ORAL ARGUMENT NOT YET SCHEDULED

No. 19-7020

IN THE UNITED STATES COURT OF APPEALS
FOR THE DISTRICT OF COLUMBIA CIRCUIT

CHANTAL ATTIAS, INDIVIDUALLY AND ON BEHALF OF ALL OTHERS SIMILARLY SITUATED, ET AL.
Plaintiffs-Appellants,

v.

CAREFIRST, INC., ET AL.
Defendants-Appellees.

On appeal from the United States District Court
for the District of Columbia, Case No. 1:15-cv-882 (CRC)
The Honorable Christopher R. Cooper

BRIEF OF *AMICUS CURIAE* ELECTRONIC PRIVACY INFORMATION CENTER (EPIC) IN SUPPORT OF APPELLANTS

MARC ROTENBERG
ALAN BUTLER
MEGAN IORIO
Electronic Privacy Information Center
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140
rotenberg@epic.org
Counsel for Amicus Curiae

July 1, 2019

CERTIFICATE AS TO PARTIES, RULINGS, AND RELATED CASES

Pursuant to D.C. Circuit Rule 28(a)(1), *Amicus Curiae* Electronic Privacy Information Center ("EPIC") certifies that:

A. Parties, Interveners, and Amici

Except for *Amicus Curiae* EPIC, all parties, interveners, and *amici* appearing before the district court and in this Court are set forth in the Brief of Appellants.

B. Ruling under Review

References to the ruling at issue appear in the Brief of Appellants.

C. Related Cases

The instant case was previously presented to this Court in Case No. 16-7108. The Court entered an opinion on August 1, 2017, reversing the lower court's August 10, 2016 order and remanding the case for further proceedings.

CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rule of Appellate Procedure 26.1 and D.C. Circuit Rules 27(a)(4) and 28(a)(1)(A), *Amicus Curiae* EPIC submits the following corporate disclosure statement:

EPIC does not have a parent, subsidiary, or affiliate. EPIC has never issued shares or debt securities to the public.

/s/ Alan Butler
ALAN BUTLER

TABLE OF CONTENTS

TABLE OF AUTHORITIES[1]

Cases

Statutes

[1] Authorities upon which we chiefly rely are marked with a *.

Other Authorities

GLOSSARY

BJS	Bureau of Justice Statistics
DOJ	Department of Justice
EPIC	Electronic Privacy Information Center
FTC	Federal Trade Commission
GAO	Government Accountability Office
OPM	Office of Personnel Management

STATUTES AND REGULATIONS

All applicable statutes, etc., are contained in the Brief for Appellants.

INTEREST OF AMICUS[2]

The Electronic Privacy Information Center ("EPIC")[3] is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and other constitutional values.

EPIC frequently participates as *amicus curiae* in state and federal cases concerning data breaches and consumer privacy protection. *See* Mot. for Leave to File Amicus Br.

EPIC has a particular interest in this case because this is the first time a court of appeals in the District of Columbia will apply state common law and statutory law in a data breach case. Given the growing risk to D.C. consumers of data breach, identity theft, and financial fraud, EPIC has a strong interest in defending consumers' right to seek legal redress. If a company chooses to collect personal data, it should be held liable if it fails to protect that data. Courts should impose a duty of reasonable data protection on businesses and allocate costs to those entities in the best position to reduce the risk of future data breaches. Court should also compensate consumers for the damages that result from a data breach.

---

[2] In accordance with Rule 29, the undersigned states that no monetary contributions were made for the preparation or submission of this brief, and counsel for a party did not author this brief, in whole or in part.

[3] EPIC IPIOP Clerk Sarah Parker participated in the preparation of this brief.

SUMMARY OF ARGUMENT

Millions of consumers suffer every year from identity theft and financial fraud. This problem is especially acute for consumers in the District of Columbia. Washington, D.C. residents have one of the highest per capita rates of identity theft in the country. Fed. Trade Comm'n, *Consumer Sentinel Network Data Book 2018*, at 21 (2019) [hereinafter *FTC Sentinel Data 2018*].[4] Not only have D.C. residents suffered from breaches of their personal data gathered by commercial firms, such as CareFirst, D.C. residents were also subject to the data breaches of the Office of Personnel Management, which compromised the personal data of 22 million federal employees, their families, and friends.

Data breaches nationwide exposed nearly 450 million records in 2018, leading to significant expenditures for an estimated 26 million Americans. Identity Theft Research Ctr., *2018 End-of-Year Data Breach Report* 1 (2019)[5] [hereinafter *2018 Data Breach Report*]; Erika Harrell, Bureau of Justice Statistics, *Victims of Identity Theft, 2016*, at 1 (2019)[6] [hereinafter *BJS Victims of Identity Theft 2016*]. Data breaches cost American consumers approximately $17.5 billion annually

[4] https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2018/consumer_sentinel_network_data_book_2018_0.pdf.
[5] https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf.
[6] https://www.bjs.gov/content/pub/pdf/vit16.pdf.

according to the Department of Justice. *BJS Victims of Identity Theft 2016*, *supra*, at 1.

