

1 David A. Selden, SBN 007499
The Cavanagh Law Firm, P.A.
2 1850 North Central Avenue, Suite 2400
Phoenix, Arizona 85004
3 dselden@cavanaghlaw.com
Phone: (602) 322-4009
4 Fax: (602) 322-4101

5 *Attorneys for Amici Curiae Chamber*
of Commerce of the United States of
6 *America, Retail Litigation Center, and*
American Hotel & Lodging Association

7
8 **IN THE UNITED STATES DISTRICT COURT**
9 **FOR THE DISTRICT OF ARIZONA**

10 Federal Trade Commission,

Case No. CV 12-1365-PHX PGR

11 Plaintiff,

12 v.

13 Wyndham Worldwide Corporation, et al.

14 Defendants.

15
16 **LODGED: PROPOSED "BRIEF OF AMICI CURIAE CHAMBER OF**
17 **COMMERCE OF THE UNITED STATES OF AMERICA, RETAIL LITIGATION**
18 **CENTER, AND AMERICAN HOTEL & LODGING ASSOCIATION IN**
19 **SUPPORT OF DEFENDANTS" ATTACHED.**
20
21
22
23
24
25
26
27
28

1 David A. Selden, SBN 007499
The Cavanagh Law Firm, P.A.
2 1850 North Central Avenue, Suite 2400
Phoenix, Arizona 85004
3 dselden@cavanaghlaw.com
Phone: (602) 322-4009
4 Fax: (602) 322-4101

5 *Attorneys for Amici Curiae Chamber*
of Commerce of the United States of
6 *America, Retail Litigation Center, and*
7 *American Hotel & Lodging Association*

8 **IN THE UNITED STATES DISTRICT COURT**
9 **FOR THE DISTRICT OF ARIZONA**

10 Federal Trade Commission,

11 Plaintiff,

12 v.

13 Wyndham Worldwide Corporation, et al.

14 Defendants.

Case No. CV 12-1365-PHX PGR

**BRIEF OF AMICI CURIAE
CHAMBER OF COMMERCE
OF THE UNITED STATES OF
AMERICA, RETAIL LITIGATION
& LODGING ASSOCIATION IN
SUPPORT OF DEFENDANTS**

15 **Of Counsel**

16 Catherine E. Stetson
17 J. Robert Robertson
Harriet P. Pearson
18 Bret S. Cohen
Hogan Lovells US LLP
19 555 Thirteenth Street, N.W.
Washington, D.C. 20004
20 cate.stetson@hoganlovells.com
robby.robertson@hoganlovells.com
21 harriet.pearson@hoganlovells.com
bret.cohen@hoganlovells.com
22 Phone: (202) 637-5600
Fax: (202) 637-5910
23 *Counsel for Amici Curiae*

24 Banks Brown
McDermott Will & Emery LLP
25 340 Madison Ave.
New York, NY 10713
26 Phone: (212) 547-5488
Fax: (646) 383-6105
27 *Counsel for Amicus Curiae American*
Hotel & Lodging Association

Deborah R. White
Retail Litigation Center
1700 N. Moore Street, Suite 2250
Arlington, VA 22209
deborah.white@rila.org
Phone: (703) 600-2067
Fax: (703) 841-1184
Counsel for Amicus Curiae Retail
Litigation Center

Robin S. Conrad
Sheldon Gilbert
National Chamber Litigation Center, Inc.
1615 H Street, N.W.
Washington, D.C. 20062
RConrad@USChamber.com
SGilbert@USChamber.com
Phone: (202) 463-5337
Fax: (202) 463-5346
Counsel for Amicus Curiae Chamber of
Commerce of the United States of America

1 **TABLE OF CONTENTS**

2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

Page

TABLE OF AUTHORITIES ii

INTEREST OF *AMICI CURIAE* 1

INTRODUCTION..... 2

ARGUMENT 4

I. THE FTC’S SECTION 5 AUTHORITY TO PROHIBIT UNFAIR
TRADE PRACTICES DOES NOT GIVE THE FTC AUTHORITY TO
ESTABLISH GENERAL DATA SECURITY POLICY 4

II. BUSINESSES CANNOT OPERATE EFFECTIVELY AND
EFFICIENTLY IN AN “EVOLVING ENFORCEMENT” REGIME 7

III. DATA SECURITY POLICY CANNOT BE DEVELOPED THROUGH
UNILATERAL PRONOUNCEMENT BY THE FTC, WITHOUT
REGARD FOR THE LEGISLATIVE PROCESS 12

