No. 14-3514

IN THE

# United States Court of Appeals for the Third Circuit

FEDERAL TRADE COMMISSION,
Plaintiff-Appellee,

v.

WYNDHAM HOTELS & RESORTS, LLC, *et al.*,
Defendants-Appellants.

On Appeal from the United States District Court
for the District of New Jersey
No. 2:13-cv-01887-ES-SCM (Salas, J.)

## BRIEF OF *AMICI CURIAE* CHAMBER OF COMMERCE OF THE UNITED STATES OF AMERICA, AMERICAN HOTEL & LODGING ASSOCIATION, AND NATIONAL FEDERATION OF INDEPENDENT BUSINESS IN SUPPORT OF APPELLANT

CATHERINE E. STETSON
HARRIET P. PEARSON
BRET S. COHEN
SEAN MAROTTA
ADAM A. COOKE
HOGAN LOVELLS US LLP
555 Thirteenth Street, N.W.
Washington, D.C. 20004
(202) 637-5600

Counsel for *Amici Curiae*

KATE COMERFORD TODD
STEVEN P. LEHOTSKY
SHELDON GILBERT
U.S. CHAMBER LITIGATION CENTER, INC.
1615 H Street, N.W.
Washington, D.C. 20062
(202) 463-5337

Counsel for *Amicus Curiae* Chamber of the Commerce of the United States of America

October 14, 2014

(Additional counsel listed on inside cover)

Additional Counsel:

BANKS BROWN
MCDERMOTT WILL & EMERY LLP
340 Madison Ave.
New York, NY 10713
(212) 547-5488

Counsel for *Amicus Curiae* American Hotel & Lodging Association

KAREN R. HARNED
NATIONAL FEDERATION OF INDEPENDENT BUSINESS SMALL BUSINESS LEGAL CENTER
1201 F Street, N.W., Suite 200
Washington, D.C. 20004
(202) 314-2048

Counsel for *Amicus Curiae* National Federation of Independent Business

## RULE 26.1 CORPORATE DISCLOSURE STATEMENT

The Chamber of Commerce of the United States of America is a non-profit, tax-exempt organization incorporated in the District of Columbia. The Chamber has no parent company and no publicly held company has ten percent or greater ownership in the Chamber.

The American Hotel & Lodging Association has no parent company and no publicly held company holds more than a ten percent interest in the AH&LA.

The National Federation of Independent Business has no parent company and no publicly held company holds more than a ten percent interest in the NFIB.

# TABLE OF CONTENTS

# TABLE OF AUTHORITIES

Page(s)

**CASES:**

## TABLE OF AUTHORITIES—Continued

Page(s)



**STATUTES AND RULES:**



**OTHER AUTHORITIES:**

## TABLE OF AUTHORITIES—Continued

Page(s)

## TABLE OF AUTHORITIES—Continued

Page(s)

IN THE

# United States Court of Appeals for the Third Circuit

---

FEDERAL TRADE COMMISSION,
Plaintiff-Appellee,

v.

WYNDHAM HOTELS & RESORTS, LLC, *et al.*,
Defendants-Appellants.

---

On Appeal from the United States District Court
for the District of New Jersey
No. 2:13-cv-01887-ES-SCM (Salas, J.)

---

**BRIEF OF *AMICI CURIAE* CHAMBER OF COMMERCE OF THE UNITED STATES OF AMERICA, AMERICAN HOTEL & LODGING ASSOCIATION, AND NATIONAL FEDERATION OF INDEPENDENT BUSINESS IN SUPPORT OF APPELLANT**

---

## STATEMENT OF INTEREST OF *AMICI CURIAE*

The Chamber of Commerce of the United States of America (the Chamber), the American Hotel & Lodging Association (AH&LA), and the National Federation of Independent Business (NFIB) respectfully submit this brief as *amici curiae* in support of petitioner Wyndham Hotels & Resorts, LLC (Wyndham)'s appeal from the District Court's order denying its motion to dismiss.[1]

[1] Pursuant to Federal Rule of Appellate Procedure 29, the Chamber, AH&LA, and NFIB certify that all parties have consented to the filing of this brief. The

The Chamber is the world's largest business federation. The Chamber represents 300,000 direct members and indirectly represents the interests of more than three million companies and professional organizations of every size, in every industry sector, and from every region of the country. A principal function of the Chamber is to represent the interests of its members in matters before Congress, the Executive Branch, and the courts. To that end, the Chamber regularly files *amicus curiae* briefs in cases raising issues of concern to the nation's business community.

The AH&LA is the only national association representing all sectors and stakeholders in the lodging industry, including individual hotel property members, hotel companies, student and faculty members, and industry suppliers. It has played this role for over a century providing members with national advocacy on Capitol Hill, public relations services and education, research, and information.

