

No. 14-3514

IN THE
United States Court of Appeals
FOR THE THIRD CIRCUIT

FEDERAL TRADE COMMISSION,

Plaintiff-Appellee,

v.

WYNDHAM HOTELS & RESORTS, LLC,

Defendant-Appellant.

On Appeal from the United States District Court
for the District of New Jersey
Case No. 13-cv-1887 (Hon. Esther Salas)

**BRIEF OF WASHINGTON LEGAL FOUNDATION AND
ALLIED EDUCATIONAL FOUNDATION
AS AMICI CURIAE IN SUPPORT OF
DEFENDANT-APPELLANT, URGING REVERSAL**

Cory L. Andrews
Richard A. Samp
WASHINGTON LEGAL
FOUNDATION
2009 Mass. Ave., N.W.
Washington, DC 20036
(202) 588-0302

Counsel for Amici Curiae

October 14, 2014

RULE 26.1 CORPORATE DISCLOSURE STATEMENTS

The Washington Legal Foundation (WLF) and the Allied Educational Foundation (AEF) are a non-profit, tax-exempt corporations organized under Section 501(c)(3) of the Internal Revenue Code. Neither WLF nor AEF has a parent corporation or issues stock, and no publicly held company has an ownership interest.

TABLE OF CONTENTS

TABLE OF AUTHORITIES	ii
IDENTITY AND INTERESTS OF <i>AMICI CURIAE</i>	1
STATEMENT OF THE CASE.....	2
SUMMARY OF ARGUMENT	5
ARGUMENT	8
I. The FTC’s Claim That Its § 5 Authority Extends to Data Security Lacks the Force of Law and Is Thus Undeserving of <i>Chevron</i> Deference	8
II. The FTC Failed to Provide Wyndham With Fair Notice of What § 5 Requires	16
CONCLUSION.....	21
COMBINED CERTIFICATIONS	
CERTIFICATE OF SERVICE	

TABLE OF AUTHORITIES

	Page(s)
CASES:	
<i>Alexander v. Sandoval</i> , 532 U.S. 275 (2001).....	1
<i>Altria Group, Inc. v. Good</i> , 555 U.S. 70 (2008).....	18
<i>Am. Farm Bureau Fed’n v. EPA</i> , No. 13-4079 (3d. Cir. dec. pending)	1
<i>Appalachian Power Co. v. EPA</i> , 208 F.3d 1015 (D.C. Cir. 2000)	6
<i>Beatrice Foods, Co. v. FTC</i> , 540 F.2d 303 (7th Cir. 1976)	19
<i>Boutilier v. INS</i> , 387 U.S. 118 (1967).....	16
<i>Bowen v. Georgetown Univ. Hosp.</i> , 488 U.S. 204 (1988).....	14
<i>Carter v. Welles-Bowen Realty, Co.</i> , 736 F.3d 722 (6th Cir. 2013)	13, 14
<i>Chevron U.S.A. Inc. v. Natural Res. Def. Council</i> , 467 U.S. 837 (1984).....	<i>passim</i>
<i>Christensen v. Harris Cnty.</i> , 529 U.S. 576 (2000).....	10, 13
<i>Christopher v. SmithKline Beecham Corp.</i> , 132 S. Ct. 2156 (2012).....	1, 17
<i>City of Arlington v. FCC</i> , 133 S. Ct. 1863 (2013).....	12, 15

	Page(s)
<i>Connally v. General Constr. Co.</i> , 269 U.S. 385 (1926).....	16
<i>Dravo Corp. v. Occupational Safety & Health Review Comm’n</i> , 613 F.2d 1227 (3d Cir. 1980).....	20
<i>E.I. du Pont de Nemours & Co. v. FTC</i> , 729 F.2d 128 (2d Cir. 1984).....	20
<i>FCC v. Fox Television Stations, Inc.</i> , 132 S. Ct. 2307 (2012).....	16, 18
<i>FDA v. Brown & Williamson Tobacco Corp.</i> , 529 U.S. 120 (2000).....	1
<i>Gen. Elec. Co. v. EPA</i> , 53 F.3d 1324 (D.C. Cir. 1995).....	16, 17
<i>Good Samaritan Hosp. v. Shalala</i> , 508 U.S. 402 (1993).....	9
<i>INS v. Cardoza-Fonseca</i> , 480 U.S. 421 (1987).....	9
<i>Lanzetta v. New Jersey</i> , 306 U.S. 451 (1939).....	16
<i>Nat’l Cable & Telecomm. Ass’n v. Brand X Internet Servs.</i> , 545 U.S. 967 (2005).....	10
<i>Pauley v. BethEnergy Mines</i> , 501 U.S. 680 (1991).....	9
<i>Pharm. Research & Mfrs. of Am. v. Thompson</i> , 362 F.3d 817 (D.C. Cir. 2004).....	1
<i>Sabetti v. DiPaolo</i> , 16 F.3d 16 (1st Cir. 1994).....	16

