No. 14-3514

IN THE UNITED STATES COURT OF APPEALS
FOR THE THIRD CIRCUIT

FEDERAL TRADE COMMISSION,
Plaintiff-Appellee,

v.

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

On Interlocutory Appeal From An Order Of
The United States District Court For The District Of New Jersey,
Case No. 13-cv-01887 (Salas, J.)

BRIEF OF AMICI CURIAE CENTER FOR DEMOCRACY & TECHNOLOGY AND ELECTRONIC FRONTIER FOUNDATION

LEE TIEN
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333

CATHERINE CRUMP
CHRIS JAY HOOFNAGLE
Samuelson Law, Technology & Public Policy Clinic
U.C. Berkeley School of Law
Berkeley, CA 94720
Telephone: (510) 642-1741

JUSTIN BROOKMAN
G.S. HANS
Center for Democracy & Technology
1634 I Street NW, Suite 1100
Washington, D.C. 20006
Telephone: (202) 637-9800

November 12, 2014

CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rules of Appellate Procedure 26.1 & 29(c)(1), amicus curiae the Center for Democracy & Technology states that it has no parent corporation and that there is no publicly held corporation that owns 10% or more of the Center for Democracy & Technology.

Pursuant to Federal Rules of Appellate Procedure 26.1 & 29(c)(1), amicus curiae the Electronic Frontier Foundation states that it has no parent corporation and that there is no publicly held corporation that owns 10% or more of the Electronic Frontier Foundation.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

FEDERAL STATUTES

STATE STATUTES

OTHER AUTHORITIES

STATEMENT OF INTEREST OF *AMICI CURIAE*

The Center for Democracy & Technology and the Electronic Frontier Foundation respectfully submit this brief as *amici curiae* in support of appellee, the Federal Trade Commission.

The Center for Democracy & Technology ("CDT") is a nonprofit public interest group that seeks to promote free expression, privacy, individual liberty, and technological innovation on the open, decentralized Internet. CDT supports laws, corporate policies, and technical tools that protect the privacy of Internet users, and advocates for stronger legal controls on government surveillance. As innovative technologies emerge with new, sophisticated data collection capabilities, protecting users' privacy and ensuring security is increasingly important. CDT works to develop privacy safeguards for consumers through a combination of legal, technical, and self-regulatory measures to ensure that services are designed in ways that preserve privacy, establish protections that apply across the lifecycle of consumers' data, and give consumers control over how their data is used in the digital age.

The Electronic Frontier Foundation ("EFF") is a member-supported civil liberties organization working to protect free speech and privacy rights in the online world. With more than 30,000 dues-paying members

nationwide, EFF represents the interests of technology users in both court cases and in broader policy debates surrounding the application of law in the digital age.

Pursuant to Federal Rule of Appellate Procedure 29, all parties have consented to the filing of this brief.

INTRODUCTION AND SUMMARY OF ARGUMENT

Through the unfairness provision of the Federal Trade Commission Act, 15 U.S.C. § 45(a), the Federal Trade Commission ("FTC") plays an invaluable role in incentivizing businesses to take reasonable data security precautions. After Wyndham Hotels & Resorts, LLC ("Wyndham") failed to take such precautions, more than 619,000 consumer payment card account numbers were compromised over the course of three sequential, substantially similar attacks. *FTC v. Wyndham Worldwide Corp. et al.*, No. 2:13-cv-01887-ES-JAD, 2014 WL 1349019, at *2-3 (D. N.J. April 7, 2014) . Wyndham now asks this Court to direct the district court to dismiss the unfairness count of the FTC's Complaint on the ground that the FTC lacks the authority to ensure businesses like Wyndham protect their customers' data.

This Court should reject Wyndham's arguments for the reasons set forth by the FTC. Amici write to emphasize three additional points: *First*,

Wyndham has provided no principled reason why the FTC's grant of general authority to bring enforcement actions against "unfair . . . acts or practices," 15 U.S.C. § 45(a) , should exclude the act or practice of implementing data security measures that are unfair. Wyndham posits that because it "*itself* was the victim of criminal conduct by others," Appellant's Br. at 3, it is immunized from its duty to adopt reasonable data security measures. This Court should reject that argument. The fact that hackers accessed the data does not abrogate Wyndham's responsibility for observing minimum data security practices to prevent harm from befalling its customers. Data security is a responsibility similar to many other business functions; there is nothing about data security that makes it fundamentally different from other obligations to provide a safe experience to the consumer.

