No. 16-16270

IN THE UNITED STATES COURT OF APPEALS
FOR THE ELEVENTH CIRCUIT

LabMD, Inc.,
***Petitioner*,**

v.

Federal Trade Commission,
***Respondent*.**

Petition for Review from the Federal Trade Commission,
In the Matter of LabMD, Inc., FTC Matter/File No. 102 3099, Docket No. 9357

BRIEF *AMICUS CURIAE* OF THE CHAMBER OF COMMERCE OF THE UNITED STATES OF AMERICA IN SUPPORT OF PETITIONER

Kate Comerford Todd
Steven P. Lehotsky
Sheldon Gilbert
U.S. CHAMBER
LITIGATION CENTER
1615 H Street, NW
Washington, DC 20062
(202) 463-5337

William S. Consovoy
CONSOVOY MCCARTHY PARK PLLC
3033 Wilson Boulevard, Suite 700
Arlington, VA 22201
(703) 243-9423

Michael H. Park
CONSOVOY MCCARTHY PARK PLLC
3 Columbus Circle, 15th Floor
New York, NY 10019
(212) 247-8006

Counsel for Amicus Curiae

Dated: January 3, 2017

CERTIFICATE OF INTERESTED PERSONS AND CORPORATE DISCLOSURE STATEMENT

Pursuant to Rules 26.1 and 29(c) of the Federal Rules of Appellate Procedure, *amicus curiae* states that the Chamber of Commerce of the United States of America has no parent company, and no publicly held company owns 10% or more of its stock.

Further, pursuant to Eleventh Circuit Rule 26.1-1, *amicus curiae* believes that the Certificate of Interested Persons contained in the Brief of Petitioner LabMD, Inc. is complete.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page

CASES

STATUTES AND REGULATIONS

OTHER AUTHORITIES

STATEMENT OF INTEREST OF *AMICUS CURIAE*[1]

The Chamber of Commerce of the United States of America ("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, from every region of the country. An important 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 Chamber respectfully submits this brief as *amicus curiae* in support of Petitioner LabMD, Inc. ("LabMD"). The businesses represented by the Chamber 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 many reasons. *Amicus curiae* has a significant interest in explaining to the Court the legal and policy implications of the August 1, 2016 Order and Opinion of the Federal Trade Commission ("Commission" or "FTC").

[1] Pursuant to Fed. R. App. P. 29(c), *amicus curiae* states that no counsel for a party authored this brief in whole or in part, and no counsel or party made a monetary contribution intended to fund the preparation or submission of this brief. No person other than *amicus curiae*, its members, or its counsel made a monetary contribution intended to fund its preparation or submission. All parties have consented to the filing of this brief.

STATEMENT OF ISSUES

Whether the Commission exceeded its legal authority in finding LabMD's data-security practices "unfair" under Section 5 of the Federal Trade Commission Act of 1914 ("Act").

SUMMARY OF ARGUMENT

The Act prohibits "unfair methods of competition in or affecting commerce." 15 U.S.C. § 45(a) ("Section 5"). Based on this provision, the FTC claims the authority to regulate cybersecurity generally and to bring administrative actions against companies that have fallen victim to hackers. This assertion of enforcement authority is overbroad as a matter of law and is misguided as a matter of policy.

Over the past decade, the FTC has departed from the statutory underpinnings of the Act's prohibition against "unfair" trade practices. It has increasingly wielded its enforcement authority to extract settlements from businesses that have been victimized by data-security breaches and that had no formal notice of the standards the FTC accuses them of violating. Although the FTC plays an important role in protecting consumers, its "unfairness" authority does not include setting and enforcing—whether through litigation or consent orders[2]—general data-security

[2] When the FTC claims that a data-security breach constitutes an "unfair" trade practice, it is often able to obtain Section 5 consent orders from the targeted

policy. Indeed, the FTC has expressly acknowledged that it does not possess the general authority to regulate data security, which is why it continues to press Congress for additional rulemaking authority.

The FTC should not be permitted to circumvent the legislative process by establishing rules through private enforcement actions. This unilateral regulation-through-settlement approach subjects American businesses to vague 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 face considerable pressure to settle in order to avoid expending substantial resources fighting the agency. The *in terrorem* effect of a notice by itself is thus significant. The threat that the FTC's arsenal of enforcement capabilities poses can discourage businesses from adopting new technologies and sharing information about breaches to avert future attacks.

Endorsing the FTC's theory that suffering a data breach is an "unfair" trade practice would expose most businesses in America to government enforcement actions whenever they suffer a cyberattack or other incident that potentially compromises personal data. Congress did not envision such a result when it passed legislation limiting the FTC's Section 5 authority over "unfair" acts or practices,

---

businesses. This case is among the few data-security "unfairness" proceedings to be reviewed by courts.

and this Court should not countenance it. The Third Circuit's decision to the contrary in *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015), was wrongly decided and, in any event, it is not binding on this Court.