	Page(s)
<i>SEC v. Chenery Corp.</i> , 332 U.S. 194 (1947).....	19
<i>Skidmore v. Swift & Co.</i> , 323 U.S. 134 (1944).....	14
<i>United States v. Chrysler Corp.</i> , 158 F.3d 1350 (D.C. Cir. 1998)	21
<i>United States v. Mead Corp.</i> , 533 U.S. 218 (2001).....	10, 11, 12, 15
<i>Util. Air Regulatory Group v. EPA</i> , 134 S. Ct. 2427 (2014)	1
<i>Watt v. Alaska</i> , 451 U.S. 259, 273 (1981).....	9
<i>Wyeth v. Levine</i> , 555 U.S. 555 (2009).....	13
STATUTES:	
15 U.S.C. § 45.....	<i>passim</i>
15 U.S.C. § 45(a)	3
15 U.S.C. § 53(b)	3
28 U.S.C. § 1292(b)	5
OTHER AUTHORITIES:	
Jeffrey Benner, <i>FTC Powerless to Protect Privacy</i> , Wired, May 31, 2001	8
Federal Trade Commission, <i>Privacy Online: Fair Information Practices in the Electronic Marketplace</i> (2000)	8, 9

	Page(s)
Federal Trade Commission, <i>Protecting Personal Information: A Guide for Business</i> (2011).....	12, 20
Maureen K. Ohlhausen, <i>Remarks to the Sixth Annual Telecom Policy Conf.</i> (Mar. 18, 2014).....	18
<i>Prepared Statement of the FTC on Data Security: Hearing Before the H. Comm. On Energy & Commerce, 112th Cong.</i> (May 4, 2011)	9
M. Scott, <i>The FTC, The Unfairness Doctrine, and Data Security Breach Litigation: Has the Commission Gone too Far?</i> , 60 Admin. L. Rev. 127 (2008).....	9
Martin Shapiro, <i>Administrative Discretion: The Next Stage</i> , 92 Yale L.J. 1487 (1983)	5, 6
Patrick J. Smith, <i>Chevron Step Zero After City of Arlington</i> , 140 Tax Notes 713 (2013)	12
Gerard M. Stegmaier & Wendell Bartnick, <i>Psychics, Russian Roulette, & Data Security: The FTC's Hidden Data- Security Requirements</i> , 20 Geo. Mason L. Rev. 673 (2013)	17, 21

IDENTITY AND INTERESTS OF *AMICI CURIAE*¹

The Washington Legal Foundation (WLF) is a non-profit, public-interest law firm and policy center with supporters in all 50 States. WLF devotes a substantial portion of its resources to defending and promoting free enterprise, individual rights, a limited, accountable government, and the rule of law. To that end, WLF regularly appears as *amicus curiae* before this and other federal courts to ensure that federal agencies are not permitted to exercise powers that Congress cannot plausibly be understood to have granted them. *See, e.g., Util. Air Regulatory Group v. EPA*, 134 S. Ct. 2427 (2014); *FDA v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120 (2000); *Am. Farm Bureau Fed'n v. EPA*, No. 13-4079 (3d. Cir. dec. pending). In addition, WLF routinely litigates in regulatory cases to ensure that undue deference is not accorded to federal regulatory agencies. *See, e.g., Christopher v. SmithKline Beecham Corp.*, 132 S. Ct. 2156 (2012); *Alexander v. Sandoval*, 532 U.S. 275 (2001); *Pharm. Research & Mfrs. of Am. v. Thompson*, 362 F.3d 817 (D.C. Cir. 2004).

The Allied Educational Foundation (AEF) is a non-profit, charitable foundation based in Englewood, New Jersey. Founded in 1964, AEF is dedicated

¹ Pursuant to Federal Rule of Appellate Procedure 29(c), *amici* state that no counsel for any party authored this brief in whole or in part, and that no person or entity, other than *amici* and their counsel, made a monetary contribution intended to fund the preparation and submission of this brief. All parties have consented to the filing of this brief.

to promoting education in diverse areas of study, such as law and public policy, and has appeared as *amicus curiae* in this and other federal courts on a number of occasions.