CONCLUSION 15

CERTIFICATE OF SERVICE 17

TABLE OF AUTHORITIES

	Page(s)
1	
2	
3	CASES:
4	<i>Altria Group, Inc. v. Good,</i>
5	555 U.S. 70 (2008)..... 11
6	<i>Boise Cascade Corp. v. FTC,</i>
7	637 F.2d (9th Cir. 1980)1
8	<i>E.I. du Pont de Nemours & Co. v. FTC,</i>
9	729 F.2d 128 (2d Cir. 1984).....11
10	<i>FCC v. FOX Television Stations,</i>
11	132 S. Ct. 2307 (2012)..... 11
12	<i>FDA v. Brown & Williamson Tobacco Corp.,</i>
13	529 U.S. 120 (2000)7
14	<i>FTC v. Hill,</i>
15	CV No. H-03-5537 (S.D. Tex. May 18, 2004) 7
16	<i>FTC v. Neovi, Inc.,</i>
17	604 F.3d 1150 (9th Cir. 2010)6
18	<i>FTC v. Sperry & Hutchinson Co. (S&H),</i>
19	405 U.S. 233 (1972)5
20	<i>In re Chrysler Corp.,</i>
21	87 F.T.C. 719 (1976)..... 11
22	<i>In re Dave & Buster's,</i>
23	FTC File No. 082 3153 (2010)8, 9
24	<i>In re Trans Union Corp.,</i>
25	118 F.T.C. 821 (1994)..... 11, 12
26	<i>Official Airline Guides, Inc. v. FTC,</i>
27	630 F.2d 920 (2d Cir. 1980).....10
28	<i>Sackett v. EPA,</i>
	132 S. Ct. 1367 (2012)..... 8
	<i>United States v. E.I. du Pont de Nemours & Co.,</i>
	366 U.S. 316 (1961)..... 11

1	<i>United States v. RockYou, Inc.</i> , No. 12-CV-1487	
2	(N.D. Cal. Mar. 28, 2012).....	10
3	STATUTES:	
4	15 U.S.C. § 45, Section 5 of the Federal Trade Commission Act.....	<i>passim</i>
5	15 U.S.C. § 45(l), as modified by 16 C.F.R. § 1.98(c).....	10
6	15 U.S.C. § 45(m)(1)(B).....	12
7	15 U.S.C. § 45(n).....	6, 7
8	15 U.S.C. § 57a.....	14
9	OTHER AUTHORITIES:	
10	Cong. Res. Serv., <i>Federal Laws Relating to Cybersecurity:</i>	
11	<i>Discussion of Proposed Revisions</i> (June 29, 2012)	13
12	<i>Consumer Online Privacy: Hearing Before the S. Comm. on Commerce, Sci., &</i>	
13	<i>Transp.</i> , 111th Cong. (July 27, 2010)	9
14	FTC, <i>Credit Report Resellers Settle FTC Charges; Security Failures Allowed</i>	
15	<i>Hackers to Access Consumers’ Personal Information</i> (Feb. 3, 2011)	12
16	<i>Data Security: Hearing Before the H. Comm on Energy & Commerce, Subcomm.</i>	
17	<i>on Commerce, Mfg., & Trade</i> , 112th Cong. (June 15, 2011)	4, 13, 14
18	FTC Policy Statement on Unfairness (Dec. 17, 1980), appended to	
19	<i>Int’l Harvester Co.</i> , 104 F.T.C. 949 (1984).....	6
20	FTC, <i>Privacy Online: Fair Information Practices in the Electronic Marketplace</i>	
21	(May 2000).....	5
22	J. Howard Beales, III, <i>The FTC’s Use of Unfairness Authority: Its Rise,</i>	
23	<i>Fall, and Resurrection</i> , 22 J. of Pub. Pol’y & Mktg. 192 (2003).....	5, 6
24	Joint Ass’n Letter to Senate Regarding Amendments to S. 3414 (July 27, 2012).....	13
25	Kenneth A. Bamberger & Dierdre K. Mulligan, <i>Privacy on the Books and</i>	
26	<i>on the Ground</i> , 63 Stan. L. Rev. 247 (2011).....	8
27	Lesley Fair, Sr. Staff Attorney, FTC Bureau of Consumer Protection,	
28	<i>Widgets, Whatzits, and Whaddayacallems</i> , Business Center Blog	
	(Aug. 30, 2011).....	9

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

Michael D. Scott, *The FTC, the Unfairness Doctrine, and Data Security Breach Litigation: Has the Commission Gone Too Far?*,
60 Admin. L. Rev. 127 (2008).....6

PCI Standards Security Council, *Payment Card Industry Security Standards Overview* (2008)..... 8

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) 12

The Data Security and Breach Notification Act of 2010: Hearing on S. 3742 Before the Subcomm. on Consumer Prot., Prod. Safety, & Ins. of the S. Comm. On Commerce, Sci., & Transp., 111th Cong. (Sept. 22, 2010) 10

1 **BRIEF OF AMICI CURIAE CHAMBER OF COMMERCE OF THE UNITED**
2 **STATES OF AMERICA, RETAIL LITIGATION CENTER, AND AMERICAN**
3 **HOTEL & LODGING ASSOCIATION IN SUPPORT OF DEFENDANTS**

4 The Chamber of Commerce of the United States of America (the "Chamber"), the
5 Retail Litigation Center ("RLC"), and the American Hotel & Lodging Association
6 ("AH&LA") submit this brief as *amici curiae* in support of Defendant Wyndham Hotels
7 & Resorts LLC ("Wyndham")’s Motion to Dismiss.

8 **INTEREST OF AMICI CURIAE**

9 The Chamber of Commerce of the United States of America is a nonprofit
10 corporation and the world’s largest business federation. The Chamber represents 300,000
11 direct members and indirectly an underlying membership of more than three million
12 companies and professional organizations of every size, in every industry sector, and
13 from every region of the country. The Chamber represents the interests of its members in
14 matters before Congress, the Executive Branch, and the courts. To that end, the Chamber
15 regularly files *amicus curiae* briefs in cases raising issues of vital concern to the nation’s
16 business community.