The time has come for companies to invest in reasonable data security precautions. Many serious breaches can be avoided entirely by implementing established data security procedures or minimizing unnecessary collection and storage of personal information. In the absence of market forces or non-litigation methods to encourage businesses to invest in data security, companies must be incentivized by courts to implement reasonable data security.

If courts do not permit individuals whose personal information has been mishandled and obtained by criminals to pursue redress, the problems of data breach and identity theft will only get worse. Many data breaches are avoidable, and companies that collect and store sensitive information are in the best position to take the reasonable measures necessary to protect the data. Shielding these companies—who have chosen to collect, use, and profit from personal information—from liability removes the incentives to adopt necessary data security measures.

ARGUMENT

The breach at CareFirst, the largest insurance provider in the District of Columbia area, imposed an enormous cost on D.C. residents. Data breaches are one of the largest and most costly threats facing American consumers today, and

the CareFirst breach hit D.C. consumers directly. D.C. residents provided sensitive personal information to CareFirst to obtain medical coverage. They should not be forced to bear the costs of data breach. The businesses that collect and store personal data should implement data security measures to minimize the risk of attack and reduce the harm from a breach. But, absent a legal duty to protect the personal information they collect, companies have failed to implement industry-standard data protection procedures.

The lower court's refusal to recognize a duty to provide reasonable data security wrongfully denies consumers relief when companies fail to protect their personal information. This allows companies to pass the costs of data breaches on to consumers, and leaves companies free to continue business practices that make future data breaches more likely.

Consumers suffer damages from the moment a data breach occurs. Consumers are told (sometimes by the companies who failed to protect their data) that they should pay for prophylactic measures including credit monitoring, identity monitoring, identity restoration, and identity theft insurance to limit the impact of the breach. Consumers also spend a significant amount of time identifying breached accounts, changing passwords, checking for fraudulent transactions, cancelling credit cards, and taking other steps to make sure that they don't become victimized yet again. These steps are all reasonable and necessary to

mitigate the harm caused by the breach. Yet the lower court refused to recognize that these predictable and reasonable mitigation expenditures constitute actual damages.

I. Consumers in the District of Columbia are facing a data breach and identity theft crisis.

A. The breach of the largest insurance provider in D.C. is part of a nationwide epidemic that threatens consumers.

Data breaches are one of the most costly threats facing American consumers today. The threat is urgent, as the D.C. government has already recognized. The D.C. Attorney General Karl A. Racine stated recently, "Data breaches and identify theft continue to pose major threats to District residents and consumers nationwide." Press Release, Office of the Att'y Gen. for the District of Columbia, AG Racine Introduces Legislation to Protect District Residents' Personal Data (March 21, 2019) [hereinafter D.C. OAG Press Release].[7]

The scale of this epidemic is immense. There were 1,244 breaches in 2018, exposing almost 450 million records to risks of identity theft and financial fraud. *2018 Data Breach Report*, *supra*, at 1. In April 2019 alone, there were 146 data breaches, putting over 40 million records at risk. Identity Theft Research Ctr., *Data Breach Reports* 3 (2019).[8] As catalogued by the Government Accountability

[7] https://oag.dc.gov/release/ag-racine-introduces-legislation-protect-district.
[8] https://www.idtheftcenter.org/wp-content/uploads/2019/05/2019-April-Data-Breach-Package.pdf.

Office, the exposure of sensitive personal information lead to harms including: financial, tax refund, and government benefits fraud; medical, synthetic, and child identity theft; and lost time, emotional distress, lost privacy, reputational harm, and harm from state-sponsored espionage. U.S. Gov't Accountability Office, GAO-19-230, *Data Breaches: Range of Consumer Risks Highlights Limitations of Identity Theft Services* 4–6 (2019) [hereinafter *GAO Data Breaches*].[9]

The risk of identity theft is increasing. According to the most recent report by the Department of Justice, an estimated 26 million Americans experience identity theft annually—a 48% increase from DOJ's previous biennial report. *Compare BJS Victims of Identity Theft 2016*, *supra*, at 1, *with* Erika Harrell, Bureau of Justice Statistics, *Victims of Identity Theft, 2014*, at 1 (2015)[10] (finding that an estimated 17.6 million consumers were victims of identity theft in the preceding year). Consumers also filed 445,000 reports of identity theft with the Federal Trade Commission in 2018, a 20% increase from the 370,000 reports filed in 2017. *FTC Sentinel Data 2018*, *supra*, at 4; Fed. Trade Comm'n, *Consumer Sentinel Network Data Book 2017*, at 3 (2018).[11]

[9] https://www.gao.gov/assets/700/697985.pdf.
[10] http://www.bjs.gov/content/pub/pdf/vit14.pdf.
[11] https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2017/consumer_sentinel_data_book_2017.pdf.