Amici agree with Appellant that nothing in the text or history of § 5 of the FTC Act gives the FTC authority to decide whether certain data security protections are “unfair.” Indeed, Congress’s repeated enactment of specific data-security-protection statutes confirms that the FTC Act cannot be construed so broadly. *Amici* will not repeat those arguments here. Rather, *amici* write separately to refute any suggestion that the FTC’s latest interpretation of § 5, as reflected in consent decrees and an informal online brochure, is entitled to *Chevron* deference. *Amici* also write separately to emphasize that, even if Congress did grant the FTC the authority it claims, the FTC has failed to provide fair notice—to Appellant or the rest of the business community—of what the law requires.

STATEMENT OF THE CASE

Appellant Wyndham Hotels & Resorts, LLC (“Wyndham”) is a leading hospitality company headquartered in Parsippany, New Jersey. *See* Am. Compl.

¶ 9. Pursuant to franchise and management agreements, over 100 independently owned hotels operate under the Wyndham brand. *Id.* Under this arrangement, Wyndham maintains a computer network that includes a central reservation system to coordinate reservations for the Wyndham-branded hotels. *Id.* ¶ 16. To further

facilitate guest reservations, each Wyndham-branded hotel maintains its own separate computer network that is linked to the Wyndham network. *Id.* ¶ 15.

Between April 2008 and January 2010, on three separate occasions, cybercriminals operating from inside Russia hacked into Wyndham's computer network, as well as the separate computer networks of several Wyndham-branded hotels. *Id.* ¶ 25. By breaching the Wyndham-branded hotels' computer networks, these cybercriminals gained unauthorized access to hotel guests' payment-card data and other personal information. *Id.*

The FTC filed suit against Wyndham in U.S. District Court for the District of Arizona, alleging under Count I that Wyndham's online privacy policy, which stated that Wyndham had made "reasonable and appropriate efforts to protect personal information against unauthorized access," constituted a "deceptive" trade practice under § 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45(a). *Id.* ¶¶ 44, 45. Count II further alleged that because Wyndham's network security protocols were neither "reasonable" nor "appropriate" they constituted "unfair" trade practices under § 5(a). *Id.* ¶¶ 1, 47. The complaint asserted jurisdiction under § 13(b) of the FTC Act, 15 U.S.C. § 53(b), and the prayer for relief sought injunctive relief as well as restitution, refund, and disgorgement of allegedly ill-gotten monies. *Id.* Over the FTC's objection, Wyndham successfully moved to transfer the case to New Jersey, where Wyndham is headquartered.

Pursuant to Fed. R. Civ. P. 12(b)(6), Wyndham moved to dismiss count II of the complaint for failure to state a claim. (D. Ct. Dkt. No. 91-1). In its motion, Wyndham argued that the FTC lacked authority under § 5 to regulate corporate data security practices. *Id.* at 7-14. Wyndham pointed out, for example, that no court had ever held that § 5's prohibition against "unfair and deceptive" practices authorized the Agency to establish data security standards for the private sector. *Id.* at 1. Yet even if the FTC enjoyed such authority, Wyndham argued, the Agency had failed entirely to provide Wyndham with constitutionally sufficient notice of what data-security practices were acceptable under § 5. *Id.* at 14-19. For example, the FTC has never published any rules, regulations, or other formal guidance explaining what conduct § 5 requires or prohibits with regard to data security. *Id.* Rather, as Wyndham's motion explained, the FTC's exercise of § 5 authority in the area of data security has consisted almost entirely of a recent series of consent decrees with private parties and an online brochure. *Id.*

Following extensive briefing and oral argument by the parties, the district court denied Wyndham's motion to dismiss. (D. Ct. Dkt. No 182). While conceding that this litigation "undoubtedly raises a variety of thorny legal issues that Congress and the courts will continue to grapple with for the foreseeable future," Judge Salas refused to, in her words, "carve out a data-security exception to the FTC's unfairness authority." *Id.* at 6, 10. Dismissing as irrelevant the FTC's

own prior pronouncements to the contrary, the court concluded that the FTC's authority over data security is a permissible complement to Congress's current data-security regulatory scheme. *Id.* at 10-12. Judge Salas rejected any suggestion that principles of fair notice require the FTC to issue rules and regulations for data security before the agency can bring a civil action for alleged violations of § 5. *Id.* at 18-20. Rather, the court held that the "flexibility necessarily inherent in Section 5" provides the FTC with sufficient discretion to regulate the private sector by way of individual adjudications. *Id.* at 21-25.

Acknowledging the absence of precedent directly addressing the nationally significant questions of law presented in this case, the district court certified its order for interlocutory appeal under 28 U.S.C. § 1292(b). On July 3, 2014, Wyndham subsequently petitioned this Court for leave to appeal; the Court granted leave to appeal on July 29, 2014.