17 The RLC is a public policy organization that identifies and engages in legal
18 proceedings that affect the retail industry. The RLC’s members include many of the
19 country’s largest and most innovative retailers. The member entities whose interests the
20 RLC represents employ millions of people throughout the United States, provide goods
21 and services to tens of millions more, and account for tens of billions of dollars in annual
22 sales. The RLC seeks to provide courts with retail-industry perspectives on important
23 legal issues, and to highlight the potential industry-wide consequences of significant
24 pending cases.

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

1 Electronic data is the pulse of American business. The companies represented by
2 the Chamber, RLC, and AH&LA use electronic data, including personal data, to enhance
3 business efficiency and to benefit consumers. For the modern company, personal and
4 other types of digitized data are essential for a multitude of reasons, including
5 administering employee benefits programs, processing payment and shipping
6 information, and enabling customer loyalty programs, among many other uses. *Amici* all
7 have a significant interest in explaining to the Court the legal and policy implications of
8 accepting the Federal Trade Commission ("FTC" or "Commission")’s arguments, and
9 assisting the Court with resolving the claims pending before it.

10 **INTRODUCTION**

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

17 The FTC has strayed down the same path again. Over the course of the past
18 decade, the FTC has departed from the statutory underpinnings of Section 5 unfairness,
19 leveraging its enforcement authority to extract settlements from businesses that
20 themselves have been victimized by data security breaches, and that have no formal
21 notice of the standards that the FTC accuses them of violating. By statute, the FTC has
22 an important role to play in protecting America’s consumers. However, the agency’s
23 “unfairness” authority does not permit it to set and enforce – whether through litigation or
24 consent orders¹ – general data-security policy.

25
26 ¹ Often when the FTC claims that a data-security breach constitutes an “unfair”
27 trade practice, the Commission has been able to obtain Section 5 consent orders from the
28 targeted businesses. This case is among the first data-security “unfairness” proceedings
to be evaluated by a court.

1 Indeed, the FTC expressly has acknowledged that Congress has not granted it the
2 general authority to regulate data security; after all, that is why the Commission currently
3 is lobbying for additional rulemaking authority. The FTC should not be permitted to
4 circumvent the full legislative process by establishing rules and principles through private
5 enforcement actions, resulting in a string of consent orders that the FTC publishes and
6 which it holds out to other businesses as if they were established law.

7 This incremental – and unilateral – regulation-through-settlement subjects
8 American businesses to vague, unknowable, and constantly changing data-security
9 standards. Companies often are unaware of the standards to which they are held until
10 after they receive a notice of investigation from the FTC, at which point they must settle
11 or expend considerable resources fighting the agency. The *in terrorem* effect of a notice
12 by itself thus is significant. The FTC’s arsenal of enforcement capabilities carries a real
13 risk of affecting business judgment, slowing the adoption of new technologies, and
14 chilling business from sharing information about breaches to avert malicious attacks in
15 the future.

16 Permitting the FTC to proceed on a theory that suffering a data breach is an
17 “unfair” trade practice would expose every business in America to the potential for a
18 government enforcement action whenever that business suffers a cyber-attack or other
19 incident that potentially compromises personal data. Congress did not envision that
20 result when it passed legislation limiting the FTC’s Section 5 unfairness authority, and
21 this Court should not countenance it.

22 The businesses represented by *amici* take seriously their responsibility to
23 safeguard all personally identifying electronic information. But it is a stark reality that
24 bad actors target business technology to obtain valuable data, including personal data and
25 intellectual property. No data security is perfect, and breaches do occur, exposing digital
26 information. But when criminals accessed Wyndham’s business computer systems, the
27 FTC sought court redress not against the thieves, but against the business that was
28

1 victimized by them, contending in Count II of its complaint that Wyndham’s data-security
2 policy was an “unfair,” and therefore unlawful, trade practice.

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

7 Defendant Wyndham's Motion to Dismiss should be granted.

8 **ARGUMENT**

9 **I. THE FTC’S SECTION 5 AUTHORITY TO PROHIBIT UNFAIR TRADE**
10 **PRACTICES DOES NOT GIVE THE FTC AUTHORITY TO ESTABLISH**
11 **GENERAL DATA SECURITY POLICY.**

12 Defendant Wyndham’s Motion to Dismiss [Dkt. #32] explains in detail why the
13 FTC does not have the authority to sanction businesses for data security breaches under
14 Section 5 of the FTC Act. [See Dkt. # 32, Wyndham Mot. 6-10]. As Wyndham explains,
15 nothing in Section 5 suggests that Congress intended to give the FTC the authority to
16 regulate data security. Multiple other laws grant the Commission the authority to
17 regulate data security *in certain, limited contexts* – something that would have been
18 entirely unnecessary if Congress already had given the Commission the broad Section 5
19 authority to regulate data security it now claims it has.² Indeed, even the FTC itself does
20 not argue that Congress has expressly authorized the Commission to regulate the data-
21 security practices of private companies. [See Dkt. #46, FTC Opp. to Wyndham Mot. 6].
22 And for good reason: for over a decade, the FTC repeatedly has lobbied for legislation
23 providing it with rulemaking authority under the Administrative Procedure Act (APA) in
24 the area of general data security, thus far to no avail. *See, e.g., Data Security: Hearing*
25 *Before the H. Comm on Energy & Commerce, Subcomm. on Commerce, Mfg., & Trade,*
26 *112th Cong. 11 (June 15, 2011) (prepared statement of FTC) [hereinafter *FTC 2011 Data**

27 ² Congress has explicitly authorized the FTC to oversee and enforce data-security
28 standards for certain industries and situations. [See, e.g., Dkt. # 32, Wyndham Mot. 7-8]
(citing FTC’s data-security authority under, among other statutes, the Fair Credit
Reporting Act, Gramm-Leach-Bliley Act, and Children’s Online Privacy Protection Act).