Second, accepting Wyndham's expansive view of due process requirements would not only invalidate the FTC's unfairness authority, but also would call into question all bodies of law premised on a reasonableness standard. As the FTC explains, all of tort law is grounded in this concept, and the duty to act reasonably is found in a broad array of statutes. Appellee's Br. at 41-44. Amici draw attention to two collections of such statutes: other federal statutes that also contain unfairness provisions virtually identical in their wording to the FTC Act, and the large number of

state data security statutes grounded in a flexible reasonableness standard. A century ago, Congress incorporated the concept of unfairness into federal law to protect the marketplace from anticompetitive business practices; it later extended this concept to protect consumers from other acts or practices that are unfair. States followed suit when crafting their own laws to protect consumers from businesses that do not reasonably secure their customers' private data. This Court should not unsettle the law by undermining the concept of unfairness today.

Finally, as a policy matter, the unfairness standard has a crucial role to play in protecting consumers. This is particularly the case because neither self-regulation nor a rigidly rule-based regime is an adequate alternative.

ARGUMENT

I. WYNDHAM PROVIDES NO PRINCIPLED REASON WHY THE FTC'S AUTHORITY TO BRING ENFORCEMENT ACTIONS AGAINST UNFAIR PRACTICES SHOULD CONTAIN A CARVE-OUT FOR UNFAIR DATA SECURITY PRACTICES.

Wyndham provides no persuasive argument why data security is categorically exempt from the FTC's authority to bring enforcement actions against "unfair . . . acts or practices." 15 U.S.C. § 45(a). The fact that data security is important, Appellant's Br. at 5, that it is a problem broadly shared by the private and public sectors, *id*. at 4, or that it is a duty that can be interfered with by malicious third parties, *id.* at 15, does not distinguish data

security from other business responsibilities. Data security is a responsibility that protects the business itself, other businesses, and the businesses' customers.

Wyndham's assertion that it was itself a victim, *id*. at 15, ignores that inadequately protecting data has far-reaching consequences. Especially in highly networked environments, a business's lax data security practices expose not only itself to potential harm, but also its customers and other businesses. And it is well-established that businesses have a legal obligation to not unreasonably leave their customers vulnerable to harm from third parties. *See* Appellee's Br. at 28 (noting precedent stating a "company's acts can be unfair . . . if they unreasonably enable third parties to harm consumers"). Consider the recent FTC enforcement action against Neovi, a company that enabled consumers to print bank checks online. *FTC v. Neovi, Inc.*, 604 F.3d 1150 (9th Cir. 2010). Neovi failed to implement adequate security measures to ensure that its users only drew checks on accounts for which they were authorized users, a failure repeatedly exploited by persons who printed checks withdrawing money from other persons' accounts without authorization. *Id.* at 1153-54. The Ninth Circuit upheld the FTC's determination that Neovi acted unfairly because the company's failure to implement adequate security measures left it "highly vulnerable to con

artists and fraudsters." *Id.* at 1154. Here, just as in *Neovi*, Wyndham failed to adequately secure its system against unauthorized access, even when Wyndham should have known its failure would likely result in consumer harm. Neither Wyndham nor its amici has provided a persuasive argument why data security should fall out of unfairness enforcement power as a categorical matter.

II. ACCEPTING WYNDHAM'S DUE PROCESS ARGUMENT WOULD JEOPARDIZE A BROAD RANGE OF LAW GROUNDED IN A FLEXIBLE REASONABLENESS STANDARD.

Wyndham contends it was denied due process because the FTC has not provided adequate guidance regarding what "reasonable and appropriate" data security measures it was obligated to implement. Appellant's Br. at 35-36. The Court should reject this argument. As the FTC maintains, reasonableness is a well-known principle of tort law long accepted as providing adequate notice. Appellee's Br. at 40; *cf. Sears, Roebuck & Co. v. FTC*, 258 F. 307, 311 (7th Cir.1919) ("If the expression 'unfair methods of competition' is too uncertain for use, then under the same condemnation would fall the innumerable statutes which predicate rights and prohibitions upon 'unsound mind,' 'undue influence,' 'unfaithfulness,' 'unfair use,' 'unfit for cultivation,' 'unreasonable rate,' 'unjust discrimination,' and the like.") Additionally, the FTC did in fact provide

notice that basic data-security precautions are required, but Wyndham still fell short. Appellee's Br. at 40.