The businesses the Chamber represents take seriously their responsibility to safeguard all personally identifying data. But the reality is that malicious actors—such as foreign intelligence services, terrorist groups, hacking collectives, and criminal organizations—target businesses to steal information, including personal data and intellectual property.[3] No data security system is perfect, and breaches sometimes occur. Perversely, the FTC does not seek to punish the perpetrators of data theft, but the businesses that have been victimized on the untenable theory that vulnerabilities in their data-security policies constituted "unfair" trade practices. In short, the FTC's effort to set cybersecurity policy is classic regulatory overreach. Section 5 of the Act does not grant it the legal authority to act as a roving regulator of data-security standards. The FTC's order should be vacated.

[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.

ARGUMENT

I. The FTC's Authority to Prohibit Unfair Trade Practices Does Not Include the Authority to Establish General Data-Security Policy.

As the Supreme Court has cautioned, "[w]hen 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 invocation of the Act's prohibition against "unfair" trade practices to regulate data security is such a claim. Cybersecurity affects just about every American business, regardless of size or industry, in our increasingly interconnected economy. The FTC's assertion of regulatory authority is precisely the type of expansive agency interpretation the Supreme Court has rejected as "an enormous and transformative expansion in [an agency]'s regulatory authority without clear congressional authorization." *Id*. This Court should reject it too.

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. Other laws grant the FTC the authority to regulate data security *in certain, limited contexts*—laws that would have been entirely unnecessary if Congress already had given the FTC the broad authority to regulate data security it now claims to have. Indeed, the

FTC has been pressing unsuccessfully for years for legislation that would give it rulemaking authority under the Administrative Procedure Act ("APA") in the area of general data security. *See, e.g.*, *Data Security: Hearing Before the H. Comm. on Energy & Commerce, Subcomm. on Commerce, Mfg., & Trade*, 112th Cong. 11 (June 15, 2011) (prepared statement of FTC) [hereinafter *FTC 2011 Data Security Testimony*], http://www.ftc.gov/os/testimony/110615datasecurityhouse.pdf.

The FTC's enforcement actions are similar to its 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 agency rarely wielded the "unfairness" aspect of its authority until 1972, when the Supreme Court in dictum cited with apparent approval a little-used FTC test for unfairness. *See* 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)*, 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: whether the conduct: (1) "offend[ed] public policy"; (2) was "immoral, unethical, oppressive, or unscrupulous"; and (3) "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 broad criteria. In 1978, for example, the FTC issued a proposed 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). In particular, that provision 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).[4]

Despite these acknowledged statutory constraints, carefully calibrated by Congress in response to years of agency overreaching, the FTC again is attempting to wield Section 5 inappropriately. Here, the FTC seeks to impose liability on LabMD for its alleged failure to implement "reasonable and appropriate" security measures. But liability under Section 5 attaches only when an act *itself* injures consumers. *See FTC v. Neovi, Inc.*, 604 F.3d 1150, 1157 (9th Cir. 2010). A business cannot violate Section 5 unless it has "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 1156-57. But an attack that first *victimizes the business itself* cannot be considered "unfair" to consumers.

[4] 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 agency'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 FTC's ability to take public policy concerns, without more, into account when pursuing unfairness enforcement actions. *See id.* at 1073.

For example, the FTC has obtained injunctions under Section 5 prohibiting defendants from engaging in "phishing" identity-theft scams, through which defendants sent e-mails 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 LabMD's victimization at the hands of a hacker with a business affirmatively engaging in a criminal enterprise like a phishing scam. Assigning liability for a data-security breach impermissibly stretches the bounds of Section 5.

In short, the FTC is using its Section 5 unfairness authority to pursue its policy prerogatives, which 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." The agency cannot exercise its regulatory authority in a manner inconsistent with its legislative mandate. *See FDA v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120, 125 (2000).

Nevertheless, the Third Circuit recently adopted an expansive interpretation of "unfair" in *FTC v. Wyndham Worldwide Corp.*, and rejected the argument that subsequent congressional action indicates that Section 5 excludes cybersecurity. 799 F.3d at 247-49. As explained above, however, the Third Circuit's decision is incorrect because it disregards limitations on the scope of the FTC's unfairness

authority and minimizes the subsequent actions of Congress. To the extent that the Third Circuit in *Wyndham* found that a data-security breach can itself ever constitute an unfair practice, that was wrong; but even if it could, the FTC would still have to establish substantial injury, as Petitioner explains. *See* LabMD Br. at 13-16. In short, the *Wyndham* decision is not binding on this Court and should not be followed.