1 *Security Testimony*]³ (supporting draft legislation that would provide FTC with APA
2 rulemaking authority); FTC, *Privacy Online: Fair Information Practices in the*
3 *Electronic Marketplace* 36-37 (May 2000)⁴ (recommending that Congress enact
4 legislation requiring commercial websites to “take reasonable steps to protect the security
5 of the information they collect from consumers” and to “provide an implementing agency
6 with the authority to promulgate more detailed standards pursuant to the Administrative
7 Procedure Act”).

8 The FTC’s enforcement actions in fact harken back to past attempts to extend its
9 authority beyond proper bounds – attempts that resulted in Congress’s adoption of a
10 statutory test constraining the FTC’s unfairness enforcement authority. Congress granted
11 the FTC the authority to prohibit “unfair or deceptive acts or practices” in 1938, but the
12 Commission rarely wielded the “unfairness” aspect of its authority until 1972, when, in
13 dicta, the Supreme Court cited with apparent approval a little-used FTC test for
14 unfairness. J. Howard Beales, III, *The FTC’s Use of Unfairness Authority: Its Rise, Fall,*
15 *and Resurrection*, 22 J. of Pub. Pol’y & Mktg. 192, 193 (2003) (citing *FTC v. Sperry &*
16 *Hutchinson Co. (S&H)*, 405 U.S. 233, 244 & n.5 (1972)). Under this old test, the FTC
17 considered three factors when determining whether business conduct was “unfair” to
18 consumers: (1) whether the conduct “offend[ed] public policy”; (2) whether it was
19 “immoral, unethical, oppressive, or unscrupulous”; and (3) whether it “cause[d]
20 substantial injury to consumers.” *S&H*, 405 U.S. at 244 n.5 (reversing FTC decision for
21 failure to articulate standards of conduct to address proven consumer injury).

22 Armed with that Supreme Court dicta, the FTC embarked on an ambitious
23 campaign of using its Section 5 unfairness authority to police business practices that met
24 *any* of these three loose and wide-ranging criteria. In 1978, for example, the Commission
25 issued a report proposing to ban all television advertising to children as “immoral,

26 ³ Available at <http://www.ftc.gov/os/testimony/110615datasecurityhouse.pdf> (last
27 visited Oct. 5, 2012).

28 ⁴ Available at <http://www.ftc.gov/reports/privacy2000/privacy2000.pdf> (last visited
Oct. 5, 2012).

1 unscrupulous, and unethical.” Beales, 22 J. of Pub. Poly’ & Mktg. at 193. Following a
2 series of similar overreaching policy positions, a political backlash ensued, culminating
3 in Congress holding hearings to investigate the FTC’s deployment of its unfairness
4 authority. See Michael D. Scott, *The FTC, the Unfairness Doctrine, and Data Security*
5 *Breach Litigation: Has the Commission Gone Too Far?* 60 Admin. L. Rev. 127, 137
6 (2008).

7 In 1994, Congress adopted 15 U.S.C. § 45(n), which codified a narrower view of
8 the FTC’s Section 5 authority first articulated in the wake of the Congressional hearings.
9 Section 45(n) provides:

10 The Commission shall have no authority under this section or section 57a
11 of this title to declare unlawful an act or practice on the grounds that such
12 act or practice is unfair *unless* [i] the act or practice causes or is likely to
13 cause substantial injury to consumers [ii] which is not reasonably
14 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 [15 U.S.C. § 45(n) (emphasis added).]⁵

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

24 ⁵ Section 45(n) of the FTC Act was based in turn on an FTC Policy Statement, *FTC*
25 *Policy Statement on Unfairness* (Dec. 17, 1980), *appended to Int’l Harvester Co.*, 104
26 F.T.C. 949, 1070 (1984), which sharply departed from the Commission’s earlier
27 expansive reading of its unfairness authority. Among other things, the Policy Statement
28 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.

1 *See id.* at 1156-57.⁶ An attack that primarily *victimizes the business itself* cannot be
2 considered “unfair” to consumers.⁷ Disregarding these constraints and assigning liability
3 to good corporate citizens for a data-security breach impermissibly stretches the bounds
4 of Section 5.

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

12 **II. BUSINESSES CANNOT OPERATE EFFECTIVELY AND EFFICIENTLY**
13 **IN AN “EVOLVING ENFORCEMENT” REGIME.**

14 Unfettered by the statutory restraints on its enforcement authority, the FTC has
15 now begun to exert its will in the data-security area by entering into and publishing a
16 series of consent orders settling charges against businesses under Section 5 for failing to
17 employ what the Commission considers “reasonable and appropriate” measures to protect
18 personal information against unauthorized access. The FTC negotiates, enters into, and
19 publishes most of these agreements before it even files a complaint, subsequently
20 claiming that the data security “standards” it announces in conjunction with the consent
21 orders are legal requirements under Section 5. This piecemeal “regulation by consent
22 order” has enabled the FTC to impose unilaterally its evolving policy choices on

23 ⁶ For example, the FTC in the past has obtained injunctions under its Section 5
24 unfairness authority prohibiting defendants from engaging in “phishing” identity-theft
25 scams, through which the defendants sent emails designed to obtain consumers’ financial
26 information under false pretenses and used that information to pay for goods or services
27 without the consumers’ consent. *See, e.g., FTC v. Hill*, CV No. H-03-5537 (S.D. Tex.
28 May 18, 2004). It is a long, illogical leap for the FTC to equate Wyndham’s victimization
at the hands of a criminal hacker with a criminal enterprise’s phishing scam.