Accepting Wyndham's argument that the concept of reasonableness fails to provide fair notice would unsettle vast swaths of well-established law. As the FTC explains, much of tort law is grounded in the concept of reasonableness, Appellant's Br. at 41, and courts do not violate due process when holding businesses liable for negligence. Also, many federal statutes impose duties to act reasonably. Appellee's Br. at 42-43.

Amici write to draw particular attention to two bodies of law that would be called into question by a ruling for Wyndham. Since the passage of the FTC Act, Congress has granted a variety of federal agencies the ability to take steps against unfair acts or practices, and accepting Wyndham's due process argument would call into question these grants of authority. Moreover, adoption of Wyndham's argument would also undermine a broad range of state laws that require businesses to adopt appropriate and reasonable data security measures.

A. Accepting Wyndham's Due Process Argument Would Call Into Question The Validity Of Congressional Grants Of Authority To A Broad Range Of Federal Agencies.

Given the breadth of Wyndham's due process argument, accepting Wyndham's position would necessarily implicate the validity of a broad

range of consumer protection statutes that enable federal agencies to combat unfair acts or practices. These statutes are scattered throughout the U.S. Code, and grant authority to the Consumer Financial Protection Bureau, federal bankruptcy courts, the Federal Aviation Administration, the Department of Agriculture, and the Federal Housing Administration. This Court should not issue a ruling that would disturb a bedrock consumer protection principle, one that has supported a century of competition and consumer protection law.

1. Consumer Financial Protection Bureau

In response to the 2008 financial crisis, Congress created the Consumer Financial Protection Bureau ("CFPB") "for the purpose[] of ensuring that, with respect to consumer financial products and services[,] consumers are protected from unfair, deceptive, or abusive acts and practices and from discrimination." 12 U.S.C. § 5511(b)(2). So that the nascent agency would effectively carry out this mandate, Congress equipped the CFPB with the power to bring enforcement actions against persons committing or engaging in practices the agency determined to be "unfair."[1]

[1] 12 U.S.C. § 5531(a) (granting the CFPB authority to take actions regarding unfair acts or practices); *id.* at § 5563(a) (setting out hearings and adjudications as within the CFPB's power); *see also* Consumer Fraud Protection Bureau Supervision and Examination Manual v.2, pt. II.C at UDAAP 2 n.2 (Oct. 2012) *available at*

The Consumer Financial Protection Act ("CFPA") deploys language that almost mirrors the language in the FTC Act, *compare* 12 U.S.C. § 5531(c)(1) *with* 15 U.S.C. § 45(n), and it is therefore unsurprising that the CFPB has modeled its enforcement policies upon the FTC's application of the standard. *See* Consumer Fraud Protection Bureau Supervision and Examination Manual v.2, pt. II.C at UDAAP 2 n.2 (Oct. 2012).[2] In effect, Congress delegated to the CFPB the same authority to define and bring enforcement actions against unfair acts or practices that it has delegated to the FTC, albeit only in the area of consumer financial products and services. A determination that the FTC cannot, consistent with due process, regulate unfair data security practices inevitably implicates the legitimacy of the CFPB's authority to regulate unfair consumer financial products and services.

Recently, in the first case to address the constitutionality of the CFPB's authority to regulate unfair acts or practices, a district court rejected the argument that the CFPA's general prohibition of "unfair, deceptive, or

---

http://files.consumerfinance.gov/f/201210_cfpb_supervision-and-examination-manual-v2.pdf (last visited Nov. 9, 2014) (describing the CFPB as having "enforcement authority to prevent unfair, deceptive, or abusive acts or practices in connection with any transaction with a consumer for a consumer financial product or service, or the offering of a consumer financial product or service").

[2] *Available at* http://files.consumerfinance.gov/f/201210_cfpb_supervision-and-examination-manual-v2.pdf (last visited Nov. 9, 2014).

abusive act[s] or practice[s]" is unconstitutionally vague. *Illinois v. Alta Colleges, Inc.*, No. 1:14-cv-03786, 2014 WL 4377579, at *4 (N.D. Ill. Sept. 4, 2014) (internal quotation marks omitted) (alterations in original). In rejecting the vagueness challenge, the court made three interconnected findings. First, because the CFPA is an economic regulation and does not inhibit a "constitutionally-protected activity, [it] is subject to a lenient vagueness test." *Id.* (citing *Vill. of Hoffman Estates v. Flipside, Hoffman Estates, Inc.*, 455 U.S. 489, 498-99 (1982)). Second, the court held that as the CFPA defines "unfair" practices, "[t]he statute easily passes that test." *Id*. Third, the court noted what Congress had made obvious: the CFPA's general prohibition against unfair practices "is virtually identical" to the prohibition against unfair practices in the FTC Act. *Id.*

