MORRISON | FOERSTER

Morrison & Foerster Client Alert

September 24, 2015

The FTC v. Wyndham Reexamined—A True Test of the Contours of Unfairness

By Andrew Serwin

This article was first published by The Lares Institute Blog (September 24, 2015).

Many articles have been written recently about the Third Circuit's recent ruling in the *FTC v. Wyndham*, — F.3d — 2015 WL 4998121 (3d Cir. 2015) which, while trumpeting the case's importance, do not address some of the more interesting aspects of the opinion. This decision, while notable at some level, sets the stage for the more important issues that the court did not decide, but which will have to be decided as the case is litigated. As a result, it is likely that future opinions will be of more importance, and this article examines certain potential issues, including some that are hinted at in the opinion.

To understand the opinion, and what it does and doesn't decide, one must understand the current procedural posture of the case. The motion before the court was a 12(b)(6), or motion to dismiss, which essentially raised two issues—whether the FTC had the authority to regulate cybersecurity in accordance with it unfairness authority, and whether Wyndham had "fair notice" of whether allegedly deficient cybersecurity practices could "fall short" of §45(a).

IT DIDN'T DECIDE THE MERITS

One of the key issues that has been blurred in certain other articles is that this decision was not a summary judgment motion under Rule 56, or otherwise on the merits of the case. Instead, it is a decision that tested the legal principles identified above, and, as the Third Circuit noted, for these purposes, the court must "accept all factual allegations as true, and construe the complaint in the light most favorable to the [FTC], and determine whether, under any reasonable reading of the complaint, the [FTC] may be entitled to relief." As a result, the court did not, and could not, make factual findings about whether Wyndham did, or did not, have adequate security. Instead, as it must under 12(b)(6), the court assumed all of the FTC's allegations were true. As discussed below, that is where the future decisions will be of critical importance as the contours of unfairness are set.

UNITED STATES

California
Tiffany Cheung (415) 268-6848
Rebekah Kaufman (415) 268-6148
Christine E. Lyon (650) 813-5770
David F. McDowell (213) 892-5383
Purvi G. Patel (213) 892-5296
Andrew Serwin (858) 720-5134
Stephanie Sharron (650) 813-4018
David M. Walsh (213) 892-5262

New York
Melissa Crespo (212) 336-4354
John F. Delaney (212) 468-8040
Michael B. Miller (212) 468-8009
Suhna N. Pierce (212) 336-4150
Marian Waldmann Agarwal (212) 336-4230
Miriam H. Wugmeister (212) 506-7213

Washington, D.C.
L. Richard Fischer (202) 887-1566
Adam J. Fleisher (202) 887-8781
Libby J. Greismann (202) 778-1607
Julie O'Neill (202) 887-8764
Cynthia J. Rich (202) 778-1652
Nathan David Taylor (202) 778-1644

EUROPE

Berlin
Hanno Timner 49 30 72622-1346
Lokke Moerel 44 20 79204054

Brussels
Karin Retzer 32 2 340 7364
Sotirios Petrovas (212) 336-4377
Alja Poler De Zwart 32 2 340 7360
Ronan Tigner 32 2 340-7358

London
Alex van der Wolk 44 20 79204074
Alistair Maughan 44 20 79204066
Daniela Guadagno 44 20 79204024
Sarah Wells 44 20 79204167

ASIA

Beijing
Paul D. McKenzie 86 10 5909 3366
Wei Zhang 86 10 5909 3366

Hong Kong
Gordon A. Milner 852 2585 0808

Singapore
Daniel P. Levison 65 6922 2041

Tokyo
Toshihiro So 81 3 3214 6568
Kyoko Sato 81 3 3214 6936
Yukihiro Terazawa 81 3 3214 6585

IT DID PERMIT THE FTC TO REGULATE CYBERSECURITY VIA UNFAIRNESS

In the security and privacy realm, the FTC uses two prongs of its statutory authority under Section 45(a)[1]—deception and unfairness. There is a significant amount of history that surrounds these concepts, which I examine in, *The Federal Trade Commission and Privacy: Defining Enforcement and Encouraging the Adoption of Best Practices*, 48 San Diego L. Rev. 809 (2011).[2] The Supreme Court has previously weighed in on the scope of the FTC's jurisdiction, the FTC has issued a statement regarding its belief regarding what unfair practices are, and ultimately Congress amended Section 45(a) to conform to these views.