The NFIB is the nation's leading small business association, representing approximately 350,000 members across the country. To fulfill its role as the voice for small business, the NFIB frequently files *amicus curiae* briefs in cases that will impact small businesses, such as this case.

---

Chamber, AH&LA, and NFIB likewise certify that no party's counsel authored this brief in whole or in part; no party or party's counsel contributed money intended to fund the brief's preparation or submission; and no person other than the Chamber, AH&LA, NFIB, and their members and counsel contributed money intended to fund the brief's preparation or submission.

The businesses represented by the Chamber, AH&LA, and NFIB use electronic data, including personal data, to enhance business efficiency and to benefit consumers. For the modern company, personal and other types of digitized data are essential for a multitude of reasons, including administering employee benefits programs, processing payment and shipping information, and enabling customer loyalty programs, among many other uses. *Amici* all have a significant interest in explaining to the Court the legal and policy implications of the District Court's order denying Wyndham's motion to dismiss.

## SUMMARY OF ARGUMENT

The Federal Trade Commission (FTC or Commission)'s use of its enforcement authority to regulate "unfair" trade practices under Section 5 of the FTC Act, 15 U.S.C. § 45, has a checkered past. Thirty years ago, the FTC sought to significantly expand the scope of its Section 5 authority, invoking the then-extant version of the statute to advance its consumer protection goals in ways far beyond those envisioned by Congress. Congress reacted to that overreach, codifying into law significant limits on the scope of the FTC's authority.

The FTC has strayed down the same path again. Over the course of the past decade, the FTC has departed from the statutory underpinnings of Section 5's prohibition against "unfair" acts or practices, leveraging its enforcement authority to extract settlements from businesses that themselves have been victimized by

data-security breaches, and that have no formal notice of the standards the FTC accuses them of violating. Although by statute the FTC has an important role to play in protecting America's consumers, the agency's "unfairness" authority does not permit it to set and enforce—whether through litigation or consent orders[2]—general data-security policy. Indeed, the FTC expressly has acknowledged that it does not possess the general authority to regulate data security, which is precisely why it has and continues to lobby Congress for additional rulemaking authority.

The FTC should not be permitted to circumvent the full legislative process by establishing rules and principles through private enforcement actions, resulting in a string of consent orders that the FTC publishes and which it holds out to other businesses as if they were established law. This incremental—and unilateral—regulation-through-settlement subjects American businesses to vague, unknowable, and constantly changing data-security standards. Companies often are unaware of the standards to which they are held until after they receive a notice of investigation from the FTC, at which point they must settle or expend considerable resources fighting the agency. The *in terrorem* effect of a notice by itself is significant. The FTC's arsenal of enforcement capabilities carries a real risk of

[2] Often when the FTC claims that a data-security breach constitutes an "unfair" trade practice, the Commission has been able to obtain Section 5 consent orders from the targeted businesses. This case is among the first data-security "unfairness" proceedings to be evaluated by a court.

affecting business judgment, slowing the adoption of new technologies, and chilling business from sharing information about breaches to avert malicious attacks in the future.

Permitting the FTC to proceed on a theory that suffering a data breach is an "unfair" trade practice would expose most businesses in America to the potential for a government enforcement action whenever that business suffers a cyber attack or other incident that potentially compromises personal data. Congress did not envision that result when it passed legislation limiting the FTC's Section 5 authority over "unfair" acts or practices, and this Court should not countenance it.

The businesses represented by *amici* take seriously their responsibility to safeguard all personally identifying electronic information. But the stark reality is that malicious actors—such as foreign intelligence services seeking competitive economic advantages over U.S. businesses, terrorist groups, hacking collectives, and criminal organizations— target business technology to obtain valuable data, including personal data and intellectual property.[3] No data security is perfect, and breaches do occur, exposing digital information. When criminals accessed

[3] *See, e.g.*, DJ Summers, *Cold War on Business: Fighting in the Cyber Trenches*, Fortune, Oct. 13, 2014, http://www.fortune.com/2014/10/13/cold-war-on-business-cyber-warfare; Press Release, U.S. Dep't of Justice, *U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage* (May 19, 2014), http://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

Wyndham's business computer systems, the FTC sought court redress not against the thieves, but against the business that was victimized by them, contending in Count II of its complaint that Wyndham's data-security policy was an "unfair," and therefore unlawful, trade practice.

The FTC has overreached. It lacks the legal authority to act as a roving regulator of data-security standards, because the statute under which the FTC has purported to act—Section 5 of the FTC Act—does not authorize the Commission to proceed as it has in this case.