A fourth step can be inferred: if the CPFB's regulatory authority is grounded in language that is not constitutionally vague, then neither is the FTC's authorizing language. To conclude otherwise would deny standard canons of statutory interpretation—if Congress had not intended the CFPB and FTC to have similar authority to protect consumers from unfair practices, then surely it would not have used indistinguishable language. *Smith v. City of Jackson, Miss*., 544 U.S. 228, 233 (2005).

2. Federal Bankruptcy Law

Federal bankruptcy law protects consumers from unscrupulous individuals who negligently or fraudulently prepare bankruptcy petitions. *See* 11 U.S.C. § 110. In particular, Congress granted bankruptcy courts the authority to order damages or injunctive relief against "a bankruptcy petition preparer [who] violates [section 110] or commits any act that the court finds to be fraudulent, unfair, or deceptive . . . ." 11 U.S.C. § 110(i)(1) (providing for damages); *see also* 11 U.S.C. § 110(j)(2) (providing for injunctive relief).

Wyndham's due process argument implicates these bankruptcy code provisions because they fail to provide further guidance as to what constitutes fraudulent, unfair or deceptive acts or conduct. However, when this very argument was addressed in *In re Doser*, the court held that the bankruptcy code provisions were not unconstitutionally vague for failing to define fraudulent, unfair or deceptive acts or conduct. *In re Doser*, 412 F.3d 1056, 1063 (9th Cir. 2005) (observing that "the terms 'fraudulent,' 'unfair,' and 'deceptive' are used in numerous federal statutes and regulations and have been consistently upheld against vagueness challenges"). In reaching this conclusion, the court relied upon *In re Barcelo*, which held that "in light of the *common and accepted* statutory usage of 'unfair and deceptive,' and the widely known elements of fraudulent conduct . . . Section 110(i) is not

impermissibly vague." *In re Barcelo*, 313 B.R. 135, 145 (Bankr. E.D.N.Y. 2004) (emphasis added).

3. Other Federal Agencies With Unfairness Authority

Congress has given other federal agencies unfairness authority as well. In 1938, the Civil Aeronautics Act granted the predecessor to the Department of Transportation regulatory authority "modeled closely after [section] 5 of the Federal Trade Commission Act." *American Airlines v. N. American Airlines*, 351 U.S. 79, 82 (1956) (explaining that courts "look to judicial interpretation of [section] 5" to resolve issues with the Civil Aeronautics Act).[3] Specifically, Congress protected consumers by granting the Department of Transportation "the general authority to prohibit and punish unfair and deceptive practices in air transportation . . . ." *Northwest, Inc. v. Ginsberg*, 134 S. Ct. 1422, 1433 (2014) (citing 49 U.S.C. § 41712(a) ("[T]he Secretary may investigate and decide whether an air carrier, foreign air carrier, or ticket agent has been or is engaged in an *unfair* or deceptive

[3] Congress also extended unfairness authority to the Federal Housing Administration. 12 U.S.C. § 1706f(d) ("In connection with the purchase of a manufactured home financed with a loan or extension of credit insured by the Federal Housing Administration under this subchapter, the Secretary shall prohibit acts or practices in connection with loans or extensions of credit that the Secretary finds to be *unfair*, deceptive, or otherwise not in the interests of the borrower.") (emphasis added).

practice . . . in air transportation or the sale of air transportation.") (emphasis added)).

Congress again used the FTC Act as the model when it empowered the Department of Agriculture with unfairness authority. The Packers and Stockyards Act makes it unlawful for packers, swine contractors, and live poultry dealers to "(e)ngage in or use any *unfair*, unjustly discriminatory, or deceptive practice or device." 7 U.S.C. § 192 (emphasis added). It also forbids any stockyard owner, market agency or dealer from engaging in "any *unfair*, unjustly discriminatory, or deceptive practice or device" with respect to a broad range of activities related to livestock. 7 U.S.C. § 213(a) (emphasis added).

The inclusion of unfairness language in federal statutes, far from being "fundamentally inconsistent with the rule of law," Appellant's Br. at 16, is an essential component of consumer protection because Congress cannot envision the myriad ways in which a company may act unfairly.