SUMMARY OF ARGUMENT

This case presents issues much broader than the fate of a single hospitality company and its efforts to prevent the FTC from improperly expanding its regulatory authority under § 5 of the FTC Act. The central challenge of administrative law over the past several decades has been to "narro[w] the category of actions considered to be so discretionary as to be exempted from review." Martin Shapiro, *Administrative Discretion: The Next Stage*, 92 Yale L.J. 1487,

1489 n.11 (1983). As the size of the administrative state continues to grow, it is more important than ever that agencies play by the rules, especially the rule of fair notice, and that stakeholders continue to have a meaningful opportunity to participate in the operation of their government. Courts have criticized the increasing use of agency-created legislative rules whereby “[l]aw is made, without notice and comment, without public participation, and without publication in the Federal Register or the Code of Federal Regulations.” *Appalachian Power Co. v. EPA*, 208 F.3d 1015, 1020 (D.C. Cir. 2000). This is just such a case.

The FTC is wrong to claim that its interpretation of the agency’s § 5 authority in prior consent decrees and an online guidance brochure are entitled to *Chevron* deference. The Supreme Court has clarified that the only agency guidance documents eligible for *Chevron* deference are those that Congress, by delegating rule-making authority to the agency, intended to have “the force of law.” *Chevron* deference thus comes into play only when an agency offers a binding interpretation of a statute it administers. As a result, only relatively formal agency documents promulgated with notice-and-comment rulemaking, such as regulations, are eligible for *Chevron* deference.

When the Supreme Court’s test for determining which agency guidance documents are eligible for deference under *Chevron* is applied to this case, it is clear that the FTC’s consent decrees and online brochure are not eligible for such

deference. The FTC's prior consent decrees and guidance brochure were not part of a formal adjudicatory process and do not contain a reasoned analysis of the FTC's interpretation of the law. Nor does the FTC even suggest that these documents have the same "force of law" as FTC regulations. Because the agency's interpretation was never the product of rigorous administrative rulemaking, no deference is warranted. At most, the FTC's litigating position is entitled to respect only to the extent that it is persuasive—nothing more.

Not only is the FTC's "catch-as-catch-can" approach to regulatory enforcement under § 5 deeply unfair to the business community, but it also falls far short of satisfying the legal standard for fair notice. The constitutional requirement that defendants be given fair notice of conduct that can subject them to punishment is deeply rooted in our legal system (and indeed in any system founded on respect for the rule of law) and applies to any defendant—criminal or civil—faced with liability at the hands of a government agency. The FTC's prior consent decrees entered into with third parties and an online brochure cannot substitute for agency rulemaking. By refusing to promulgate any rules or regulations for data security, the FTC deprives companies like Wyndham of "fair notice" of what conduct is forbidden or required under the FTC Act.

ARGUMENT

I. The FTC's Claim That Its § 5 Authority Extends to Data Security Lacks the Force of Law and Is Thus Undeserving of *Chevron* Deference

Section 5 of the FTC Act is altogether silent on the issue of data security. Before the district court's ruling below, no court had ever held that § 5's prohibition on "unfair and deceptive" practices gave the FTC authority to regulate data security. Although no specific statute grants the FTC authority to establish and enforce data security standards for the private sector, the FTC claims that such authority can be found in § 5's general prohibition on "unfair and deceptive" trade practices. Below, the FTC claimed that its expansive interpretation of § 5 of the FTC Act is entitled to binding deference under *Chevron U.S.A. Inc. v. Natural Res. Def. Council*, 467 U.S. 837 (1984). Not so.

As a preliminary matter, the FTC has on earlier occasions publicly disclaimed the very authority it now asserts in this case.² That is precisely why the FTC has repeatedly asked Congress to enact legislation expressly granting it

² In a May 2000 report, for example, the Commission flatly admitted that it "lack[ed] authority to require firms to adopt information practice policies or to abide by the fair information practice principles on their Web Sites, or portions of their Web sites." FTC, *Privacy Online: Fair Information Practices in the Electronic Marketplace*, at 34 (2000). As one FTC official has explained, "[t]he agency's jurisdiction is [over] deception The agency doesn't have the jurisdiction to enforce privacy." Jeffrey Benner, *FTC Powerless to Protect Privacy*, *Wired*, May 31, 2001 (quoting Lee Peeler, the FTC's former Associate Director of Advertising Practices).

authority over data security.³ When Congress refused to grant these repeated requests, the FTC “decided to move forward on its own without any new, specific privacy laws or delegation of authority from Congress.” M. Scott, *The FTC, The Unfairness Doctrine, and Data Security Breach Litigation: Has the Commission Gone too Far?*, 60 Admin. L. Rev. 127, 143 (2008).