The District Court's order denying Wyndham's motion to dismiss the "unfair" practices count of the Amended Complaint should be reversed.

## ARGUMENT

### I. THE FTC'S SECTION 5 AUTHORITY TO PROHIBIT UNFAIR TRADE PRACTICES DOES NOT GIVE THE FTC AUTHORITY TO ESTABLISH GENERAL DATA-SECURITY POLICY.

As the Supreme Court emphasized just last term, "When an agency claims to discover in a long-extant statute an unheralded power to regulate a significant portion of the American economy, we typically greet its announcement with a measure of skepticism." *Utility Air Regulatory Grp. v. EPA*, 134 S. Ct. 2427, 2444 (2014) (internal quotation and citation omitted). The FTC's use of Section 5's prohibition against "unfair" acts or practices to regulate data security—which affects just about every American business, regardless of size or industry, in our

increasingly interconnected economy—is precisely the type of expansive agency interpretation that the Supreme Court rejected as "an enormous and transformative expansion in [an agency]'s regulatory authority without clear congressional authorization," and which this Court should reject as well. *Id.*

Appellant Wyndham's opening brief explains in detail why the FTC does not have the authority to sanction businesses for data-security breaches under Section 5 of the FTC Act. *See* Wyndham Br. 18-35. As Wyndham explains, a data-security breach that harms a business cannot form the basis of an "unfair" business practice, and nothing in Section 5 suggests that Congress intended to give the FTC the authority to regulate general data security. Multiple other laws grant the Commission the authority to regulate data security *in certain, limited contexts*—laws that would have been entirely unnecessary if Congress already had given the Commission the broad Section 5 authority to regulate data security it now claims it has.[4] Indeed, for over a decade the FTC repeatedly has lobbied for legislation providing it with rulemaking authority under the Administrative Procedure Act (APA) in the area of general data security, thus far to no avail. *See, e.g., Data Security: Hearing Before the H. Comm. on Energy & Commerce,*

[4] Congress has explicitly authorized the FTC to oversee and enforce data-security standards for certain industries and situations. *See, e.g.*, Wyndham Br. 24-25 (citing FTC's data-security authority under, among other statutes, the Fair Credit Reporting Act and the Gramm-Leach-Bliley Act).

*Subcomm. on Commerce, Mfg., & Trade*, 112th Cong. 11 (June 15, 2011) (prepared statement of FTC) [hereinafter *FTC 2011 Data Security Testimony*][5] (supporting draft legislation that would provide FTC with APA rulemaking authority); FTC, *Privacy Online: Fair Information Practices in the Electronic Marketplace* 36-37 (May 2000)[6] (recommending that Congress enact legislation requiring commercial websites to "take reasonable steps to protect the security of the information they collect from consumers" and to "provide an implementing agency with the authority to promulgate more detailed standards pursuant to the Administrative Procedure Act").

The FTC's enforcement actions in fact harken back to past attempts to extend its authority beyond proper bounds—attempts that resulted in Congress's adoption of a statutory test constraining the FTC's unfairness enforcement authority. Congress granted the FTC the authority to prohibit "unfair or deceptive acts or practices" in 1938, but the Commission rarely wielded the "unfairness" aspect of its authority until 1972, when, in a dictum, the Supreme Court cited with apparent approval a little-used FTC test for unfairness. J. Howard Beales, III, *The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection*, 22 J. of Pub. Pol'y & Mktg. 192, 193 (2003) (citing *FTC v. Sperry & Hutchinson Co. (S&H)*,

[5] http://www.ftc.gov/os/testimony/110615datasecurityhouse.pdf.

[6] http://www.ftc.gov/reports/privacy2000/privacy2000.pdf.

405 U.S. 233, 244 & n.5 (1972)). Under this old test, the FTC considered three factors when determining whether business conduct was "unfair" to consumers: (1) whether the conduct "offend[ed] public policy"; (2) whether it was "immoral, unethical, oppressive, or unscrupulous"; and (3) whether it "cause[d] substantial injury to consumers." *S&H*, 405 U.S. at 244 n.5 (reversing FTC decision for failure to articulate standards of conduct to address proven consumer injury).

Armed with that Supreme Court dictum, the FTC embarked on an ambitious campaign of using its Section 5 unfairness authority to police business practices that met *any* of these three loose and wide-ranging criteria. In 1978, for example, the Commission issued a report proposing to ban all television advertising to children as "immoral, unscrupulous, and unethical." Beales, 22 J. of Pub. Pol'y & Mktg. at 193. Following a series of similarly expansive policy positions, a political backlash ensued, culminating in Congress holding hearings to investigate the FTC's deployment of its unfairness authority. *See* Michael D. Scott, *The FTC, the Unfairness Doctrine, and Data Security Breach Litigation: Has the Commission Gone Too Far?*, 60 Admin. L. Rev. 127, 137 (2008).