II. Businesses Cannot Operate Effectively and Efficiently in an "Evolving Enforcement" Regime.

Over the past decade, the FTC has increasingly exerted its will in the data-security area by entering into and publishing dozens of consent orders settling charges against businesses for failing to employ "reasonable and appropriate" measures to protect personal information. The FTC typically negotiates, enters into, and publishes these agreements before even filing a complaint, and then claims afterwards that the data-security "standards" announced in conjunction with the consent orders are legal requirements under Section 5. This piecemeal "regulation by consent order" has enabled the FTC to impose its evolving policy preferences on companies with little oversight by Congress, with limited participation from all relevant stakeholders (including the business community), and without judicial review. *Cf. Sackett v. EPA*, 132 S. Ct. 1367, 1374 (2012) (rejecting the 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 year-long, multi-stakeholder effort to develop a framework to guide and enhance efforts to reduce data-security risks to critical infrastructure. *See* NIST, *Framework for Improving Critical Infrastructure Cybersecurity Version 1.0* (Feb. 12, 2014), https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf. NIST's open and collaborative effort to develop a cybersecurity framework contrasts sharply with the FTC's backwards-looking, opaque approach to enforcing its own 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 of what they should do 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 constantly change.[5] The fact that

[5] *See, e.g.*, 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."); Gerard Stegmaier & Wendell Bartnick, *Another Round in the Chamber: FTC Data*

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 data-security standards issued by private-sector organizations.[6]

In many cases, the FTC has announced 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), http://www.ftc.gov/os/caselist/0823153/100608davebusterscmpt.pdf. When 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 FTC to deploy 20/20 hindsight—"you were breached, therefore your security must have been inadequate"—when evaluating data breaches.

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 the fair notice doctrine).

[6] For example, to accept payment cards from the major card brands, businesses must comply with the 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.

The FTC has admonished businesses to follow and to 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), http://www.ftc.gov/os/testimony/100727consumerprivacy.pdf (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"). But discerning consistent standards from these consent orders is futile because the FTC's definition of "reasonable" depends on the business it is investigating. The FTC has stated that the reasonableness of data-security measures "will depend on the size and complexity of the business, and the sensitivity of the information at issue." *The Data Security & Breach Notification Act of 2010: Hearing on S. 3742 Before the Subcomm. on Consumer Prot., Prod. Safety, & Ins.*, 111th Cong. 7 n.22 (Sept. 22, 2010), http://www.ftc.gov/os/testimony/100922datasecuritytestimony.pdf. Piecemeal, individualized consent orders against businesses in different industries cannot provide general guidance.

The FTC's regulation by consent order has an especially 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 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 submissions to consent decrees. Not surprisingly, a significant number of the FTC's data-security consent decrees have involved small businesses. In addition to imposing exorbitant costs, the FTC's regulatory approach shifts the focus of small-business personnel away from managing and growing their businesses to responding to intrusive FTC investigations. Indeed, that is exactly what happened here. *See* LabMD Br. at 6 ("[A]s a result of the crushing burdens imposed upon it by the FTC's investigation and ensuing action, LabMD was forced to wind down operations and stop diagnosing cancer.").

Complying with consent orders also is onerous. In its data-security consent decrees, the FTC typically insists on a period 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), http://ftc.gov/os/caselist/1023120/120327rockyouorder.pdf. If the FTC later determines that a company subject to a consent order is not in compliance with a "new" data-security principle, then the company may be 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). In short, it is difficult for a company subject to an FTC consent order even to know if it is in compliance 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 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," "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."). Even the Third Circuit in *Wyndham* noted that consent orders, because they "admit no liability" and "focus on prospective requirements on the defendant," can be "of

little use … in trying to understand the specific requirements imposed by § 45(a)." *Wyndham*, 799 F.3d at 257 n.22; *see also id*. at n.23 ("it may be unfair to expect private parties back in 2008 to have examined FTC complaints or consent decrees" in search of data security standards to illuminate the meaning of Section 5).

The FTC's actions investigating, testifying about, and providing public guidance on companies' data-security obligations under the Act do not give it authority over the field. If that were the case, then any agency could assume authority over a subject matter on its own accord simply by making public statements about it. But agencies are permitted to act only with, and within, the authorization of Congress.

The FTC's efforts to regulate by consent order also contradicts Supreme Court precedent and the FTC's own opinions. *See Altria Group, Inc. v. Good*, 555 U.S. 70, 89 n.13 (2008) (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 adopted as modified by full Commission); *In re Trans Union Corp.*, 118 F.T.C. 821, 864 n.18 (1994) (noting that a "consent agreement [with a party] is binding only between the Commission and [that party]"). Congress also emphasized the

uniqueness of consent orders in its revision to the 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 FTC Pronouncements Without Regard for the Legislative Process.