⁷ In addition, as Wyndham correctly observes, consumer injury from payment card
data theft is “always avoidable and never substantial.” [Dkt. #32, Wyndham Mot. 12].

1 businesses without the oversight of the legislative branch, without participation of the
2 corporate community and other interested stakeholders, and without judicial review. *Cf.*
3 *Sackett v. EPA*, 132 S. Ct. 1367, 1374 (2012) (rejecting notion that an agency should be
4 permitted to “strong-arm[] . . . parties into ‘voluntary compliance’ without the
5 opportunity for judicial review”).

6 Regulating in this manner not only inappropriately circumvents the legislative and
7 judicial processes; it also gives *no* advance notice to businesses on what they are required
8 to do to comply with the law in a rapidly changing technological environment. FTC
9 complaints and consent orders premised on businesses not maintaining “reasonable,”
10 “appropriate,” “adequate,” or “proper” data security measures are ambiguous and can
11 (and do) constantly change. Kenneth A. Bamberger & Dierdre K. Mulligan, *Privacy on*
12 *the Books and on the Ground*, 63 *Stan. L. Rev.* 247, 291 (2011) (“The reasonableness
13 standard is fluid, evolving, and open to constant reinterpretation.”). The FTC, however,
14 rejects the commonsense idea of setting forth “particularized guidelines” for businesses
15 to follow, reasoning that doing so would be impossible because “[d]ata security industry
16 standards are continually changing in response to evolving threats and new
17 vulnerabilities.” [Dkt. #46, FTC Opp. to Wyndham Mot. 12]. But it is *precisely because*
18 the appropriate standards are difficult to ascertain that businesses cannot be held to a
19 nebulous notion of “reasonableness,” all without any formal guidance before they find
20 themselves in violation of the law.⁸

21 For example, in many cases, the FTC will announce a violation of Section 5 based
22 on a set of data security practices that, “taken together,” allegedly failed to provide
23 reasonable and appropriate security measures. *See, e.g.,* Complaint, *In re Dave &*
24

25 ⁸ The FTC’s position is further belied by the fact that in order to accept payment cards
26 from the major card brands, businesses must comply with the strict Payment Card Industry
27 Data Security Standard (PCI DSS) subject to verified compliance audits on an annual basis.
28 *See* PCI Standards Security Council, *Payment Card Industry Security Standards Overview*
(2008), https://www.pcisecuritystandards.org/pdfs/pcissc_overview.pdf (last visited Oct. 5,
2012).

1 *Buster's*, FTC File No. 082 3153, at 2 (2010).⁹ Where this occurs, it is unclear whether
2 the FTC would consider each of the offending practices to constitute a distinct Section 5
3 violation, or if not, what combinations of practices the FTC would deem to constitute an
4 unfair practice in the future. And companies have no way of finding out. The absence of
5 clear standards thus enables the Commission to use 20/20 hindsight – “you were
6 breached, therefore your security must have been inadequate” – when evaluating data
7 breaches.

8 The FTC expressly encourages businesses to follow and adopt the data-security
9 practices announced in its consent orders. *See Consumer Online Privacy: Hearing*
10 *Before the S. Comm. on Commerce, Sci., & Transp.*, 111th Cong. 9 (July 27, 2010)
11 (prepared statement of FTC)¹⁰ (testimony of FTC Chairman Jon Leibowitz that “[t]he
12 Commission’s robust enforcement actions have sent a strong signal to industry about the
13 importance of data security, while providing guidance about how to accomplish this
14 goal”); Lesley Fair, Sr. Staff Att’y, FTC Bureau of Consumer Prot., *Widgets, Whatzits,*
15 *and Whaddayacallems*, Business Center Blog (Aug. 30, 2011),
16 <http://business.ftc.gov/blog/2011/08/widgets-whatzits-and-whaddayacallems> (last visited
17 Oct. 5, 2012) (encouraging businesses to interpret its Section 5 fiats broadly: “[S]avvy
18 marketers of widgets pay attention to FTC cases involving whatzits and whaddayacallems
19 . . . it’s wise to look at the big picture – and not just at legal developments directly
20 affecting your business.”). But discerning any consistent standards from these consent
21 orders is futile because the FTC’s definition of what data security principles are
22 “unreasonable” depends on the business it is investigating. Indeed, by the FTC’s own
23 admission, it does not issue general data-security rules in part because “industries and
24 businesses have a variety of network structures that store or transfer different types of
25 data, and reasonable network security will reflect the likelihood that such information

26 ⁹ Available at <http://www.ftc.gov/os/caselist/0823153/100608davebusterscmpt.pdf>
27 (last visited Oct. 5, 2012).

28 ¹⁰ Available at <http://www.ftc.gov/os/testimony/100727consumerprivacy.pdf> (last
visited Oct. 5, 2012).