In 1994, Congress enacted the FTC Amendments Act of 1994, Pub. L. No. 103-312, § 9, 108 Stat. 1691, 1695, which established a new 15 U.S.C. § 45(n), codifying a narrower view of the FTC's authority under Section 5 than the one first articulated in the wake of the congressional hearings. Section 45(n) provides:

> The Commission shall have no authority under this section or section 57a of this title to declare unlawful an act or practice on the grounds that such act or practice is unfair *unless* [i] the act or practice causes or is likely to cause substantial injury to consumers [ii] which is not reasonably avoidable by consumers themselves and [iii] 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. [15 U.S.C. § 45(n) (emphasis added).][7]

Despite these acknowledged statutory constraints, carefully calibrated by Congress in response to years of agency overreaching, the FTC again is attempting to use Section 5 inappropriately. The FTC in this case seeks to impose liability on Wyndham for failure to implement "reasonable and appropriate" security measures. But liability under Section 5 attaches only when an act *itself* is injurious to consumers. *See FTC v. Neovi, Inc.*, 604 F.3d 1150, 1157 (9th Cir. 2010). So, for example, a business violates Section 5 if it "ha[s] reason to believe" that its actions will cause substantial consumer injury, or when it "facilitate[s] and provide[s] substantial assistance" to a scheme that causes injury. *See id.* at 1156-

[7] Section 45(n) of the FTC Act was based in turn on an FTC Policy Statement, *FTC Policy Statement on Unfairness* (Dec. 17, 1980), *appended to Int'l Harvester Co.*, 104 F.T.C. 949, 1070 (1984), which sharply departed from the Commission's earlier expansive reading of its unfairness authority. Among other things, the Policy Statement concluded that the third *S&H* factor—consumer injury—was the most important, lessening the ability of the FTC to take public policy concerns, without more, into account when pursuing unfairness enforcement actions. *Id.* at 1073.

57.[8] An attack that first *victimizes the business itself* cannot be considered "unfair" to consumers.[9] Disregarding these constraints and assigning liability to good corporate citizens like Wyndham for a data-security breach impermissibly stretches the bounds of Section 5.

Instead of following established precedent, the FTC is using its Section 5 unfairness authority to pursue solely its policy prerogatives—something Congress expressly rejected in 15 U.S.C. § 45(n) when it instructed that "public policy considerations may not serve as a primary basis for such determination." Although the Commission surely has the best of intentions, it cannot exercise its unfairness authority in a manner inconsistent with its legislative mandate. *See FDA v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120, 125 (2000).

---

[8] For example, the FTC in the past has obtained injunctions under Section 5 prohibiting defendants from engaging in "phishing" identity-theft scams, through which defendants sent emails designed to obtain consumers' financial information under false pretenses and used that information to pay for goods or services without the consumers' consent. *See, e.g.*, *FTC v. Hill*, CV No. H-03-5537 (S.D. Tex. May 18, 2004). It is a long, illogical leap for the FTC to equate Wyndham's victimization at the hands of criminal hackers with a business affirmatively engaging in a criminal enterprise (a phishing scam).

[9] In addition, as Wyndham correctly observes, the FTC has failed to demonstrate that consumer injury from payment card data theft is substantial and not avoidable. *See* Wyndham Br. 45-50.

## II. BUSINESSES CANNOT OPERATE EFFECTIVELY AND EFFICIENTLY IN AN "EVOLVING ENFORCEMENT" REGIME.

Unfettered by the statutory restraints on its enforcement authority, the FTC has now begun to exert its will in the data-security area by entering into and publishing a series of consent orders settling charges against businesses under Section 5 for failing to employ what the Commission considers "reasonable and appropriate" measures to protect personal information against unauthorized access. The FTC negotiates, enters into, and publishes most of these agreements before it even files a complaint, subsequently claiming that the data-security "standards" it announces in conjunction with the consent orders are legal requirements under Section 5. This piecemeal "regulation by consent order" has enabled the FTC to impose unilaterally its evolving policy choices on businesses without the oversight of the legislative branch, without participation of the corporate community and other interested stakeholders, and without judicial review. *Cf. Sackett v. EPA*, 132 S. Ct. 1367, 1374 (2012) (rejecting notion that an agency should be permitted to "strong-arm[] . . . parties into 'voluntary compliance' without the opportunity for judicial review").