B. Accepting Wyndham's Due Process Arguments Would Cast Substantial Doubt On The Constitutionality Of A Broad Range Of State Data Security Statutes.

Wyndham's due process argument would call into question the validity of numerous state statutes as well. Since 2005, ten state legislatures have enacted data security statutes in an effort to protect consumers'

personal information.[4] Because information security is a general duty shared by many different kinds of businesses, state legislatures relied upon a reasonableness standard as the lodestar for regulatory enforcement. *See, e.g.*, Cal. Civ. Code § 1798.81.5(b) ("A business . . . shall implement and maintain reasonable security procedures . . . ."). Furthermore, the prevalence of a reasonableness standard in state data security statutes indicates that it is an important component of consumer protection.

Not one of these state data security statutes contains the specific guidance Wyndham demands regarding what minimum standards are sufficient for compliance. Rather than exhaustively listing specific requirements, the majority of the statutes instead require businesses to comply with a flexible reasonableness standard.[5] For example, Arkansas, California, and Rhode Island all require businesses to "implement and maintain *reasonable* security procedures and practices *appropriate* to the nature of the information, to protect the personal information from

[4] Ark. Code Ann. § 4-110-104(b); Cal. Civ. Code § 1798.81.5(b); Conn. Gen. Stat. § 42-471(a); Md. Code Ann., Com. Law § 14-3503(a); 201 Mass. Code Regs. 17.00; Nev. Rev. Stat. § 603A.210; Or. Rev. Stat. § 646A.622; R.I. Gen. Laws § 11-49.2-2; Tex. Bus. & Com. Code Ann. § 521.052; Utah Code Ann. § 13-44-201.

[5] *See* Ark. Code Ann. § 4-110-104(b); Cal. Civ. Code § 1798.81.5(b); Md. Code Ann., Com. Law § 14-3503(a); Nev. Rev. Stat. § 603A.210(1) ; Or. Rev. Stat. § 646A.622(1); R.I. Gen. Laws § 11-49.2-2(2); Tex. Bus. & Com. Code Ann. § 521.052(a); Utah Code Ann. § 13-44-201(1).

unauthorized access, destruction, use, modification, or disclosure." Ark. Code Ann. § 4-110-104(b) (emphasis added); Cal. Civ. Code § 1798.81.5(b) (same); R.I. Gen. Laws § 11-49.2-2(2) (same). Accordingly, accepting Wyndham's argument that such specificity is a necessary component of due process would call into question the validity of all of these statutes.

1. Wyndham's Standards Render Even The Most Detailed State Statutes Insufficient.

Only three states have enacted data security statutes that detail minimum requirements beyond the implementation and maintenance of data security practices that are reasonable or appropriate given the nature of the information handled. *See* 201 Mass. Code Regs. 17.00; Nev. Rev. Stat. § 603A.210; Or. Rev. Stat. § 646A.622. Of these three statutes, Massachusetts' is the most comprehensive. The statute requires businesses to "develop, implement, and maintain a comprehensive information security program . . . contain[ing] administrative, technical, and physical safeguards that are appropriate to [] the size, scope and type of business . . . ; [] the amount of resources available . . . ; [] the amount of stored data; and [] the need for security and confidentiality of both consumer and employee information." 201 Mass. Code Regs. 17.03(1). The statute also establishes minimum technical standards with which every data security program must comply. *E.g. id.* at 17.04(4) (identifying the "reasonable monitoring of

systems, for unauthorized use of or access to personal information" as one of the technical requirements). Similarly, Oregon requires businesses to comply with a reasonableness standard supplemented with minimum administrative, physical, and technical requirements. Or. Rev. Stat. § 646A.622(2)(d) (listing necessary elements of a compliant data security scheme). Nevada fortifies its reasonableness standard with separate requirements for businesses that accept payment cards. Nev. Rev. Stat. § 603A.215 (requiring compliance with Payment Card Industry Data Security Standard).