Washington, D.C. residents are deeply affected by this national crisis. D.C. consumers report identity theft to the FTC at the fifth highest level per capita in the country, behind Georgia, Nevada, California, and Florida. *FTC Sentinel Data 2018*, *supra*, at 21 (noting 1,156 identity theft reports from the D.C. population). Common forms of identity theft for D.C. residents include credit card, phone, utilities, employment, tax, loan, and lease fraud. *Id.* at 30. According to the FTC, the District of Columbia also ranks number one per capita for "Fraud and Other Reports." *Id.* at 20.

In addition to regional breaches such as the CareFirst breach, D.C. consumers are also affected by national data breaches such as the massive Equifax, Whole Foods, and Marriott breaches. D.C. OAG Press Release, *supra*; Heather Haddon, *Whole Foods Data Breach Affected About 100 Taprooms, Restaurants*, Wall St. J. (Oct. 10, 2017)[12]; Bill Bostock, *All the Hotels Affected by the Marriott Data Breach that Affected 500 Million Consumers*, Bus. Insider (Nov. 30, 2018).[13] In fact, the 2017 Equifax breach exposed the personal information of nearly 350,000—around half of all—D.C. residents. D.C. OAG Press Release, *supra*.

[12] https://www.wsj.com/articles/whole-foods-data-breach-affected-about-100-taprooms-restaurants-1508526726.
[13] https://www.businessinsider.com/marriott-data-breach-which-hotels-affected-2018-11.

D.C. residents have also been impacted by local government data breaches, including the improper disclosure of the Social Security numbers of nurses by the D.C. Department of Health and the exposure of the confidential information of nearly 1,500 households receiving housing assistance by the D.C. Department of Human Services. Fenit Nirappil, *D.C. Government Data Breach Exposed Nurses' Social Security Numbers*, Wash. Post (May 24, 2018)[14]; Martin Austermuhle, *D.C. Mistakenly Disclosed Confidential Information of Homeless Residents To Advocacy Group*, WAMU (Jul. 26, 2017).[15] And D.C. residents were acutely impacted by the massive data breach at the Office of Personnel Management because many D.C. residents are federal government employees. *See In re Office of Personnel Management Data Sec. Breach Litig.*, ___ F.3d ___, No. 17-5217 (D.C. Cir. June 21, 2019).

B. Data breaches impose significant financial costs on D.C. consumers and others.

Data breaches are incredibly costly to District consumers and will remain so until reasonable data precautions are implemented. To give context to the scale of these costs, data breaches cost American consumers more than $17.5 billion dollars

[14] https://www.washingtonpost.com/local/dc-politics/dc-government-data-breach-exposed-nurses-social-security-numbers/2018/05/24/1c63a278-5f62-11e8-a4a4-c070ef53f315_story.html.
[15] https://wamu.org/story/17/07/26/d-c-mistakenly-disclosed-confidential-information-homeless-residents-advocacy-group/.

in 2016 according to the most recent statistics from the Bureau of Justice. *BJS Victims of Identity Theft 2016*, *supra*, at 1.

The costs can quickly balloon for consumers after a data breach. These costs begin with credit monitoring and repair services and can snowball due to identity theft. Staff of Permanent Subcomm. on Investigations of the S. Comm. on Homeland Security and Governmental Affairs, 116th Cong., *How Equifax Neglected Cybersecurity and Suffered a Devastating Data Breach* 1 (2019) [hereinafter *How Equifax Neglected Cybersecurity*] (noting that victims of data breaches "can be left with years of expense and hassle").[16] Data breaches often lead to unauthorized credit card purchases, tax fraud, and fraudulent loans and medical expenditures. *GAO Data Breaches*, *supra*, at 4–6. This in turn destroys victims' credit scores, forces them to pay higher interest rates, prevents them from obtaining loans, leads to their utilities being cut off, and, in extreme cases, forces them to file bankruptcy or lose their homes. On the whole, two-thirds of identity-theft victims reporting a direct financial loss in 2016. *BJS Victims of Identity Theft 2016*, *supra*, at 7. Victims of data breaches also experience heavy emotional costs, from problems with family and friends to severe distress. *Id.* at 10–12.

[16] https://www.hsgac.senate.gov/imo/media/doc/FINAL%20Equifax%20Report.pdf.

While the majority of data breach costs are borne by consumers, data breaches are also costly for businesses. The average total cost of a data breach for organizations globally was $3.86 million in 2018, with an average cost per lost or stolen record of $148. Mary L. Fullington, *Consequences of a Security Breach of PII*, 39 E. Min. L. Found. § 14.04 (2018); Ponemon Institute, *2018 Cost of a Data Breach Study: Global Overview* 3 (2018).[17] While this is a global phenomenon, it affects Americans—including D.C. residents—more than citizens of other countries. Organizations in the United States experience the highest total average cost of a data breach at $7.91 million—$2.6 million higher than the next highest region, the Middle East. *Id.* at 13.