By way of comparison, the National Institute of Standards and Technology (NIST)—a federal agency with deep experience in the complex technical standards, guidelines, and best practices related to data security—recently engaged in a yearlong, multi-stakeholder effort to develop a framework to guide and

enhance efforts to reduce data-security risks to critical infrastructure. NIST, *Framework for Improving Critical Infrastructure Cybersecurity Version 1.0* (Feb. 12, 2014).[10] The lengthy, transparent, and collaborative effort used to produce and vet the NIST cybersecurity framework stands in stark contrast to the FTC's backwards-looking, opaque approach to enforcing self-defined data-security standards one consent order at a time.

The FTC's post-hoc manner of regulating cybersecurity not only inappropriately circumvents the legislative and judicial processes, it also gives *no* advance notice to businesses on what they are required to do to comply with the law in a rapidly changing technological environment. FTC complaints and consent orders premised on businesses not maintaining "reasonable," "appropriate," "adequate," or "proper" data-security measures are ambiguous and can (and do) constantly change. Kenneth A. Bamberger & Dierdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 Stan. L. Rev. 247, 291 (2011) ("The reasonableness standard is fluid, evolving, and open to constant reinterpretation."); *see also* Gerard Stegmaier & Wendell Bartnick, *Another Round in the Chamber: FTC Data Security Requirements and the Fair Notice Doctrine*, 17 No. 5 J. Internet L. 1, 24-28 (2013) (identifying problems with FTC Section 5 enforcement actions under

[10] http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.

fair notice doctrine). The fact that security standards are changing in response to evolving threats does not justify holding businesses to a nebulous notion of "reasonableness." Businesses can and do regularly comply with rules-based data-security standards issued by private-sector organizations, so it is not unreasonable to insist that such rules be formalized through legislation or rulemaking before finding a business in violation of the law.[11]

For example, in many cases the FTC will announce a violation of Section 5 based on a set of data-security practices that, "taken together," allegedly failed to provide reasonable and appropriate security measures. *See, e.g.*, Complaint, *In re Dave & Buster's*, FTC File No. 082 3153, at 2 (May 20, 2010).[12] Where this occurs, it is unclear whether the FTC would consider each of the offending practices to constitute a distinct Section 5 violation, or if not, what combinations of practices the FTC would deem to constitute an unfair practice in the future. And companies have no way of finding out. The absence of clear standards thus enables the Commission to use 20/20 hindsight—"you were breached, therefore your security must have been inadequate"—when evaluating data breaches.

---

[11] For example, in order to accept payment cards from the major card brands, businesses must comply with the strict Payment Card Industry Data Security Standard (PCI DSS) subject to verified compliance audits on an annual basis. *See* PCI Standards Security Council, *Payment Card Industry Security Standards Overview* (2008), https://www.pcisecuritystandards.org/pdfs/pcissc_overview.pdf.

[12] http://www.ftc.gov/os/caselist/0823153/100608davebusterscmpt.pdf.

The FTC expressly encourages businesses to follow and adopt the data-security practices announced in its consent orders. *See Consumer Online Privacy: Hearing Before the S. Comm. on Commerce, Sci., & Transp.*, 111th Cong. 9 (July 27, 2010) (prepared statement of FTC)[13] (testimony of FTC Chairman Jon Leibowitz that "[t]he Commission's robust enforcement actions have sent a strong signal to industry about the importance of data security, while providing guidance about how to accomplish this goal"); Lesley Fair, Sr. Staff Att'y, FTC Bureau of Consumer Prot., *Widgets, Whatzits, and Whaddayacallems,* Business Center Blog (Aug. 30, 2011, 10:44AM)[14] (encouraging businesses to interpret its Section 5 fiats broadly: "[S]avvy marketers of widgets pay attention to FTC cases involving whatzits and whaddaycallems . . . it's wise to look at the big picture—and not just at legal developments directly affecting your business"). But discerning any consistent standards from these consent orders is futile because the FTC's definition of what data-security principles are "unreasonable" depends on the business it is investigating. Indeed, the FTC has recognized that what data-security measures it considers "reasonable . . . will depend on the size and complexity of the business, and the sensitivity of the information at issue." *The Data Security and Breach Notification Act of 2010: Hearing on S. 3742 Before the Subcomm. on*

[13] http://www.ftc.gov/os/testimony/ 100727consumerprivacy.pdf.

[14] http://business.ftc.gov/blog/2011/08/widgets-whatzits-and-whaddayacallems

*Consumer Prot., Prod. Safety, & Ins. of the S. Comm. On Commerce, Sci., & Transp.*, 111th Cong. 7 n.22 (Sept. 22, 2010) (prepared statement of FTC).[15] Piecemeal, context-specific consent orders against other businesses cannot provide general guidance.