But even these more detailed data security statutes fail to provide the specific guidance Wyndham contends is necessary to satisfy due process requirements. For instance, Wyndham points out that "the [FTC] has provided no guidance as to (1) what firewall configurations a business must employ, (2) what types of MAC or IP address authentication are necessary, (3) what encryption techniques must be used to secure consumer data, or (4) what password requirements a business must impose on its employees." Appellant's Br. at 37. Yet, even Massachusetts' statute—the most detailed of all of the state data protection schemes—fails to provide businesses with this kind of detailed guidance. *See, e.g.*, 201 Mass. Code Regs. 17.04(3) (identifying the "[e]ncryption of all transmitted records and files containing personal information" as necessary but failing to dictate specific encryption

techniques and settings). Oregon's statute also fails to meet Wyndham's standard of specificity, because although it requires that security programs designate an individual who will "assess[] risks in network and software design," it does not detail how such technical assessments should be conducted. *See* Or. Rev. Stat. § 646A.622(2)(d)(B)(i). Nevada does impose detailed requirements regarding the handling of payment card information, but its general data security statute rests upon a reasonableness standard that would be felled by accepting Wyndham's argument. *See* Nev. Rev. Stat. § 603A.210(1) ("A data collector that maintains records which contain personal information of a resident of this State shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification or disclosure.").

2. States Deliberately Adopted Reasonableness Standards To Provide Consumers With Greater Protection.

That ten states have incorporated a reasonableness standard into their data security statutes indicates that this approach is an important component of consumer protection. Additionally, the business community previously

favored a reasonableness standard over the command-and-control approach Wyndham now argues is necessary to satisfy due process.[6]

California is one state that incorporated a reasonableness standard into its data security statute specifically because of industry concerns.[7] As the bill's author noted, "the bill specifically [sought] to avoid the specific mandates and requirements that industry ha[d] consistently opposed in other bills." Cal. S. Judiciary Comm., Bill Analysis, 2003-2004 A.B. 1950, at 6 (2004). Instead, the bill was intended to "establish a minimum baseline standard that draws upon the reasonableness standard well-established in existing law." *Id.* Committee staff agreed that a function of the bill was "letting industry exercise its own judgment as to what constitutes an appropriate level of security." *Id.* at 6-7. Far from being a "dragnet" for California to hold virtually any business liable for violating an "unknown

[6] In fact, even Amicus Curiae Chamber of Commerce of the United States of America has previously opposed such detailed regulation. Pl.'s Resp. Br. at 21, *FTC v. Wyndham*, 2014 WL 1349019 (May 20, 2013).

[7] California recently approved three amendments to its data security statute, none of which materially affect the discussion of the statute in this brief. The new legislation takes steps including 1) extending the reasonable data security requirement to businesses who merely "maintain" personal information about California residents, 2) "prohibit[ing] the sale, advertisement, or offer to sell an individual social security number," and 3) requiring "appropriate identity theft prevention and mitigation services" be made available to affected residents at no cost, if the person or business providing the notification of the breach was also the source of the breach. 2013-2014 Cal. Stat. Ch. 855 (A.B. 1710).

(and unknowable) standard," Appellant's Br. at 36, the legislature determined the reasonableness standard to be wise public policy and consistent with due process. *See* Cal. S. Judiciary Comm., Bill Analysis, A.B. 1950, at 7 (2004) (noting "the Civil Code contains many standards which are not bright line rules, which appear to have caused few problems for industry").

State legislatures enacted data security statutes in order to ensure the protection of consumers' data. *See, e.g.,* Cal. Civ. Code § 1798.81.5(a) ("It is the intent of the Legislature to ensure that personal information about California residents is protected. To that end, the purpose of this section is to encourage businesses that own or license personal information about Californians to provide *reasonable* security for that information.") (emphasis added). Accepting Wyndham's arguments that the reasonableness standard in data security fails to provide businesses with adequate fair notice would endanger and undermine these states' deliberate efforts to protect consumers.

III. CONSUMER DATA PROTECTION MUST INVOLVE AN UNFAIRNESS PROVISION BECAUSE NEITHER SELF-REGULATION NOR A RIGIDLY RULE-BASED REGIME IS AN ADEQUATE ALTERNATIVE.

Unfair data security practices harm consumers and competitors. And "[i]t is generally agreed that the core principles of privacy protection can

only be effective if there is a mechanism in place to enforce them." JC Cannon, *Privacy in Technology: Standards and Practices for Engineers and Security and IT Professionals* 2 (International Association of Privacy Professionals 2014). Without the specter of FTC enforcement, companies will fail to adopt reasonable data security protections, as consumers lack the market strength to sufficiently incentivize businesses to appropriately safeguard their data. Regulatory oversight of businesses is therefore critical to prevent unfair data security practices.