1 will be targeted and, if so, the likelihood of attack.” [See Dkt. #46, FTC Opp. to
2 Wyndham Mot. 12]; see also *The Data Security and Breach Notification Act of 2010:*
3 *Hearing on S. 3742 Before the Subcomm. on Consumer Prot., Prod. Safety, & Ins. of the*
4 *S. Comm. On Commerce, Sci., & Transp.*, 111th Cong. 7 n.22 (Sept. 22, 2010) (prepared
5 statement of FTC)¹¹ (“The Commission recognizes that what [data security measures it
6 considers] reasonable . . . will depend on the size and complexity of the business, the
7 nature and scope of its activities, and the sensitivity of the information at issue.”).
8 Piecemeal, context-specific consent orders against other businesses cannot provide
9 general guidance.

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

21 The FTC does have limited discretion to develop the contours of the unfairness
22 doctrine through the adjudicative process. But courts have long recognized that failure to
23 apply limiting principles to unfairness under Section 5 would permit the FTC “to
24 substitute its own business judgment” for that of companies, *Official Airline Guides, Inc.*
25 *v. FTC*, 630 F.2d 920, 927 (2d Cir. 1980), and “blur the distinction between guilty and

26 ¹¹ Available at <http://www.ftc.gov/os/testimony/100922datasecuritytestimony.pdf>
27 (last visited Oct. 5, 2012).

28 ¹² Available at <http://ftc.gov/os/caselist/1023120/120327rockyouorder.pdf> (last visited
Oct. 5, 2012).

1 innocent commercial behavior.” *Boise Cascade Corp. v. FTC*, 637 F.2d, 573, 580-82
2 (9th Cir. 1980). Without well-defined standards for determining whether conduct is
3 “unfair” under Section 5, “the door would be open to arbitrary or capricious
4 administration of § 5,” resulting in “a state of complete unpredictability.” *E.I. du Pont de*
5 *Nemours & Co. v. FTC*, 729 F.2d 128, 138-39 (2d Cir. 1984). And it is in this “state of
6 complete unpredictability” that the FTC now operates with substantial, unchecked power,
7 raising significant due process concerns. *See FCC v. FOX Television Stations*, 132 S. Ct.
8 2307, 2317 (2012) (“A fundamental principle in our legal system is that laws which
9 regulate persons or entities must give fair notice of conduct that is forbidden or
10 required.”).

11 The Commission weakly addresses this legal requirement, claiming that its
12 Section 5 data security enforcement against Wyndham “is not moving in a new direction”
13 because it “has been investigating, testifying about, and providing public guidance on
14 companies’ data security obligations under the FTC Act for more than a decade.”
15 [Dkt. #46, FTC Opp. to Wyndham Mot. 13]. That argument implies that any
16 administrative agency can exercise authority over a subject matter on its own accord
17 simply by making public statements about it. That is not how it works. Administrative
18 agencies are permitted to act only with, and within, the authorization of Congress.
19 Importuning Congress to permit them to act is not the same.

20 The FTC’s recent attempt to regulate by consent order likewise contradicts U.S.
21 Supreme Court precedent and the FTC’s own opinions. *See Altria Group, Inc. v. Good*,
22 555 U.S. 70, 89 n.13 (2008) (stating that an FTC “consent order is in any event only
23 binding on the parties to the agreement”); *United States v. E. I. du Pont de Nemours &*
24 *Co.*, 366 U.S. 316, 330 n.12 (1961) (“The circumstances surrounding . . . negotiated
25 [consent orders] are so different that they cannot be persuasively cited in a litigation
26 context.”); *In re Chrysler Corp.*, 87 F.T.C. 719, 742 n.12 (1976) (ALJ decision 1975,
27 adopted as modified by full Commission 1976); *see also In re Trans Union Corp.*, 118
28 F.T.C. 821, 864 n.18 (1994) (noting that a “consent agreement [with one party] is binding

1 only between the Commission and [that party]”). Congress also emphasized the
2 uniqueness of consent orders in its revision to the FTC Act by excluding them as
3 precedent for “civil penalties.” 15 U.S.C. § 45(m)(1)(B). It is thus inappropriate for the
4 FTC to use consent orders to establish industry-wide standards.

5 **III. DATA SECURITY POLICY CANNOT BE DEVELOPED THROUGH**
6 **UNILATERAL PRONOUNCEMENT BY THE FTC, WITHOUT REGARD**
7 **FOR THE LEGISLATIVE PROCESS.**

8 Last year, the Commission entered into consent orders with three resellers of
9 credit reports for allegedly “unreasonable” data security measures. See Press Release,
10 FTC, *Credit Report Resellers Settle FTC Charges; Security Failures Allowed Hackers to*
11 *Access Consumers’ Personal Information* (Feb. 3, 2011).¹³ These were the first-ever
12 Section 5 data-security enforcement actions in which the FTC held a company
13 responsible for its *users’* data-security failures. Four FTC Commissioners acknowledged
14 that fact in a rare statement issued along with the consent orders:

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

23 Revised Statement of Commissioner Brill, In Which Chairman Leibowitz and
24 Commissioners Rosch and Ramirez Join, *In re Settlement One Credit Corp., ACRAnet,*
25 *Inc., and Fajilan & Assocs.*, FTC File Nos. 082 3208, 098 3088, 092 3089 (Aug. 15,
26 2011).¹⁴ This statement is emblematic of the FTC’s “shoot first, ask questions later” ad-
27 hoc approach to regulating data security, with the Commission admitting that it enforces
28 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 holding the respondents in this case responsible to

¹³ Available at <http://www.ftc.gov/opa/2011/02/settlement.shtm> (last visited Oct. 5, 2012).