The FTC's regulation by consent order has a particularly pernicious impact on small businesses. Because they have no way of knowing in advance what the FTC considers commercially "reasonable" data-security measures, many small businesses must divert scarce resources away from addressing cybersecurity breaches to retaining legal counsel in anticipation of and response to potential FTC investigations and enforcement actions. Many other small businesses lack the resources to retain legal counsel, which gives the FTC additional leverage to compel so-called voluntary submission to consent decrees. Not surprisingly, a significant number of the FTC's data-security consent decrees have been with small and independent businesses. *See* FTC Bureau of Consumer Prot., Legal Resources, http://business.ftc.gov/legal-resources/29/35 (last visited October 14, 2014). In addition to imposing exorbitant costs, the FTC's regulatory approach shifts the attention of small business personnel away from managing and growing their businesses to responding to intrusive FTC investigations. *See, e.g.*, Amy

[15] http://www.ftc.gov/os/testimony/100922datasecuritytestimony.pdf.

Wenk, *Atlanta Medical Lab Facing off Against FTC*, Atl. Bus. Chron., Sept. 7, 2012.[16]

Complying with consent orders also is onerous. In just about all of its data-security consent orders, the FTC has insisted on periods of supervision of *twenty years*, during which the target company must provide independent audit results and other reports indicating its compliance with the FTC's security principles. *See, e.g.*, Consent Decree and Order for Civil Penalties, Injunction, and Other Relief, *United States v. RockYou, Inc.*, No. 12-CV-1487 (N.D. Cal. Mar. 28, 2012).[17] If the FTC later determines that a company subject to a consent order is not in compliance with a "new" data-security principle, the company is subject to civil penalties of up to $16,000 per violation. *See* 15 U.S.C. § 45(*l*), *as modified by* 16 C.F.R. § 1.98(c). Essentially, a company subject to an FTC consent order can never know if it is compliant with the order until the FTC says it is not.

The FTC does have limited discretion to develop the contours of the unfairness doctrine through the adjudicative process. But courts have long recognized that failure to apply limiting principles to unfairness under Section 5 would permit the FTC "to substitute its own business judgment" for that of

[16] http://www.bizjournals.com/atlanta/print-edition/2012/09/07/atlanta-medical-lab-facing-off-against.html?page=all.

[17] http://ftc.gov/os/caselist/1023120/120327rockyouorder.pdf.

companies, *Official Airline Guides, Inc. v. FTC*, 630 F.2d 920, 927 (2d Cir. 1980), and "blur the distinction between guilty and innocent commercial behavior." *Boise Cascade Corp. v. FTC*, 637 F.2d, 573, 580-82 (9th Cir. 1980). Without well-defined standards for determining whether conduct is "unfair" under Section 5, "the door would be open to arbitrary or capricious administration of § 5," resulting in "a state of complete unpredictability." *E.I. du Pont de Nemours & Co. v. FTC*, 729 F.2d 128, 138-39 (2d Cir. 1984). And it is in this "state of complete unpredictability" that the FTC now operates with substantial, unchecked power, raising significant due process concerns. *See FCC v. FOX Television Stations*, 132 S. Ct. 2307, 2317 (2012) ("A fundamental principle in our legal system is that laws which regulate persons or entities must give fair notice of conduct that is forbidden or required.").

The Commission's actions investigating, testifying about, and providing public guidance on companies' data-security obligations under the FTC Act do not give it authority over the field. If that were the case, any administrative agency could exercise authority over a subject matter on its own accord simply by making public statements about it. That is not how it works. Administrative agencies are permitted to act only with, and within, the authorization of Congress. Importuning Congress to permit them to act is not the same.

The FTC's recent attempt to regulate by consent order likewise contradicts U.S. Supreme Court precedent and the FTC's own opinions. *See Altria Group, Inc. v. Good*, 555 U.S. 70, 89 n.13 (2008) (stating that an FTC "consent order is in any event only binding on the parties to the agreement"); *United States v. E. I. du Pont de Nemours & Co*., 366 U.S. 316, 330 n.12 (1961) ("The circumstances surrounding . . . negotiated [consent orders] are so different that they cannot be persuasively cited in a litigation context."); *In re Chrysler Corp.*, 87 F.T.C. 719, 742 n.12 (1976) (ALJ decision 1975, adopted as modified by full Commission 1976); *see also In re Trans Union Corp.*, 118 F.T.C. 821, 864 n.18 (1994) (noting that a "consent agreement [with one party] is binding only between the Commission and [that party]"). Congress also emphasized the uniqueness of consent orders in its revision to the FTC Act by excluding them as precedent for "civil penalties." 15 U.S.C. § 45(m)(1)(B). It is thus inappropriate for the FTC to use consent orders to establish industry-wide standards.