The Supreme Court has recognized that “the consistency of an agency’s position is a factor in assessing the weight that position is due.” *Good Samaritan Hosp. v. Shalala*, 508 U.S. 402, 417 (1993). Where, as here, an “agency interpretation of a relevant provision . . . conflicts with the agency’s earlier interpretation,” the new interpretation “is ‘entitled to considerably less deference’ than a consistently held agency view.” *INS v. Cardoza-Fonseca*, 480 U.S. 421, 446 n.30 (1987)(quoting *Watt v. Alaska*, 451 U.S. 259, 273 (1981)); *see also Pauley v. BethEnergy Mines*, 501 U.S. 680, 698 (1991)(“[T]he case for judicial deference is less compelling with respect to agency positions that are inconsistent with

³ *See, e.g.,* FTC, *Privacy Online, supra*, at 36-37 (requesting that Congress “enact legislation to ensure adequate protection of consumer privacy online” by establishing “the basic standards of practice governing the collection of information online, and provid[ing] an implementing agency with the authority to promulgate more detailed standards pursuant to the [APA], including authority to enforce those standards”); *Prepared Statement of the FTC on Data Security: Hearing Before the H. Comm. On Energy & Commerce*, 112th Cong., at 11 (May 4, 2011)(“[T]he Commission reiterates its support for federal legislation that would (1) impose data security standards on companies and (2) require companies, in appropriate circumstances, to provide notification to consumers when there is a security breach.”).

previously held views.”).

Even if the FTC’s interpretation were consistent, the agency has not promulgated that interpretation in a binding way with the force of law. In *Chevron*, the Supreme Court held that “ambiguities in statutes within an agency’s jurisdiction to administer are delegations of authority to the agency to fill the statutory gap in reasonable fashion.” *Nat’l Cable & Telecomm. Ass’n v. Brand X Internet Servs.*, 545 U.S. 967, 980 (2005)(citing *Chevron*, 467 U.S. at 865-66). All agency interpretations, however, are not entitled to deference. In *United States v. Mead Corp.*, 533 U.S. 218 (2001), the Supreme Court clarified that an agency’s interpretation qualifies for deference only “when it appears that Congress delegated authority to the agency generally to make rules carrying the force of law, *and* that the agency interpretation claiming deference was promulgated in the exercise of that authority.” 533 U.S. at 226-27 (emphasis added); *see also Christensen v. Harris Cnty.*, 529 U.S. 576, 587-88 (2000).

Underlying *Mead*’s restriction on the reach of *Chevron* is that a court may defer to an agency’s interpretation of an ambiguous statute only when it is clear that Congress has granted the agency “the authority to promulgate binding legal rules.” *Brand X Internet Servs.*, 545 U.S. at 980-81; *see also Mead*, 533 U.S. at 230-31 & n.11. The procedures that Congress instructs an agency to use provide one good indication that such a delegation has in fact occurred. As *Mead*

emphasized, “[i]t is fair to assume generally that Congress contemplates administrative action with effect of law when it provides for a relatively formal administrative procedure.” 533 U.S. at 230.

Importantly, even an agency exercising its delegated interpretive authority must do so through administrative procedures designed to produce binding rules with the force of law. In *Mead*, for example, the Supreme Court observed that the Customs Service had a “general rulemaking power” by which it could make regulations with the force of law. *Id.* at 232. But the statutory interpretations contained in agency rulings promulgated outside that power were *not* entitled to deference. The Court found it “difficult . . . to see in the agency practice itself any indication that [the agency] ever set out with lawmaking pretense in mind” when it announced the interpretations. *Id.* at 233. The Court emphasized that those interpretations were not themselves subject to the rigors of notice and comment, were of limited precedential value, and were issued with little deliberation. *Id.* at 233-34.

In other words, administrative interpretations have the force of law (*i.e.*, are entitled to deference) only when they reflect “the fairness and deliberation that should underlie a pronouncement of such force.” *Id.* at 230. And while *Mead* left open the possibility that agency interpretations other than those promulgated by notice-and-comment rulemaking might be eligible for *Chevron* deference, *see, e.g.*,

533 U.S. at 227, that possibility appears to have been foreclosed altogether in *City of Arlington v. FCC*, 133 S. Ct. 1863, 1874 (2013) (“*Mead* denied *Chevron* deference to action, by an agency with rulemaking authority, that was not rulemaking.”; “It suffices to decide this case that the preconditions to deference under *Chevron* are satisfied because Congress has unambiguously vested the FCC with general authority to administer the Communications Act through rulemaking and adjudication, and the agency interpretation at issue was promulgated in the exercise of that authority.”). If anything, *City of Arlington* clarifies and reinforces *Mead*’s holding that an agency’s informal interpretations are undeserving of *Chevron* deference. See generally Patrick J. Smith, *Chevron Step Zero After City of Arlington*, 140 Tax Notes 713 (2013).