Data breaches are growing more frequent and having more severe consequences in the District and elsewhere in the country, and they will continue to do so if the consumer data crisis continues unchecked. On average, U.S. organizations have a 26.9% chance of experiencing a material data breach in the next two years. *Id.* at 32. The costs of breaches are also increasing year over year. *Id.* at 3 (noting an increase of 6.4% in the cost of data breaches between 2017 and 2018). Furthermore, the urgency of this epidemic has been noted by both this Court and the lower court in this case. *See Attias v. CareFirst, Inc.*, 865 F.3d 620, 628 (D.C. Cir. 2017) (recognizing that the "plaintiffs would face a substantial risk of

[17] https://www.ibm.com/downloads/cas/861MNWN2.

identity theft if their social security and credit card numbers were accessed by a network intruder . . . [based] on 'experience and common sense'"); *Attias v. CareFirst, Inc.*, 199 F. Supp. 3d 193, 196 (D.D.C. 2016) (remarking that "theft of electronic data has become commonplace in our digital economy, victimizing millions of Americans each year").

C. The D.C. Government has identified safeguarding the privacy of D.C. residents as a top priority.

Local officials have identified data protection as a top priority for the District. For example, D.C. Attorney General Karl A. Racine recently introduced a bill designed to modernize D.C.'s data breach law and strengthen protections for residents' personal information. In doing so, he confirmed that, "data breaches and identity theft continue to pose major threats to District residents and consumers nationwide. . . . The District's current data security law does not adequately protect residents." D.C. OAG Press Release, *supra*.

The District government has been committed to addressing data protection for over a decade. Officials first adopted a modernized data policy in 2006 and updated that policy in 2011, 2014, and 2017 after extensive public comment. Robert Bobb, *Executive Memorandum* (Jun. 12, 2006) (identifying the agency responsibility to "identify information that should be designated private on account

of law or other privacy reasons . . .")[18]; Michael Watson, *Diving into D.C.'s Data Policy*, D.C. Policy Center (Aug. 31, 2017).[19] The District's current data policy recognizes the significant risks of data breaches and sets minimum data protection standards in place, noting that, "because inappropriate disclosure of personal information and misuse of data for activities such as identity theft are significant concerns, the District's data must also be managed and responsibly protected." Office of the Mayor, Mayor's Order 2017-115, *District of Columbia Data Policy* (2017).[20]

D. Liability rules should ensure that businesses invest in data protection measures to combat the threat of data breach.

The solution to this growing crisis is simple. If companies choose to collect, use, and profit from consumer data, they need to implement reasonable data security measures to protect that data. Many industry-standard data protection strategies are low-cost or free. Yet businesses continue to fail to implement even the most basic data security precautions. Absent liability, companies will not internalize the costs of poor data security; those costs will be born entirely by consumers.

Reasonable data security precautions can minimize—or even avoid entirely—the high costs of data breaches and identity theft. According to the Department of

[18] https://opendatapolicyhub.sunlightfoundation.com/collection/washington-dc-2006-06-12/.
[19] https://www.dcpolicycenter.org/publications/diving-into-dc-data-policy/.
[20] https://octo.dc.gov/page/district-columbia-data-policy.

Homeland Security's Computer Emergency Readiness Team, as many as 85% of targeted attacks are preventable. Comput. Emergency Readiness Team, TA15-119, *Alert: Top 30 Targeted High Risk Vulnerabilities* (2016).[21] In many cases, attackers gain access because of well-known vulnerabilities or carelessness by the company that collected the data. *See, e.g.*, Office of Pers. Mgmt., Office of the Inspector Gen., 4A-CI-00-18-038, *Final Audit Report: Federal Information Security Modernization Act Audit Fiscal Year 2018*, at 5 (2018)[22] (noting that the OPM Inspector General had "assessed [OPM's information security governance program] to be a material weakness or a significant deficiency in OPM's internal control structure since FY 2007").

In order to avoid these highly preventable attacks, businesses need to invest in data protection and security measures. They should do so by following industry standards. Brief of Amicus Curiae Electronic Privacy Information Center (EPIC) and Thirty-Three Technical Experts and Legal Scholars in Support of Respondent 23–29, *FTC v. Wyndham*, 799 F.3d 236 (3d Cir. 2015) (No. 14-3514) (identifying existing cybersecurity frameworks that provide clear guidance for safeguarding sensitive customer data).

[21] https://www.us-cert.gov/ncas/alerts/TA15-119A.
[22] https://www.opm.gov/our-inspector-general/reports/2015/federal-information-security-modernization-act-audit-fy-2015-final-audit-report-4a-ci-00-15-011.pdf.

The investment required is financially reasonable. Many of these best practices—such as minimizing the unnecessary collection and storage of personal information, implementing established data security procedures, and strengthening organizational procedures to build a culture of security—are easy and low-cost or free. *See, e.g.*, White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Economy* 21 (2012)[23] (stating that companies "should collect only as much personal data as they need to accomplish purposes"); Kroll, *Data Breach Protection Tips* (2015)[24] (advocating employee education "about appropriate handling and protection of sensitive data").