Ultimately, the Unfairness Statement was codified by Congress via an amendment to 15 U.S.C. § 45(n), which now reflects the consumer injury focus. Under this formulation a practice is unfair if it (1) causes or is likely to cause substantial injury to consumers (2) that is not reasonably avoidable by consumers themselves and (3) not outweighed by countervailing benefits to consumers or to competition.[3]

There are two notable portions of the Third Circuit's decision regarding these factors. The first is that, contrary to Wyndham's position, the Third Circuit did find that the FTC did have jurisdiction to pursue unfairness claims based upon an alleged lack of information security, stating that the court was "not persuaded that the alleged conduct falls outside the plain meaning of 'unfair.'"[4] This essentially, subject to potential appeals, at least in the Third Circuit, ends the arguments made by Wyndham, and others, on the jurisdictional arguments regarding unfairness and security.

The second raises some issues about what the FTC must prove in order to establish unfairness based upon allegations related to cybersecurity. Wyndham argued that while the FTC must, at minimum, produce evidence to establish these three factors before an act is declared to be unfair, the FTC may have to establish other additional factors beyond those identified in §45(n). While this issue was not one the Court had to decide at this time, it did seem to indicate that in this context the three unfairness factors might not completely express the burden the FTC must meet.[5]

IT DID DECIDE WYNDHAM HAD "FAIR NOTICE"

Like any government agency, the FTC's jurisdiction is not unlimited, and due process concerns, among other legal issues, place an outer limit on certain regulatory activities. The concept of "fair notice" is one of those outer limits, and this issue was also examined by the Third Circuit. The court began its analysis by stating "A conviction or punishment violates the Due Process Clause of our Constitution if the statute or regulation under which it is obtained 'fails to provide a person of ordinary intelligence fair notice of what is prohibited, or is so standardless that it authorizes or encourages seriously discriminatory enforcement.'"[6]

---

[1] 15 U.S.C.A. §45 is also referred to as Section 5 of the FTC Act.

[2] This law review article can be found at http://www.laresinstitute.com/wp-content/uploads/2012/03/FTC.pdf.

[3] Serwin, The Federal Trade Commission and Privacy: Defining Enforcement and Encouraging the Adoption of Best Practices, 48 San Diego L. Rev. 809 (2011).

[4] *FTC v. Wyndham*, — F.3d — 2015 WL 4998121 (3d Cir. 2015).

[5] *FTC v. Wyndham*, — F.3d — 2015 WL 4998121 (3d Cir. 2015)("Arguably, § 45(n) may not identify all of the requirements for an unfairness claim. (While the provision forbids the FTC from declaring an act unfair "unless" the act satisfies the three specified requirements, it does not answer whether these are the only requirements for a finding of unfairness.) ").

[6] *FTC v. Wyndham*, — F.3d — 2015 WL 4998121 (3d Cir. 2015), citing FCC v. Fox Television Stations, Inc., —— U.S. —— 132 S. Ct. 2307, 2317, 183 L. Ed. 2d 234 (2012).

The issue here was Wyndham's argument that it did not have fair notice of the standards—what cybersecurity practices the FTC believed were required—under Section 45(a). The court did not accept this argument, finding, at least at the pleading stage, that Wyndham need only have fair notice that its alleged conduct could fall within Section 45(a). It will remain to be seen on remand what level of notice the District Court believes was necessary and appropriate regarding the standards themselves that the FTC seeks to impose upon companies under its unfairness jurisdiction.

IT DID NOT DECIDE THAT CONSENT DECREES WERE "PRECEDENTIAL"

As part of the fair notice analysis, the court examined what the impact the FTC's prior consent decrees had in this context. The court was clear on this point:

We agree with Wyndham that the consent orders, which admit no liability and which focus on prospective requirements on the defendant, were of little use to it in trying to understand the specific requirements imposed by § 45(a).[7]

This statement will be important both for Wyndham in this case, as well as other companies as they attempt to navigate negotiations with the FTC in the future. Thus it seems clear that while the prior consent decrees provide some guidance regarding what the FTC thinks, they do not offer binding precedent as an opinion of a court would.

IT DID NOT APPEAR TO IMPOSE A BURDEN TO REVIEW CONSENT DECREES, AT LEAST IN 2008

While not directly relevant to the fair notice arguments, the court also noted that, in contrast to the FTC's position, in 2008 it could have been "unfair" to expect companies to review the FTC complaints or consent decrees that it posts on its website.[8] The ultimate relevance of this point in the Wyndham case will be determined as the case progresses, but the court clearly stated that these documents may not be the kinds of legal documents that companies "typically consulted."[9] Whether that same analysis will hold true for companies examining these issues today will remain to be seen, but at least for Wyndham and others in 2008, the court declined to impose this burden.