In 2011, the FTC 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), http://www.ftc.gov/opa/2011/02/settlement.shtm. 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.[7]

[7] 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,

This statement captures the FTC's "shoot first, ask questions later" approach to regulating data security, with the agency admitting that it enforces standards against businesses *without any notice*. The FTC may have thought that it was being helpful to the business community by informing it of the standard "[l]ooking forward"; but in reality, it was holding the respondents to a standard that they did not know existed. That will happen every time the FTC enforces a new element of its evolving data-security policy.

A better way to establish consistent and transparent data-security standards is through a dialogue with all stakeholders, accomplished through democratically accountable means, not by agency fiat. At the same time the FTC is wielding "all of the tools at its disposal" to enforce its own data-security prerogatives against individual companies, policymakers, the business community, consumer advocacy groups, and other interested entities are engaging in a serious dialogue over how to craft data-security policy in the United States. The discussions among these many groups, including the Chamber and the FTC, include 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.

---

092 3089 (rev. Aug. 15, 2011), http://www.ftc.gov/os/2011/08/110819settlementonestatement.pdf.

See generally U.S. Chamber of Commerce, *U.S. Chamber Policy Priorities for 2014* at 20-21 (Sept. 2014), https://www.uschamber.com/sites/default/files/2014_policy_priorities-september_2014.pdf (describing cybersecurity policy initiatives, including "[e]nact[ing] cybersecurity information-sharing legislation that includes robust safeguards for businesses that voluntarily exchange threat data with their peers and government partners"); Cong. Research Serv., *Federal Laws Relating to Cybersecurity: Overview and Discussion of Proposed Revisions* (June 20, 2013), https://www.fas.org/sgp/crs/natsec/R42114.pdf (analyzing proposed cybersecurity legislation); *FTC 2011 Data Security Testimony* (advocating for data-security legislation).

In recent years, Congress has rejected a number of data-security bills, including ones that would have given the FTC rulemaking authority over consumer data security. 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 Act, the agency may 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

agencies under the APA; among other restrictions, the statute permits interested parties to cross-examine witnesses. But the FTC has *never attempted to issue data-security rules in this manner*. Instead, the FTC 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 violating its congressional mandate. Instead of respecting the legislative process and the proper means for seeking and receiving express authority to regulate data security generally, the FTC, as it did in the late 1970s, is again exceeding the bounds of its Section 5 unfairness authority by engaging improperly in *ultra vires* regulation by consent order.

* * *

Amicus curiae admits the importance of data security and cybersecurity in today's digitally connected world. Businesses have every incentive 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 craft fair, transparent, and consistent legal frameworks that companies can efficiently assess and apply.

The FTC historically has had an important, statutorily mandated role to play in protecting consumers. But its attempt here 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 FTC's Order should be vacated.

Respectfully submitted,

/s/ William S. Consovoy

William S. Consovoy
CONSOVOY MCCARTHY PARK PLLC
3033 Wilson Boulevard, Suite 700
Arlington, VA 22201
(703) 243-9243

Michael H. Park
CONSOVOY MCCARTHY PARK PLLC
3 Columbus Circle, 15th Floor
New York, NY 10019
(212) 247-8006

Counsel for Amicus Curiae

Kate Comerford Todd
Steven P. Lehotsky
Sheldon Gilbert
U.S. CHAMBER LITIGATION CENTER
1615 H Street, NW
Washington, DC 20062
(202) 463-5337

Dated: January 3, 2017

CERTIFICATE OF COMPLIANCE

Pursuant to Fed. R. App. P. 32(a)(7)(C), I certify the following:

This brief complies with the type-volume limitations of Fed. R. App. P. 29(d) because it contains 4,687 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii).

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 Word 2015 in Times New Roman 14-point font.

This brief has been scanned for viruses and is virus-free.

By: */s/ William S. Consovoy*

William S. Consovoy
CONSOVOY MCCARTHY PARK PLLC
3033 Wilson Boulevard, Suite 700
Arlington, VA 22201
(703) 243-9423

Counsel for Amicus Curiae

CERTIFICATE OF SERVICE

I hereby certify that on this 3rd day of January, 2017, a true and correct copy of the foregoing was filed with the Clerk of the United States Court of Appeals for the Eleventh Circuit via the Court's CM/ECF system, which will send notice of such filing to all counsel who are registered CM/ECF users.

Under 11th Cir. R. 25-3(a), no independent service by other means is required.

By: */s/ William S. Consovoy*

William S. Consovoy
CONSOVOY MCCARTHY PARK PLLC
3033 Wilson Boulevard, Suite 700
Arlington, VA 22201
(703) 243-9423

Counsel for Amicus Curiae