the FTC adequately pled a substantial injury to consumers because the FTC allegations, taken as true, included unreimbursed financial injury. In concluding, the court held that the FTC's allegations of Wyndham's unreasonable data security practices supported reasonable inferences

[181] *Id.* (internal citations and quotations omitted).

[182] *Id.* at 15. Interestingly, the court seems to infer that fair notice of reasonable and appropriate data-security measures may be drawn from the numerous public complaints, consent agreements, and public statements issued by the FTC, and further implies that those same promulgations could provide guidance for courts and litigators as to determining whether data security measures are reasonable and appropriate in specific circumstances. *Id.* at 14–15.

[183] *Id.*

[184] Wyndham Worldwide Corp., No. 13-1887(ES), 2014 WL 1349019, at 16.

[185] *Id.* at 3.

[186] *See id.* at 16.

[187] This analysis focuses on two of Wyndham's issues in challenging the FTC's allegations: (1) that the FTC insufficiently pled that Wyndham's conduct caused or was likely to cause substantial injury to consumers and; (2) that the FTC insufficiently pled that the consumer injuries were not reasonably avoidable by the consumers themselves. *See id*. at 16. *See also* discussion *supra* Part III.B.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.149 ● http://tlp.law.pitt.edu

in the FTC's favor that "[Wyndham's] data[]security practices *caused* theft of personal data, which ultimately *caused* substantial injury to customers."[188]

Finally, the court summarily refused to accept Wyndham's claim that the alleged consumer injuries were reasonably avoidable.[189] The court reasoned that Wyndham "effectively asks the Court to hold that, as a matter of law, any financial injury from payment card theft data is reasonably avoidable and that the FTC's allegation to the contrary, could not be true under any factual scenario."[190] The court held that they could not "make such a far-reaching conclusion regarding an issue that seems fact-dependent."

E. Looking to Trial

Bearing in mind that the court's opinion was subject to the standards of review for a motion to dismiss, several important implications may be drawn from the court f opinion. It is likely that, given the court's emphasis on the standard of review for a motion to dismiss, the most important determinations for the court at trial will involve a factual determination of whether the FTC can prove that Wyndham's practices caused substantial injury, not reasonably avoidable by the consumer. Most telling of this notion is the court's attempt to downplay the gravity of its decision to dismiss, and perhaps to assuage industry concern, explicitly noting that:

> To be sure the Court does *not* render a decision on liability. Instead, it resolves a motion to dismiss a complaint. And this decision does *not* give the FTC a blank check to sustain a lawsuit against every business that has been hacked. Instead the court denies a motion to dismiss given the allegations in *this* complaint—which must be taken as true *at this stage* in view of binding and persuasive precedent.[191]

On the surface, the court assures a narrow holding and almost hesitantly permits the suit to proceed based on the specific allegations in the Wyndham complaint, justified only by precedent and the federal standard of review on a

---

[188] Wyndham Worldwide Corp., No. 13-1887(ES), 2014 WL 1349019, at 17. *See also supra* note 136.

[189] *Id.*

[190] *Id.*

[191] *Id.*

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.149 ● http://tlp.law.pitt.edu

motion to dismiss. Significantly, the court emphasizes that the decision would not issue the FTC a blank check to sustain lawsuits against any business impacted by third-party breaches, limited only by a forceful disclaimer that "the court denies a motion to dismiss given the allegations in *this* complaint—which must be taken as true *at this stage*."[192] While the court's opinion is not necessarily dispositive of what may proceed at trial, it seems apparent that the court believes both that the FTC's unfairness authority encompasses the enforcement of reasonable and appropriate data security, and that the FTC need not formally promulgate rules and regulations to bring an unfairness claim in federal court.[193]

The court's treatment of the third issue, whether the FTC's allegations sufficiently supported a claim of substantial, unavoidable consumer injury, is particularly noteworthy. Even though Wyndham argued that no injury-in-fact resulted from the breaches, the court accepted the FTC's allegations, stating that "for the purposes of resolving [Wyndham's] motion, the[] allegations must be accepted as true."[194] Amazingly, in a footnote to that discussion, the court provided

> [t]he parties contest whether non-monetary injuries are cognizable under [§ 45 of the FTCA]. Although *the Court is not convinced that non-monetary harm, is as a matter of law, unsustainable under [§ 45 of the FTCA]*, the Court need not reach this issue given the analysis of the substantial harm element above.[195]

The notion that non-monetary harm may be cognizable under an unfairness claim, is itself a profound implication, and one that could significantly expand the scope of the FTC's unfairness authority. Further, because the court adopted the FTC's allegations as true and thereby was able to reasonably infer that a substantial consumer injury had occurred, the issue of whether a non-monetary harm is a sustainable injury under § 45 may, indeed, be left to open court. At the very least, although the court need not have reached the issue on a motion to dismiss, the court's dicta infers that the issue may well arise at trial—and that, for now, the Federal District Court of New Jersey *may* consider non-monetary harm as a sustainable consumer injury under § 45.

---

[192] *Id.* at 4 (emphasis added).

[193] *Id.* at 1.

[194] Wyndham Worldwide Corp., No. 13-1887(ES), 2014 WL 1349019, at 16.

[195] *See id.* at 17 n.15

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.149 ● http://tlp.law.pitt.edu

CONCLUSION

The outcome, of course, remains to be seen and predictions are, at present, premature. In the interim, this article has aimed to provide (1) an understanding of the history of the FTC's unfairness authority; (2) an examination of important examples of the FTC's enforcement of the unfairness authority through consent orders, in order to provide the factors, and data security measures that the FTC considers reasonable and appropriate for collecting personally identifiable consumer information; (3) a discussion of arguments challenging the FTC's unfairness authority posited in *Wyndham*, and an evaluation their strengths; and (4) most fundamentally, to dispel inapposite and rudimentary characterizations of the FTC's unfairness authority enforcement as irrational, inconsistent or illegitimate.

The central significance *Wyndham* was summed earlier in this piece as a question: after a business has electronically collected and stored personal information, how far must it go to protect it? The answer: cash is king.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.149 ● http://tlp.law.pitt.edu