As the FTC observes, Wyndham has abandoned its untenable argument that the FTC must formally promulgate rules identifying each prohibited practice before bringing an enforcement action. Appellee's Br. at 52 n.17. However, Wyndham continues to maintain that the FTC must provide, ex ante, highly specific guidance regarding what data security practices are required. Appellant's Br. at 37 (faulting the FTC for failing to specify, among other things, what firewall configurations a business must deploy). Wyndham's revised argument is no less untenable. Static and inflexible ex ante prescriptions would prevent the FTC from effectively adapting its consumer protection efforts to new technologies and to evolving threats. The FTC's power to regulate unfair data security practices is effective *precisely* because Congress has imbued the FTC with the flexibility

to respond to varied and new threats to consumers. It is this flexible power that permits the FTC to find a balance between these two approaches—a laissez-faire market approach and rigid ex ante prescriptions—and to effectively regulate unfair data security practices.

A. The FTC's Ability To Bring Actions Against Businesses That Use Unfair Data Security Practices Ensures That Consumers' Personal Data Is Adequately Protected.

Consumer demands alone cannot sufficiently incentivize businesses to create adequate data security regimes: there must be an "effective 'cop on the beat.'" Lydia B. Parnes & Carol J. Jennings, *Through the Looking Glass: A Perspective on Regulatory Reform at the Federal Trade Commission*, 49 Admin L. Rev. 989, 1003 (1997). Consumers depend on this "cop," here the FTC, to provide the critical enforcement presence. Other traditional methods of enforcement, such as market signaling and private civil lawsuits, have proved ineffective.

In theory, a free marketplace would effectively police insecurity, but real-world barriers, most notably information asymmetries, leave consumers without the ability to properly assess the data security efficacy of businesses. *See* Chris Jay Hoofnagle, *Identity Theft: Making the Known Unknowns Known*, 21 Harv. J.L. & Tech. 97, 100 (2007) ("[P]roviding more accurate, institutional-level statistics on identity theft would make the security of

personal information a new product differentiator . . . ."). Victims of identity theft are rarely able to identify where their sensitive personal data was stolen—if they are even aware of the theft. *Id.* at 99, 105. Thus unable to know who exposed their information, consumers cannot signal their displeasure by withholding their business from companies with lax security. J. Howard Beales III & Timothy J. Muris, *Choice or Consequence: Protecting Privacy in Commercial Information*, 75 U. Chi. L. Rev. 109, 127 (2008).

Not only are consumers poorly positioned to judge the adequacy of a business's security measures ex ante, but also ex post remedies for data security breaches have been elusive. In many other contexts, legislative statutes provide individuals with a private right of action. *E.g.* 15 U.S.C. §§ 1640, 1667d, 1679g, 1681n, 1681o, 1691e, 1692k, 1693m (each creating civil liability for persons who fail to comply with provisions of the Consumer Credit Protection Act, codified at 15 U.S.C. ch. 41). And when small individual harms are visited upon a great number of persons, class certification can allow for remedial action. But in the context of data security, those standard redresses have been found wanting. Courts have been unwilling to hold that individuals whose data has been hacked but who cannot demonstrate that it has been misused have standing. *See, e.g.*, *Reilly*

v. Ceridian Corp., 664 F.3d 38, 41 (3rd Cir. 2011) (rejecting standing on the ground that "allegations of hypothetical, future injury are insufficient to establish standing"). They have also been unwilling to find that potential classes satisfy certification requirements. *See, e.g.*, *In re Hannaford Bros. Co. Customer Data Sec. Breach Litigation*, 293 F.R.D. 21, 33 (D. Me. 2013) (finding that the proposed class failed to meet the predominance requirement of Federal Rule of Civil Procedure 23(b)(3)).

Without realistic threats of market share loss or becoming embroiled in non-regulatory civil litigation, many individual businesses "do not have appropriate incentives to protect the data they possess." Beales & Muris, *supra*, at 126-27. The FTC's authority to bring civil enforcement actions against companies who practice unfair data security helps to remedy that problem. *See Protecting Personal Consumer Information from Cyber Attacks and Data Breaches: Hearing Before the S. Comm. on Commerce, Sci. and Transp.*, 113th Cong. 2 (March 26, 2014) (testimony of Edith Ramirez) ("As the nation's leading privacy enforcement agency, the Commission has undertaken substantial efforts for over a decade to promote data security and privacy in the private sector through civil law enforcement,

education, and policy initiatives.").[8] The FTC uses its consumer unfairness authority as a "flexible tool" to protect consumers by addressing harmful practices that do not comfortably fit under the prohibition against deceptive practices. Tim Muris & Bob Pitofsky, *More that Law Enforcement: The FTC's Many Tools—A Conversation with Tim Muris and Bob Pitofsky*, 72 Antitrust L.J. 773, 800-01 (2005). Removing the FTC's ability to police unfair business practices would remove a "very important part of the FTC's consumer protection authority." *Id.* at 800.