Companies that identify a breach in under 100 days spend an average of $1.1 million less than companies that lack the tools to quickly identify breaches, and firms that contain a breach in less than 30 days save an average of $1.16 million by doing so. Ponemon Institute, *supra*, at 36–37. Implementing security automation also saves companies an average of $1.55 million per data breach. *Id.* at 38. Despite this, many companies still fail to take upfront steps to protect consumer data and prevent breaches—leading to justified criticism after firms unsurprisingly experience breaches. *See, e.g., How Equifax Neglected Cybersecurity*, *supra*.

[23] https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf.
[24] http://www.kroll.com/en-us/cyber-security/data-breach-prevention/cyber-risk-assessments/data-breach-prevention-tips.

II. Courts in the District of Columbia should recognize a duty of reasonable data protection.

This Court has never applied state tort and contract law to a data breach claim. In fact, the D.C. Court of Appeals itself has not had the chance to consider whether state law imposes an affirmative obligation to maintain data security. Given this uncertainty about such an important question of state law, this Court should exercise its discretion to certify the question(s) to the D.C. Court of Appeals pursuant to D.C. Code Ann. § 11-723. *See Owens v. Republic of Sudan*, 864 F.3d 751, 811–12 (D.C. Cir. 2017) (certifying a state tort law question to the D.C. Court of Appeals). The scope of negligence and contract liability for a data breach under state law is clearly "vital to a correct disposition" of this case, and thus is appropriate for certification given the uncertainty. *Id*. at 812 (quoting *Tidler v. Eli Lilly & Co.*, 851 F.2d 418, 426 (D.C. Cir. 1988)). There is ample support for recognition of a duty of reasonable data security based on widely accepted tort law principles.

A. The duty of reasonable data protection is consistent with tort law principles recognized in the District of Columbia.

The duty of reasonable data protection is consistent with common law principles applied in the District of Columbia. While this duty was not specifically

enumerated as one of the original privacy torts[25], these four torts do not preclude the recognition of other duties in privacy cases. Danielle Keats Citron, *Mainstreaming Privacy Torts*, 98 Cal. L. Rev. 1805, 1836 (2010) [hereinafter Citron, *Mainstreaming Privacy Torts*]. Many new types of privacy injuries have emerged over the years that require the adaptation of traditional tort principles to new claims. This is especially true in the data breach context.

The immense scale of harms stemming from data breaches were inconceivable to courts and litigants during the first half of the 20th Century. Just as Prosser reconceived an approach to Warren and Brandeis' privacy torts by "look[ing] to existing law to construct the four privacy torts, courts could look to mainstream tort concepts to tackle contemporary privacy injuries." *Id.* at 1835–36.

As Professor Danielle Citron has explained, there are several ways in which mainstream tort concepts map onto contemporary privacy injuries, creating claims that are "'new wrinkles' on established rules rather than . . . radical changes in law."

---

[25] The privacy tort was first conceived by Samuel Warren and Louis Brandeis in 1890. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193, 195 (1890). Seventy years later, Dean Prosser, following a comprehensive survey of state common law privacy cases, concluded there were in fact four privacy torts, including: (1) unreasonable intrusion upon a person's seclusion; (2) appropriation of someone's name or likeness; (3) unreasonably giving publicity to a person's private life; and (4) publicizing someone in a false light. William L. Prosser, *Handbook of the Law of Torts* 829–42 (3d ed. 1964). Prosser's taxonomy continues to shape modern privacy tort law, but does not preclude other privacy claims.

Id. These include: (1) the use of the strict-liability rule of *Rylands v. Fletcher*, [1868] 3 L.R.E. & I. App. 330, 339–40 (H.L.), to encompass leaks of sensitive personal information, giving companies liability for all data breach damages that are "the natural consequence of [the personal information's] escape;" and (2) the use of the breach of confidence tort to address unwanted disclosures of personal information. Citron, *Mainstreaming Privacy Torts*, *supra*, at 1844–50. Professors Richards and Hartzog have noted also that "While there are antecedents to Protection from common law duties owed by bodyguards (for physical protection) and banks and lawyers (for protection of secrets and money), Protection has taken on particular importance in the digital age." Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 Stan. Tech. L. Rev. 431, 466 (2016).

Courts have followed Professor Citron's approach in recognizing the duty to provide reasonable data security based on established tort doctrines. For example, the Pennsylvania Supreme Court recently held that data collectors have a duty of reasonable data security based on an "application of an existing duty to a novel factual scenario, as opposed to the imposition of a new, affirmative duty." *Dittman v. UPMC*, 196 A.3d 1036, 1046 (Pa. 2018). This follows Prosser's approach of "borrowing from doctrine and focusing on injury prevention and remedy" to create the four enumerated privacy torts. Citron, *Mainstreaming Privacy* Torts, *supra* at 1806. Furthermore, the expansion of this duty mirrors the historic expansion of

torts more broadly, including in the evolution of torts to recognize the increased risk of injury, loss of a chance, and fear of disease.