Chevron deference thus comes into play only when an agency offers a binding interpretation of a statute it administers. To date, the FTC has published no guidance or rulemaking in the Federal Register to explain what it deems to be the statutory basis of its authority over data security under § 5. Nor has the FTC published any policy statements setting forth its view of the agency’s authority to regulate the data-security practices of the private sector. Instead, the FTC relies solely on a collection of prior consent decrees it entered into with private parties and a business guidance brochure, *Protecting Personal Information: A Guide for Business* (2011), which appears on the agency’s website. But such consent decrees

and guidance brochures offer only non-binding advice about the FTC's enforcement agenda, not a controlling interpretation of the statute. "Agency recommendations of this sort, even when cast as policy considerations or preferences, do not bind courts tasked with interpreting a statute." *Carter v. Welles-Bowen Reality, Co.*, 736 F.3d 722, 726 (6th Cir. 2013).

Although a court may evaluate the fairness and deliberation with which an agency has rendered an interpretation—and, thereby, that interpretation's persuasive weight—from the procedures the agency employed, the Supreme Court has repeatedly emphasized that the inquiry does not end there: "Interpretations such as those in opinion letters—like interpretations contained in policy statements, agency manuals, and enforcement guidelines, all of which lack the force of law—do not warrant *Chevron*-style deference." *Christensen*, 529 U.S. at 587. Here, the FTC's sweeping claim to § 5 authority over data security—gleaned only from the FTC's prior consent decrees and informal business guidance brochure—squarely falls into this category of pronouncements that are unworthy of deference.

In *Wyeth v. Levine*, 555 U.S. 555 (2009), the Supreme Court considered whether to accord deference to FDA's interpretation of the scope of its own preemption authority. 555 U.S. at 576-581. Even though FDA provided for a notice of proposed rulemaking, it chose not to seek comment on the scope of

permissible preemption. *See id.* at 577. When FDA ultimately promulgated a final rule that “articulated a sweeping position on the [FDA’s] preemptive effect in the regulatory preamble,” the Court refused to give that preamble deference in light of FDA’s “procedural failure,” which made the agency’s interpretive pronouncements “inherently suspect.” *Id.* The same result should obtain here.

“The point of *Chevron* is to encourage agencies to *resolve* statutory ambiguities, not to create new uncertainties.” *Welles-Bowen*, 736 F.3d at 727 (emphasis in original). The FTC’s prior consent decrees and guidance brochure were not part of a formal adjudicatory process and do not contain a reasoned analysis of the FTC’s interpretation of the law. Such informal interpretations are entitled to nothing more than “respect” under this Court’s decision in *Skidmore v. Swift & Co.*, but only to the extent that those interpretations have the “power to persuade.” 323 U.S. 134, 140 (1944). And the FTC’s litigating position in this case (and in previous cases) is even less deserving of deference. *See Bowen v. Georgetown Univ. Hosp.*, 488 U.S. 204, 212-13 (1988)(“Deference to what appears to be nothing more than an agency’s convenient litigating position would be entirely inappropriate.”).

More fundamentally, allowing regulatory agencies to adopt new, expansive interpretations of statutes, without the protections of notice-and-comment rulemaking, would significantly undercut the interests of predictability and

finality—two chief goals of administrative law. The protections afforded through notice-and-comment rulemaking are a vital part of the effort to provide certainty, predictability, and stability to administrative law. If administrative agencies such as FTC come to believe that rulemaking procedures are too cumbersome or inconvenient to follow, and are instead allowed to disrupt stakeholders' settled expectations by seeking massive liability under the agency's post hoc reinterpretation of existing law, then an important safeguard for our representative system of government will be lost, and the rule of law will be undermined.