## III. DATA-SECURITY POLICY CANNOT BE DEVELOPED THROUGH UNILATERAL PRONOUNCEMENT BY THE FTC, WITHOUT REGARD FOR THE LEGISLATIVE PROCESS.

In 2011, the Commission entered into consent orders with three resellers of credit reports for allegedly "unreasonable" data-security measures. *See* Press Release, FTC, *Credit Report Resellers Settle FTC Charges; Security Failures*

*Allowed Hackers to Access Consumers' Personal Information* (Feb. 3, 2011).[18] These were the first-ever Section 5 data-security enforcement actions in which the FTC held a company responsible for its *users'* data-security failures. Four FTC Commissioners acknowledged that fact in a rare statement issued along with the consent orders:

> [W]e are also cognizant of the fact that these are the first cases in which the Commission has held resellers responsible for downstream data protection failures. Looking forward, the actions we announce today should put resellers—indeed, all of those in the chain of handling consumer data—on notice of the seriousness with which we view their legal obligations to proactively protect consumers' data. The Commission should use all of the tools at its disposal to protect consumers from the enormous risks posed by security breaches that may lead to identity theft.

Revised Statement of Commissioner Brill, In Which Chairman Leibowitz and Commissioners Rosch and Ramirez Join, *In re Settlement One Credit Corp.*, *ACRAnet, Inc., and Fajilan & Assocs.*, FTC File Nos. 082 3208, 098 3088, 092 3089 (Aug. 15, 2011).[19] This statement is emblematic of the FTC's "shoot first, ask questions later" ad-hoc approach to regulating data security, with the Commission admitting that it enforces standards against businesses *without any prior notice*. The FTC may have thought that it was being magnanimous to *future* businesses by informing them of the standard "[l]ooking forward"; in reality, it was

[18] http://www.ftc.gov/opa/2011/02/settlement.shtm.

[19] http://www.ftc.gov/os/2011/08/110819settlementonestatement.pdf.

holding the respondents in this case responsible to a standard that they did not know existed. And that will happen each and every time the FTC enforces a new element of its evolving data-security policy.

There is, of course, a *right* way to establish consistent and transparent data-security standards: through a dialogue with all involved stakeholders, accomplished through democratically accountable means, not just by agency fiat. At the same time the Commission is wielding "all of the tools at its disposal"—and then some—to enforce its own data-security prerogatives against individual companies, policymakers, businesses, consumer advocacy groups, and other interested entities—including *amici*—are engaging in a serious debate over how to craft data-security policy in the United States. The dialogue among these many groups, including the Chamber and the Commission, includes not only the protection of consumer information but also the overall functioning of the nation's digitally enabled critical infrastructures and the appropriate mix of policies to encourage and support adoption of security measures in the face of rapidly evolving threats. *See generally* U.S. Chamber of Commerce, *U.S. Chamber Policy Priorities for 2014* at 20-21 (Sept. 2014)[20] (describing cybersecurity policy initiatives, including "[e]nact[ing] cybersecurity information-sharing legislation

[20] https://www.uschamber.com/sites/default/files/2014_policy_priorities-september_2014.pdf.

that includes robust safeguards for businesses that voluntarily exchange threat data with their peers and government partners"); Cong. Res. Serv., *Federal Laws Relating to Cybersecurity: Overview and Discussion of Proposed Revisions* (June 20, 2013)[21] (analyzing proposed cybersecurity legislation); *FTC 2011 Data Security Testimony* (advocating for data-security legislation).

As Wyndham points out, a number of data-security bills were recently introduced in Congress, including bills that would have given the FTC rulemaking authority over consumer data security. None were enacted. *See* Wyndham Br. 29-30. Instead of focusing its policy efforts on Congress, however, the FTC has engaged in backdoor regulation by consent orders without having to answer to Congress or the courts.

Furthermore, the FTC has neglected to effectuate its policy goals through Section 18 rulemaking. Under Section 18 of the FTC Act, the Commission is authorized to prescribe "rules which define with specificity acts or practices which are unfair" in violation of Section 5. 15 U.S.C. § 57a. By congressional design, this rulemaking authority is more burdensome on the FTC than rulemaking authority normally provided to administrative agencies under the APA; among other restrictions, for example, the statute permits interested parties to cross-examine witnesses. But the FTC has *never attempted to issue data-security rules*

[21] https://www.fas.org/sgp/crs/natsec/R42114.pdf.