IT DID NOT DECIDE HOW TO ASSESS CONSUMER HARM

Now that the jurisdictional issues are resolved, at least for now, the case will move on to the merits, which means the burden will shift to the FTC to prove its case and produce evidence to support the three elements of unfairness noted above. While all three elements will likely be litigated, the first point whether the alleged practices cause, or are likely to cause substantial injury to consumers will certainly be a key issue.

This issue is frequently addressed in the data security class action litigation context involving a related issue—Article III standing, and the Article III issues can be summarized in the three part test set forth by the Supreme Court. The plaintiff has the burden in those cases to establish:

- That it has suffered an injury in fact—an invasion of a legally-protected interest which is (a) concrete and particularized; and (b) actual or imminent, not conjectural or hypothetical;

[7] *FTC v. Wyndham*, — F.3d — fn. 22, 2015 WL 4998121 (3d Cir. 2015).

[8] *FTC v. Wyndham*, — F.3d — fn. 23, 2015 WL 4998121 (3d Cir. 2015).

[9] *Id.*

- A causal connection between the injury and the conduct complained of—the injury has to be fairly traceable to the challenged action of the defendant, and not the result of the independent action of some third party not before the court; and
- That it is likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision.[10]

In the data breach context, many courts have found that the plaintiff cannot meet the burden to establish the requisite level of injury, which results in dismissal of the case.[11] In fact, this conclusion was recently reached by the District Court in New Jersey, the District Court that will decide this matter, in a case involving the alleged improper mailing of Social Security numbers which permitted them to be visible.[12]

Interestingly, in examining situations where the FTC has been given rulemaking authority in other contexts, the Court examined other statutory schemes that appear to have differing harm standards. One such example is the GLBA, which the Court stated empowered the FTC to establish appropriate standards "… to protect against unauthorized access to or use of … records … which could result in substantial harm *or inconvenience to any customer.*"[13]

How the GLBA standard will be interpreted versus the injury element of Section 5 noted above, as well as what the District Court will examine and decide what the FTC must produce to meet its burden on this point remains to be seen, but this will be one of the key issues as we test the contours of unfairness and cybersecurity.

About Morrison & Foerster:

We are Morrison & Foerster — a global firm of exceptional credentials. Our clients include some of the largest financial institutions, investment banks, Fortune 100, technology and life science companies. We've been included on *The American Lawyer's A-List* for 11 straight years, and *Fortune* named us one of the "100 Best Companies to Work For." Our lawyers are committed to achieving innovative and business-minded results for our clients, while preserving the differences that make us stronger. This is MoFo. Visit us at www.mofo.com.

Morrison & Foerster has a world-class privacy and data security practice that is cross-disciplinary and spans our global offices. With more than 60 lawyers actively counseling, litigating, and representing clients before regulators around the world on privacy and security of information issues, we have been recognized by *Chambers* and *Legal 500* as having one of the best domestic and global practices in this area.

[10] Serwin, Information Security and Privacy, Section 34:27 (West 2015), *citing Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560, 112 S. Ct. 2130, 119 L. Ed. 2d 351, 34 Env't Rep. Cas. (BNA) 1785, 22 Envtl. L. Rep. 20913 (1992).

[11] *See, e.g., In re Zappos.com, Inc.,* Customer Data Sec. Breach Litig. — F.Supp.3d —- 2015 WL 3466943, (D. Nev. 2015)(holding that "the increased risk of identity theft and fraud stemming from the Zappos.com security breach does not constitute injury in fact sufficient to confer standing."); Fernandez v. Leidos, Inc., — F.Supp.3d —- 2015 WL 5095893 (E.D.Cal. 2015)(holding that plaintiff's allegations of identity theft, which included "(i) multiple attempted logins to his Microsoft and Yahoo accounts requiring him to change his passwords and login information several times, and (ii) notification by his bank, Bank of America, that someone posing as Fernandez attempted to open a bank account in a Bank of America branch in San Diego, California, using his wrongfully disclosed and compromised PII/PHI" were insufficient to establish Article III standing); Lewert v. P.F. Chang's China Bistro, Inc., 2014 WL 7005097, (N.D.Ill. 2014).

[12] *Crisafulli v. Ameritas Life Ins. Co.,* 2015 WL 1969176, (D.N.J. April 29, 2015).

[13] *FTC v. Wyndham,* — F.3d — 2015 WL 4998121, *8 (3d Cir. 2015) (emphasis in original).

For more information about our people and services and the resources we offer such as our treatise setting out the U.S. and international legal landscape related to workplace privacy and data security, "*Global Employee Privacy and Data Security Law,*" or our free online Privacy Library, please visit our practice page and follow us on Twitter @MoFoPrivacy.

Because of the generality of this update, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations. Prior results do not guarantee a similar outcome.