¹⁴ Available at <http://www.ftc.gov/os/2011/08/110819settlementonestatement.pdf> (last visited Oct. 5, 2012).

1 a standard that they did not know existed. And that will happen each and every time the
2 FTC enforces a new element of its evolving data-security policy.

3 There is, of course, a *right* way to establish consistent and transparent data-
4 security standards: through a dialogue with all involved stakeholders, accomplished
5 through democratically accountable means, not just by agency fiat. At the same time the
6 Commission is wielding “all of the tools at its disposal” – and then some – to enforce its
7 own data-security prerogatives against individual companies, policymakers, businesses,
8 consumer advocacy groups, and other interested entities – including *amici* – are engaging
9 in a serious debate over how to craft data security policy in the United States. The
10 dialogue among these many groups, including the Chamber and the Commission,
11 includes not only the protection of consumer information but also the overall functioning
12 of the nation’s digitally enabled critical infrastructures. *See generally* Joint Ass’n Letter
13 to Senate Regarding Amendments to S. 3414 (July 27, 2012)¹⁵ (advocating for delay in
14 consideration of “vitaly important” data security bill because “work is still needed as
15 disagreement persists regarding certain provisions of a federal bill”); Cong. Res. Serv.,
16 *Federal Laws Relating to Cybersecurity: Discussion of Proposed Revisions* (June 29,
17 2012)¹⁶ (analyzing proposed cybersecurity legislation); *FTC 2011 Data Security*
18 *Testimony* (advocating for data security legislation). As Wyndham points out, a number
19 of bills were introduced in Congress in 2011 and 2012, including bills that would have
20 given the FTC rulemaking authority over general data security. None were enacted. [*See*
21 Dkt. #32, Wyndham Mot. 8-9]. Instead of focusing its policy efforts on Congress,
22 however, the FTC has engaged in backdoor rulemaking through its consent orders
23 without having to answer to Congress or the courts.

24
25 _____
26 ¹⁵ Available at [http://www.uschamber.com/sites/default/files/hill-](http://www.uschamber.com/sites/default/files/hill-letters/Joint%20Association%20Letter%20re%20Amdts%20to%20S%203414.pdf)
27 [letters/Joint%20Association%20Letter%20re%20Amdts%20to%20S%203414.pdf](http://www.uschamber.com/sites/default/files/hill-letters/Joint%20Association%20Letter%20re%20Amdts%20to%20S%203414.pdf) (last
28 visited Oct. 5, 2012).

¹⁶ Available at <https://www.fas.org/sgp/crs/natsec/R42114.pdf> (last visited Oct. 5,
2012).

1 The FTC failed to effectuate its policy goals through Section 18 rulemaking.
2 Under Section 18 of the FTC Act, the Commission is authorized to prescribe “rules
3 which define with specificity acts or practices which are unfair” in violation of Section 5.
4 15 U.S.C. § 57a. By Congressional design, this rulemaking authority is more
5 burdensome on the FTC than rulemaking authority normally provided to administrative
6 agencies under the APA; among other restrictions, for example, the statute permits
7 interested parties to cross-examine witnesses. But the FTC has *never attempted to issue*
8 *data-security rules in this manner*. Instead, the Commission has eschewed this
9 rulemaking procedure as too cumbersome to promulgate data-security rules, instead
10 advocating for less-burdensome rulemaking authority under the APA. *See FTC 2011*
11 *Data Security Testimony* at 11 (supporting provision in draft legislation granting APA
12 rulemaking authority to FTC in lieu of Section 18 rulemaking authority because
13 “effective consumer protection requires that the Commission be able to promulgate these
14 rules in a more timely and efficient manner”). Issuing prescriptive data-security
15 requirements outside of the context of these established rulemaking procedures further
16 demonstrates that the FTC is not interested in pursuing constitutionally and legislatively
17 required channels, in line with how it proceeded over thirty years ago.

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

24 * * *

25 *Amici* acknowledge the importance of data security and, more broadly,
26 cybersecurity, in today’s digitally connected world. Businesses have every incentive to
27 move to protect their digital assets in this dynamic technological environment. And
28 government has an important role to play as well, both in protecting governmental

1 operation and in partnering with industry to provide fair, transparent, and consistent legal
2 frameworks that companies can efficiently assess and apply in a rapidly changing
3 environment.

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

8 **CONCLUSION**

9 For these reasons, and for those stated in Wyndham's Motion to Dismiss, the
10 Motion should be granted.

11 RESPECTFULLY SUBMITTED this 5th day of October, 2012.

12 THE CAVANAGH LAW FIRM, P.A.

13
14 By: s/David A. Selden
15 David A. Selden
16 1850 North Central Avenue, Suite 2400
17 Phoenix, AZ 85004
dselden@cavanaghlaw.com
18 Phone: (602) 322-4009
19 Fax: (602) 322-4101
20 *Attorneys for Amici Curiae*

21 **Of Counsel:**

22 Catherine E. Stetson
23 J. Robert Robertson
24 Harriet P. Pearson
25 Bret S. Cohen
26 Hogan Lovells US LLP
27 555 Thirteenth Street, N.W.
28 Washington, D.C. 20004
cate.stetson@hoganlovells.com
robby.robertson@hoganlovells.com
harriet.pearson@hoganlovells.com
bret.cohen@hoganlovells.com
Phone: (202) 637-5600
Fax: (202) 637-5910
Counsel for Amici Curiae