In sum, the FTC failed to adopt its new interpretation of § 5 through procedures “reasonably suggesting that Congress ever thought of [such pronouncements] as deserving the deference claimed for them here.” *Mead*, 533 U.S. at 231. The FTC never formally put the world on notice that it was planning to enforce such a radically expansive interpretation of its authority under § 5, never amended its implementing regulations, and never solicited public comments about its new interpretation of the FTC Act. To accord *Chevron* deference under these circumstances would be to invite all agencies to circumvent the protections of notice-and-comment rulemaking simply by imposing ad hoc interpretations and substantive requirements on all affected stakeholders. The scope of *Chevron* deference cannot be permitted to reach so far. *See City of Arlington*, 133 S. Ct. at 874 (“[W]here Congress has established an ambiguous line, the agency can go no

further than ambiguity will fairly allow.”).

II. The FTC Failed to Provide Wyndham With Fair Notice of What § 5 Requires

Even if § 5 does give the FTC inherent authority to impose data-security standards on the business community, due process requires that “parties receive fair notice before being deprived of property.” *Gen. Elec. Co. v. EPA*, 53 F.3d 1324, 1328 (D.C. Cir. 1995). The Supreme Court has long held that “the dividing line between what is lawful and unlawful cannot be left to conjecture.” *Connally v. General Constr. Co.*, 269 U.S. 385, 393 (1926). Fundamental fairness requires that citizens “be informed as to what the State commands or forbids.” *Lanzetta v. New Jersey*, 306 U.S. 451, 453 (1939). “The idea is that ordinary individuals trying to conform their conduct to law should be able to do so by reading the *face* of a statute—not by having to appeal to outside legal materials.” *Sabetti v. DiPaolo*, 16 F.3d 16, 17 (1st Cir. 1994) (emphasis in original) (Breyer, J.).

The requirements of fair notice and warning apply with equal force in civil enforcement actions brought by administrative agencies. *See, e.g., FCC v. Fox Television Stations, Inc.*, 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.”); *Boutilier v. INS*, 387 U.S. 118, 123 (1967) (“[T]he ‘void for vagueness’ doctrine [is] applicable to civil as well as criminal actions.”). As the Supreme Court recently emphasized, “[i]t is one thing to

expect regulated parties to conform their conduct to an agency's interpretations once the agency announces them; it is quite another to require regulated parties to divine the agency's interpretations in advance or else be held liable when the agency announces its interpretations for the first time in an enforcement proceeding and demands deference." *Christopher v. SmithKline Beecham Corp.*, 132 S. Ct. 2156, 2168 (2012). In cases "where the regulation is not sufficiently clear to warn a party about what is expected of it—an agency may not deprive a party of property by imposing civil or criminal liability." *Gen. Elec. Co.*, 53 F.3d at 1329.

Such Supreme Court precedent highlights the critical role of agency guidance in giving regulated entities fair notice of what practices could subject them to liability. Such concerns are even more pronounced in this case, given the rapidly evolving nature of data security and online privacy. Indeed, "given the literal breadth of Section 5 and the FTC's efforts to foster best practices, in most [data-security] cases entities subject to potential enforcement are confronted by a minefield where it can be nearly impossible to distinguish between advisable and required data-security behavior." Gerard M. Stegmaier & Wendell Bartnick, *Psychics, Russian Roulette, & Data Security: The FTC's Hidden Data-Security Requirements*, 20 Geo. Mason L. Rev. 673, 681 (2013).

The FTC's current approach to data security deprives companies like

Wyndham of “fair notice of conduct that is forbidden or required.” *FCC v. Fox*, 132 S. Ct. at 2317. The text of § 5 itself clearly provides no meaningful notice to regulated parties about data security; it generally prohibits “unfair and deceptive” business practices without going into any further detail as to what practices might be prosecuted as “unfair” or “deceptive.” *See* 15 U.S.C. § 45. As detailed above, the FTC has never promulgated any rules, regulations, or other formal guidance explaining what data-security practices the Commission believes § 5 to forbid or require. Rather, the FTC’s exercise of authority in data-security has consisted almost entirely of a series of consent decrees with private parties. Such regulation by consent decree typifies the FTC’s intentionally “enforcement-centric rather than rulemaking-centric” regulatory approach, which “is *ex post* rather than *ex ante* and case-by-case rather than one-size-fits-all.” Maureen K. Ohlhausen, *Remarks to the Sixth Annual Telecom Policy Conf.*, at 11 (Mar. 18, 2014).

Such an inscrutable approach to regulatory enforcement is not only deeply unfair to the business community, but it falls far short of satisfying the legal standard for fair notice. To begin with, it is widely understood that a consent decree binds only the parties to the agreement. *See, e.g., Altria Group, Inc. v. Good*, 555 U.S. 70, 89 n.13 (2008)(acknowledging that a “FTC consent order is . . . only binding on the parties to the agreement”). Such private settlements in no way constrain the FTC’s future enforcement decisions; unlike formal rulemaking, they

do not even purport to lay out general enforcement principles. “Nor is a consent decree a controlling precedent for later Commission action.” *Beatrice Foods, Co. v. FTC*, 540 F.2d 303, 312 (7th Cir. 1976). Rather, the “function of filling in the interstices of [a statute] should be performed, as much as possible, through quasi-legislative promulgation of rules to be applied in the future.” *SEC v. Chenery Corp.*, 332 U.S. 194, 202 (1947).