Other courts have already recognized the duty to provide reasonable data security based on the tort doctrines of negligence, the affirmative duty to refrain from causing others harm, the foreseeability of harm, and the fiduciary duties that apply based on the special relationship between the parties. *See, e.g.*, *In re Sony Gaming Networks & Customer Data Sec. Breach Litig*., 996 F. Supp. 2d 942, 966 (S.D. Cal. 2014); *In re Arby's Restaurant Group, Inc. Litigation*, No. 1:17-cv-514-AT, 2018 WL 2128441, at *4-5 (N.D. Ga. Mar. 5, 2018); *Daly v. Metropolitan Life Insurance Co.*, 782 N.Y.S. 2d 530, 535 (N.Y. Sup. Ct. 2004); *Jones v. Commerce Bancorp, Inc*., No. 06-cv-835-HB, 2006 WL 1409492, at *1–2 (S.D.N.Y. May 23, 2006); *Dittman*, 196 A.3d at 1038; and *Spade v. United States*, 763 F. App'x 294, 296 (3d Cir. 2019) (remanding a case for consideration of *Dittman*'s effect if FECA does not separately bar the claim).

In determining the existence of a duty owed to a plaintiff, D.C. courts have applied a "foreseeability of harm" test, which is based on the recognition that "duty must be limited to avoid liability for unreasonably remote consequences. . . . *Inherent also in the concept of duty is the relationship between the parties out of which the duty arises*." *Hedgepeth v. Whitman Walker Clinic*, 22 A.3d 789, 794 (D.C. 2011) (alteration in original). "Indeed, the [D.C. Court of Appeals] cases

suggest a sliding scale: If the relationship between the parties strongly suggest a duty of protection, then specific evidence of foreseeability is less important, whereas if the relationship is not of a type that entails a duty of protection, then the evidentiary hurdle is higher." *Workman v. United Methodist Comm.*, 320 F.3d 259, 265 (D.C. Cir. 2003).

An additional basis for this duty lies in the fiduciary relationship between CareFirst and its customers. By requiring consumers to provide intimate personal data—and profiting from the collection and storage of this data—CareFirst enters into a relationship of trust and confidence that goes beyond its contractual duties. As Professor Jack Balkin has explained, online service providers who collect, analyze, use, sell, and distribute personal information serve as "information fiduciaries" who should have special duties similar to those of other professional fiduciaries like doctors or lawyers. Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. Davis L. Rev 1183, 1225 (2016). Companies like CareFirst that collect personal data from consumers should thus be treated as fiduciaries and be liable if they do not satisfy their duty to protect the sensitive data that they collect.

Unlike consumers, businesses know where and how the consumer data they have collected is stored. They have direct control over the storage and security of personal information and can prevent data breaches from happening in the first instance. Consumers, on the other hand, cannot directly protect their information

once it has been collected by a business; their control is limited to containing harm if a breach does occur. This places companies in the best position to implement adequate precautions to protect consumer data.

Efficiency is maximized when businesses are incentivized to implement data security precautions. Economic theory dictates that that the party who is in the best position to avoid harm—the least cost avoider—should bear the costs of an accident. Guido Calabresi, *The Costs of Accidents: A Legal And Economic Analysis* 135 (1970) ("A pure market approach to primary accident cost avoidance would require allocation of accident costs to those acts or activities (or combinations of them) which could avoid the accident costs most cheaply."); Ronald Coase, *The Problem of Social Cost*, 3 J. Law & Econ. 1 (1960) (articulating a theory of cost allocation to promote efficient allocations of property resources). Liability rules that hold a least-cost avoider responsible for unreasonable conduct thus create the socially efficient outcome of least consequential harm at least preventative cost.

Correctly identifying the least-cost avoider becomes particularly important where transaction costs are high, as in the case of one party injuring a large and diffuse group of individuals. Calabresi, *supra*, at 135–38; *see* Harold Demsetz, *When Does the Rule of Liability Matter?*, 1 J. Legal. Stud. 13, 27–28 (1972) (arguing that when transaction costs are high, the legal system can "improve the allocation of

resources by placing liability on that party who in the usual situation could be expected to avoid the costly interaction most cheaply").

"Database operators"—such as companies that collect and store consumer data—"constitute the cheapest cost avoiders vis-à-vis individuals whose information sits in a private entity's database." Danielle Keats Citron, *Reservoirs of Danger: the Evolution of Public and Private Law at the Dawn of the Information Age*, 80 Southern Cal. L. Rev. 241, 284 (2007) [hereinafter Citron, *Reservoirs of Danger*] (arguing that data brokers should be strictly liable for unsecure databases and data breaches). A company maintaining databases of consumer data "has exclusive knowledge about, and control over, its information system," giving them "distinct informational advantages about the vulnerabilities in their computer networks" which are critical for effective minimization of threats. *Id.* at 285. These companies have information about how personal data is stored and protected that consumers lack and thus "sit[] in the best position to make decisions about the costs and benefits of its information-gathering" and distribution. *Id.*

Consumers do not have the ability to avoid these breaches because they "have no information about, and have no practical means to find out, where their personal data resides" or how it is protected. *Id.* at 285–86; *see also Understanding Consumer Attitudes About Privacy: Hearing Before the Subcomm. on Commerce, Manufacturing, and Trade of the H. Comm. on Energy & Commerce*, 112th Cong.