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

Robin S. Conrad
Sheldon Gilbert
Chamber of Commerce of the
United States of America
1615 H Street, N.W.
Washington, D.C. 20062
RConrad@USChamber.com
SGilbert@USChamber.com
Phone: (202) 463-5337
Fax: (202) 463-5346
*Counsel for Amicus Curiae Chamber of
Commerce of the United States of America*

Deborah R. White
Retail Litigation Center
1700 N. Moore Street, Suite 2250
Arlington, VA 22209
deborah.white@rila.org
Phone: (703) 600-2067
Fax: (703) 841-1184
*Counsel for Amicus Curiae Retail Litigation
Center*

Banks Brown
McDermott Will & Emery LLP
340 Madison Ave.
New York, NY 10713
Phone: (212) 547-5488
Fax: (646) 383-6105
*Counsel for Amicus Curiae American Hotel &
Lodging Association*

1 **CERTIFICATE OF SERVICE**

2 I hereby certify that on October 5, 2012, I electronically transmitted the attached
3 document to the Clerk's Office using the CM/ECF System for filing and transmittal of a
4 Notice of Electronic Filing to the following CM/ECF registrants:

5 Andrea Vanina Arias
aarias@ftc.gov
6 John Andrew Krebs
jkrebs@ftc.gov
7 Jonathan Eli Zimmerman
zimmerman1@ftc.gov
8 Katherine E. McCarron
kmccarron@ftc.gov
9 Kevin H. Moriarty
kmoriarty@ftc.gov
10 Kristin Krause Cohen
kcohen@ftc.gov
11 Lisa Naomi Weintraub Schifferle
lschifferle@ftc.gov
12 Federal Trade Commission - Washington, DC
600 Pennsylvania Ave. NW
13 Washington, DC 20580
Attorneys for Plaintiff

14 David B. Rosenbaum
drosenbaum@omlaw.com
15 Anne M. Chapman
achapman@omlaw.com
16 Osborn Maledon, P.A.
17 2929 North Central Avenue, Suite 2100
Phoenix, Arizona 85012-2794
18 *Attorneys for Defendants*

19 Eugene F. Assaf, P.C. (*Pro Hac Vice*)
eugene.assaf@kirkland.com
20 K. Winn Allen, 1000590 (*Pro Hac Vice*)
winn.allen@kirkland.com
21 Kirkland & Ellis LLP
22 655 Fifteenth Street, N.W.
Washington, D.C. 20005
Attorneys for Defendants

23 Douglas H. Meal (*Pro Hac Vice*)
douglas.meal@ropesgray.com
24 Ropes & Gray, LLP
25 Prudential Tower
26 800 Boylston Street
Boston, MA 02199-3600
Attorneys for Defendants

27
28 s/Michele Maul

Lodged Proposed Document

[2:12-cv-01365-PGR Federal
Trade Commission v. Wyndham
Worldwide Corporation et al](#)

PROTO,STD

**U.S. District Court
DISTRICT OF ARIZONA**

Notice of Electronic Filing

The following transaction was entered by Selden, David on 10/5/2012 at 7:47 PM MST and filed on 10/5/2012

Case Name: Federal Trade Commission v. Wyndham Worldwide Corporation et al

Case Number: [2:12-cv-01365-PGR](#)

Filer: Chamber of Commerce of the United States

Document Number: [58](#)

Docket Text:

LODGED Proposed BRIEF AMICI CURIAE re: [32] MOTION to Dismiss Case . Document to be filed by Clerk if Motion to Leave to File or Amend is granted. Filed by Chamber of Commerce of the United States. (Selden, David)

2:12-cv-01365-PGR Notice has been electronically mailed to:

Andrea Vanina Arias aarias@ftc.gov, damodeo@ftc.gov

Anne Michelle Chapman achapman@omlaw.com, jgreenwood@omlaw.com

David A Selden dselden@cavanaghlaw.com, mmaul@cavanaghlaw.com

David B Rosenbaum drosenbaum@omlaw.com, kdourlein@omlaw.com

Douglas Harlan Meal douglas.meal@ropesgray.com, CourtAlert@ropesgray.com, nancy.loubier@ropesgray.com

Eugene F Assaf eugene.assaf@kirkland.com

Heather Zachary Heather.Zachary@wilmerhale.com

John Andrew Krebs jkrebs@ftc.gov

Jonathan Cedarbaum jonathan.cedarbaum@wilmerhale.com

Jonathan Eli Zimmerman jzimmerman1@ftc.gov

K Winn Allen winn.allen@kirkland.com

Katherine E McCarron kmccarron@ftc.gov

Kevin H Moriarty kmoriarty@ftc.gov, vaery@ftc.gov

Kristin Krause Cohen kcohen@ftc.gov

Lisa Naomi Weintraub Schifferle lschifferle@ftc.gov

Shiva Nagaraj shiva.nagaraj@wilmerhale.com

Steven P Lehotsky steven.lehotsky@wilmerhale.com

2:12-cv-01365-PGR Notice will be sent by other means to those listed below if they are affected by this filing:

The following document(s) are associated with this transaction:

Document description:Main Document

Original filename:n/a

Electronic document Stamp:

[STAMP dcecfStamp_ID=1096393563 [Date=10/5/2012] [FileNumber=9350431-0
] [6827253860f489499bd0f14335563c0e1126751fcb7fc89956aae68672cdb1276e5
c51cf2cb538a7014b7f0cdaf9e4cd0020 f4193cdce69041ea75e975221b54]]