B. Requiring The FTC To Issue Detailed Guidelines Before It Can Act To Protect Consumers From Unfair Data Security Practices Would Leave The FTC Unable To Adjust To New Threats.

Because approaching data security regulation with specific rules and prescriptions risks leaving consumers under-protected and businesses overregulated, regulators have drawn upon reasonableness to fill the void. Especially in a dynamic regulatory arena, such as data security, risk often tips from the combination of multiple factors, and prescriptive regulations will often fail to capture the possible permeations that can shift data security practices from fair and reasonable to unreasonable and unfair. Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the*

[8] *Available at* http://www.ftc.gov/system/files/documents/public_statements/293861/140326datasecurity.pdf

Ground, 63 Stan. L. Rev. 247, 303 (2011). And a static regulatory scheme can encourage a myopic focus on compliance at the expense of consumer protection, thus disengaging the regulatory system from the underlying policy goal of data security regulation: protecting consumers from companies that treat their customers unfairly.

Demanding that the FTC promulgate specific ex ante prescriptions delineating exactly which technical mechanisms a business must install to create "reasonable" and "fair" data security practices inevitably results in a classic Goldilocks' problem. While a hypothetical set of defined best practices may capture the best practices of a few companies, many other companies will find themselves forced to implement unneeded security mechanisms. Still others will find the requirements insufficient to adequately protect their customers' personal data, but will discover the resulting safe-harbor of legal compliance permits them to take the minimum precautions above the baseline demanded by the market. As demonstrated above, these precautions will inevitably be less than "fair" data security would demand.

And given the "rapidly-evolving nature of data security," technical requirements enshrined in static prescriptions will quickly suffer from obsolescence. *FTC v. Wyndham*, 2014 WL 1349019, at *14. Ex ante regulations only reflect contemporary beliefs about how to best achieve the

desired result, and codifying those beliefs into a static rule restricts regulators from adapting to changing circumstances and emerging new threats. Bamberger & Mulligan, *supra*, at 303. Instead, the constant evolution of technology and associated security threats means that security is a process—"[t]here is no silver bullet and no one fix to ensure both privacy and security. Rather, it takes continual education, awareness and the application of appropriate controls in accordance with statute, standards and policies." Cannon, *supra*, at 18.

In sum, it is the very feature of flexibility that gives the FTC the informed discretion to enforce data security standards on behalf of consumers. Neither reliance on industry self-regulation alone nor the issuance of detailed prescriptions would adequately protect consumers' data.

CONCLUSION

For the foregoing reasons, amici EFF and CDT urge this Court to affirm the judgment below.

Respectfully Submitted,

November 12, 2014

/s/ Catherine Crump
Catherine Crump
Chris Jay Hoofnagle
Samuelson Law, Technology & Public Policy Clinic
U.C. Berkeley School of Law
Berkeley, CA 94720-7200
Telephone: (510) 642-1741
ccrump@law.berkeley.edu
choofnagle@law.berkeley.edu

Justin Brookman
G.S. Hans
Center for Democracy & Technology
1634 I Street NW, Suite 1100
Washington, DC, 20006
Telephone: (202) 637-9800
jbrookman@cdt.org
ghans@cdt.org

Lee Tien
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
tien@eff.org

COMBINED CERTIFICATIONS

I hereby certify:

1. I am a member in good standing of the bar for the United States Court of Appeals for the Third Circuit.
2. This brief complies with the typeface requirements of Fed. R. App. P. 29(c) and 32(a)(5) because it has a proportionally spaced 14-point typeface.
3. This brief complies with the type-volume limitations of Fed. R. App. P. 29(d) and 32(a)(7)(B) because it contains 5,440 words, excluding those parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii).
4. The text of the electronically filed brief is identical to the text in the paper copies.
5. A virus detection program (System Center 2012 Endpoint Protection) has scanned the electronic file and no virus was detected.

November 12, 2014 _____/s/ Catherine Crump_____
Catherine Crump

CERTIFICATE OF SERVICE

I certify that on November 12, 2014, the foregoing *amici 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/ Catherine Crump_____

Catherine Crump