102–03 (2011) (statement of Prof. Alessandro Acquisti)[26] ("Research has suggested that US consumers are often ill-informed about the collection and usage of their personal information, and the consequences of those usages. This puts them in a position of asymmetric information, and sometimes disadvantage, relative to the data holders that collect and use that information.").

Even if consumers knew where to look, they "cannot detect and understand the security offered" by database operators. Citron, *Reservoirs of Danger*, *supra*, at 284-85. "Even individuals knowledgeable about information security will find it difficult to assess how well a database system is designed and implemented." *Id.* at 285. And even if consumers did know how to secure their data, "it is unclear what [they] could do if informed about a database operator's vulnerabilities." *Id.*

Unlike the companies, consumers cannot effectively insure against the risk of identity theft. *Id.* Experts have found that identity theft insurance "falls way short" of what consumers need. Priya Anand, *Is Identity-Theft Insurance a Waste of Money?* MarketWatch (Mar. 31, 2014).[27] Unlike car insurance, which covers car damage and personal injuries, identity theft insurance doesn't cover the injuries consumers suffer after their identity is stolen. Nancy Mann Jackson, *Identity Theft*

[26] https://www.gpo.gov/fdsys/pkg/CHRG-112hhrg74605/pdf/CHRG-112hhrg74605.pdf.
[27] http://www.marketwatch.com/story/is-identity-theft-insurance-a-waste-of-money-2014-03-31.

Insurance: How Does It Work and Will It Save Your Good Name?, Bankrate (June 15, 2015).[28] These policies reimburse for certain enumerated costs: phone bills, notary and certified mailing costs, lost wages, or attorney fees. *Id.* However, they fail to reduce the most substantial cost: "the time and hassle required to rectify the situation." *Id.*

A recent report by the Government Accountability Office described the responsibility of entities that hold consumer information to protect that data, citing experts who stated that "the burden should not be on consumers to protect data they do not control." *GAO Data Breaches*, *supra*, at 14. A recent Senate report on the Equifax data breach expressed the same sentiment. *How Equifax Neglected Cybersecurity*, *supra*, at 1 (noting that "a consumer taking appropriate care of this information may not be enough to keep PII out of the hands of criminal hackers" because "businesses collect and compile data about their customers and potential customers").

However, correct allocation of responsibilities does not by itself result in the efficient minimization of harm. If companies are not adequately incentivized to implement adequate data security measures, then consumers will continue to be injured and face devastating downstream harms.

[28] http://www.bankrate.com/finance/insurance/insurance-identity-theft-1.aspx.

B. Imposing a duty of reasonable data protection is necessary to incentivize adequate investment in data security.

Market pressures[29] and regulations alone have not been sufficient to motivate companies to invest in adequate data security. Liability rules are crucial to incentivize mitigation of risk. Given the urgency of the data breach crisis, courts should remove barriers to data security litigation and ensure that companies collecting data bear the costs of data breaches.

Litigation is a commonly used mechanism to incentivize mitigation of risk. *See* Richard A. Posner, *Economic Analysis of Law* 491 (3d ed. 1986) (stating that the legal system determines "what allocation of resources would maximize efficiency" when "the costs of a market determination would exceed those of a legal determination"). Damages force defendants to internalize the full measure of the harm and take sufficient care to prevent future injury. *See Friends of the Earth, Inc. v. Laidlaw Envtl. Serv. (TOC), Inc.*, 528 U.S. 693, 185 (2000) (finding that civil penalties have a deterrent effect and can therefore prevent future injury).

---

[29] The data breach problem cannot be solved through simple market economics. Citron, *Reservoirs of Danger*, *supra*, at 286. Bringing together hundreds of millions of consumers to bargain with every database operator would be prohibitively expensive and logistically impossible. *Id.* "Large consumer blocks also encounter difficulty expressing collectively their relative preferences." *Id.* (internal quotation marks and modifications omitted). These substantial transaction costs counsel towards "imposing liability on the party best able to reduce costs" in order to result "in the most efficient allocation of resources." *Id.* at 286–87 (citing Demsetz, *supra*).