Even a cursory examination of the language contained in the consent decrees belies the Commission’s suggestion that they provide any sort of meaningful guidance. Of the 45 known data-security related actions brought by the FTC that were settled by consent decree, nearly all of them contain provisions stipulating that the agreement does not constitute an admission of any violation of the law. The fact that those consent agreements, by their very terms, manifest no finding of wrongdoing whatsoever utterly belies the FTC’s suggestion that such agreements can somehow provide the world with notice of what actual wrongdoing looks like. The circumstances of each case are different, and the FTC has never explained why data-security practices in one case may violate § 5 while those same practices may not violate § 5 in another case.

The FTC’s online brochure provides even less useful information by way of fair notice. This single pamphlet contains little more than opaque recommendations like “SCALE DOWN. Keep only what you need for your business” and “LOCK

IT. Protect the information that you keep.” FTC, *Protecting Personal Information: A Guide for Business* (2011), available at <http://goo.gl.m8d2NQ>. In any event, these are recommendations, not the law, and no business would be entitled to a safe harbor from prosecution even if it attempted to follow these recommendations to the letter.

Simply put, the FTC has not satisfied its “duty to define the condition under which conduct . . . would be unfair so that businesses will have an inkling as to what they can lawfully do rather than be left in a state of complete unpredictability.” *E.I. du Pont de Nemours & Co. v. FTC*, 729 F.2d 128, 138-39 (2d Cir. 1984). This Court has refused to punish a defendant’s past conduct when an agency’s newly expanded interpretation of the law fails to provide clear guidance for compliance. *See Dravo Corp. v. Occupational Safety & Health Review Comm’n*, 613 F.2d 1227, 1232-33 (3d Cir. 1980)(rejecting an agency’s expansive interpretation where the agency did not “state with ascertainable certainty what is meant by the standards [it] ha[d] promulgated”).

Because “complaints and consent orders differ when identifying non-complying practices and imposing data-security safeguards,” it remains “unclear whether nonparties to the investigation should attempt to follow the complaint, the consent order, or both when complying with Section 5, or whether the failure to implement some or all of the measures would result in a prohibited unfair

practice.” Stegmaier & Bartnick, *supra*, at 693. The law does not require a business to heed a regulation “with the exercise of extraordinary intuition or with the aid of a psychic.” *United States v. Chrysler Corp.*, 158 F.3d 1350, 1357 (D.C. Cir. 1998).

CONCLUSION

The interests of fairness, predictability, and the rule of law were all injured in this case. For the foregoing reasons, *amici* Washington Legal Foundation and Allied Educational Foundation respectfully request that the Court reverse the judgment below.

Respectfully submitted,

/s/ Cory L. Andrews

Cory L. Andrews

Richard A. Samp

WASHINGTON LEGAL

FOUNDATION

2009 Mass. Ave., N.W.

Washington, DC 20036

(202) 588-0302

Counsel for Amici Curiae

COMBINED CERTIFICATIONS

I hereby certify that:

1. This brief complies with the type-volume limitations of Fed. R. App. P. 32(a)(7)(B) because this brief contains 4,908 words, excluding those 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 typestyle requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced serif typeface using Microsoft Office Word 2010 in 14-point Times New Roman font.
3. Pursuant to Local Rule 46.1, Cory L. Andrews is a member in good standing of the bar for the United States Court of Appeals for the Third Circuit.
4. The text of the electronically filed brief is identical to the text in the paper copies.
5. A virus detection program (VIPRE Business, Version 5.0.4464) has scanned the electronic file and no virus was detected.

Dated: October 14, 2014

/s/ Cory L. Andrews
Cory L. Andrews

CERTIFICATE OF SERVICE

Pursuant to Fed. R. App. P. 25(d), I hereby certify that on October 14, 2014, the foregoing *amicus curiae* brief was filed electronically with the Clerk of the Court for the United States Court of Appeals for the Third Circuit using the appellate CM/ECF system. To the best of my knowledge, all parties to this case are represented by counsel who are registered CM/ECF users and will be served electronically by the appellate CM/ECF system.

/s/ Cory L. Andrews
Cory L. Andrews