*in this manner*. Instead, the Commission has eschewed this rulemaking procedure as too cumbersome to promulgate data-security rules, instead advocating for less-burdensome rulemaking authority under the APA. *See FTC 2011 Data Security Testimony* at 11 (supporting provision in draft legislation granting APA rulemaking authority to FTC in lieu of Section 18 rulemaking authority because "effective consumer protection requires that the Commission be able to promulgate these rules in a more timely and efficient manner").

By sidestepping both the legislative and authorized administrative methods for advancing its policy goals, the FTC is in violation of its congressional mandate. Instead of respecting the legislative process and the proper means for seeking and receiving express authority to regulate in the general data-security space, the FTC, much as it did in the late 1970s, has breached the boundaries of its Section 5 unfairness authority by engaging improperly in *ultra vires* regulation by consent order.

* * *

*Amici* acknowledge the importance of data security and, more broadly, cybersecurity, in today's digitally connected world. Businesses have every incentive to move to protect their digital assets in this dynamic technological environment. And government has an important role to play as well, both in protecting governmental operations and in partnering with industry to provide fair,

transparent, and consistent legal frameworks that companies can efficiently assess and apply in a rapidly changing environment.

The FTC historically has had an important, statutorily mandated role to play in protecting consumers. But its attempt to expand its current unfairness enforcement power to the technically complex and dynamic risk-management practices of businesses in almost every sector has stretched its statutory authority beyond the breaking point.

## CONCLUSION

For the foregoing reasons, the District Court's order denying Wyndham's motion to dismiss the "unfair" practices count of the Amended Complaint should be reversed.

Respectfully submitted,

s/ Catherine E. Stetson
CATHERINE E. STETSON
HARRIET P. PEARSON
BRET S. COHEN
SEAN MAROTTA
ADAM A. COOKE
HOGAN LOVELLS US LLP
555 Thirteenth Street, N.W.
Washington, D.C. 20004
(202) 637-5600

Counsel for *Amici Curiae*

KATE COMERFORD TODD
STEVEN P. LEHOTSKY
SHELDON GILBERT
U.S. CHAMBER LITIGATION CENTER, INC.
1615 H Street, N.W.
Washington, D.C. 20062
(202) 463-5337

Counsel for *Amicus Curiae* Chamber of Commerce of the United States of America

BANKS BROWN
MCDERMOTT WILL & EMERY LLP
340 Madison Ave.
New York, NY 10713
(212) 547-5488

Counsel for *Amicus Curiae* American Hotel & Lodging Association

KAREN R. HARNED
NATIONAL FEDERATION OF INDEPENDENT BUSINESS SMALL BUSINESS LEGAL CENTER
1201 F Street, N.W., Suite 200
Washington, D.C. 20004
(202) 314-2048

Counsel for *Amicus Curiae* National Federation of Independent Business

## CERTIFICATE OF COMPLIANCE

1. This brief complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because it contains 5,365 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii).

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because it has been prepared in a proportionally spaced typeface using Microsoft Office Word 2010 in Times New Roman 14-point font.

3. This brief complies with 3d Cir. Local App. R. 31.1(c) because the text of the electronic brief is identical to the text in the paper copies.

/s/ Catherine E. Stetson
CATHERINE E. STETSON
HOGAN LOVELLS US LLP
555 Thirteenth Street, N.W.
Washington, D.C. 20004
(202) 637-5600

Counsel for *Amici Curiae*

## CERTIFICATE OF BAR MEMBERSHIP

Pursuant to 3d Cir. Local App. R. 28.3(d) and 46.1(e), I hereby certify that I am a member in good standing of the bar of the United States Court of Appeals for the Third Circuit.

/s/ Catherine E. Stetson
CATHERINE E. STETSON
HOGAN LOVELLS US LLP
555 Thirteenth Street, N.W.
Washington, D.C. 20004
(202) 637-5600

Counsel for *Amici Curiae*

## CERTIFICATE OF VIRUS DETECTION

Pursuant to 3d Cir. Local App. R. 31.1(c), I hereby certify that I have run Symantec Endpoint Protection Version 12.1.4013.4013 on this file. No virus was detected.

/s/ Catherine E. Stetson
CATHERINE E. STETSON
HOGAN LOVELLS US LLP
555 Thirteenth Street, N.W.
Washington, D.C. 20004
(202) 637-5600

Counsel for *Amici Curiae*

## CERTIFICATE OF SERVICE

I hereby certify that on October 14, 2014, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system, which will send notification of such filing to all registered users of the CM/ECF system.

/s/ Catherine E. Stetson
CATHERINE E. STETSON
HOGAN LOVELLS US LLP
555 Thirteenth Street, N.W.
Washington, D.C. 20004
(202) 637-5600

Counsel for *Amici Curiae*