Without court-imposed liability, there is little reason for a company to invest in prevention and mitigation. Companies have no incentive to invest in data protection because the cost of a data breach is minor as compared to their revenue. Examples of this discrepancy of scale include: Sony's 2014 breach cost only 0.9%-2% of their projected sales revenue; Target's major 2013 breach cost the company only 0.1% of their annual sales; and Home Depot's 2014 breach cost less than 0.1% of their annual sales. Benjamin Dean, *Why Companies Have Little Incentive to Invest in Cybersecurity*, The Conversation (March 4, 2015).[30] This disincentivizes the least cost avoider from reasonably protecting personal data, instead creating a market failure in which companies take greater risks because consumers bear the costs of the risks. *Id.*

This misallocation of liability allows companies to profit from consumers' personal information while leaving them to bear the immediate harms and downstream consequences of the company's failure to implement data security. For example, less than five years after the original data breach, CareFirst's customer data was breached again and social security numbers were compromised. CareFirst, *CareFirst Announces "Phishing" Email Incident; 6,800 Members Offered*

[30] http://theconversation.com/why-companies-have-little-incentive-to-invest-in-cybersecurity-37570.

Protection (March 30, 2018).[31] Even as Plaintiffs advocated for reimbursement for their expenditures resulting from the 2014 data breach, CareFirst failed to implement adequate security precautions to prevent additional data breaches from occurring.

As Professor Alessandro Acquisti has explained, rules that impose liability on parties responsible for data breaches serve "as a deterrent for firms by raising their expected costs of engaging in some harmful activity and compensating injured parties for their loss." Alessandro Acquisti & Sasha Romanosky, *Privacy Costs and Personal Data Protection: Economic and Legal Perspectives*, 24 Berkeley Tech. L. J. 1061, 1072 (2009). This simultaneously forces firms to invest in more secure data practices and ensures that privacy harms are adequately compensated.

It is both inefficient and morally wrong for consumers to bear the lion's share of costs from inadequate data security. Forcing victims of data breaches to prove that they suffered specific instances of identity theft connected to a specific data breach imposes an impossible burden on victims. Indeed, with mounting data breaches there may be no way to know *which* breach caused a particular instance of identity theft. *See BJS Victims of Identity Theft 2016*, *supra*, at 7 (finding that only 26% of U.S. identity-theft victims know how their personal information was obtained).

---

[31] https://member.carefirst.com/members/news/media-news/2018/carefirst-announces-phishing-email-incident-6800-members-offered-protection.page.

III. Consumers suffer actual damages when a data breach forces them to pay to prevent, mitigate, or counteract identity theft.

This Court recently explained in *In re: OPM*, ___ F. 3d ___, No. 17-5217 (D.C. Cir. June 21, 2019), that when Plaintiffs allege that hackers have obtained their sensitive personal information and have alleged specific instances of fraud, those allegations "support the inference that [Plaintiffs] face a substantial—as opposed to a merely speculative or theoretical—risk of future identity theft." *Id*., slip op. at 16. "It hardly takes a criminal mastermind to imagine how such information could be used to commit identity theft." *Id*., slip op. at 15. The purchase of "credit protection and/or repair services after learning of [a] data breach" are the "paradigmatic example of 'actual damages' resulting from the violation of privacy protections." *Id.*, slip op. at 32.

The lower court's reliance on *Randolph v. ING Life Ins. and Annuity Co.*, 973 A.2d 702 (D.C. 2009), is misplaced because that case involved the theft of a laptop, not the malicious hacking of sensitive personal information. As other courts have recognized, "there was no evidence [in *Randolph*] that the theft occurred for the specific purpose of obtaining the information on the laptop as opposed to the computer itself." *In re Equifax, Inc., Customer Data Sec. Breach Litig.*, 362 F. Supp. 3d 1295, 1316 (N.D. Ga. 2019).

Paying for mitigation services is the common-sense response to a data breach. The U.S. market for identity theft services was about $3 billion annually from 2015-

2017. *GAO Data Breaches*, *supra*, at 7–8. A recent study found that 98% of victims of identity theft and 84% of non-victims of identity theft took preventative action. *BJS Victims of Identity Theft 2016*, *supra*, at 15. A simple search for "what to do after a data breach" instantly draws consumers to sources which advise prophylactic expenditures. Paul Wagenseil, *What to Do After a Data Breach*, Tom's Guide (Apr. 15, 2019).[32] The Federal Trade Commission's online resources for consumers also enumerate identity theft mitigation options for affected consumers. Fed. Trade Comm'n, Consumer Information, *Identity Theft: A Recovery Plan* (2016).[33] As previously discussed, these mitigation expenditures also make economic sense because early expenditure can sharply decrease the overall costs of a data breach.

Government and expert reports recommend that consumers rely on credit monitoring and other prophylactic services after a data breach, and advise businesses to provide these services to consumers after a breach occurs. For example, the Federal Trade Commission advises businesses experiencing data breaches to "consider offering at least a year of free credit monitoring or other support." Fed. Trade Comm'n, *Data Breach Response: A Guide for Business* 7 (2019).[34] The Department of Homeland Security has also recognized that "[a] mitigation product

[32] https://www.tomsguide.com/us/data-breach-to-dos,news-18007.html.
[33] *Available at* https://www.consumer.ftc.gov/articles/0235-identity-theft-protection-services.
[34] https://www.ftc.gov/system/files/documents/plain-language/pdf-0154_data-breach-response-guide-for-business-042519-508.pdf.

that provides assistance to breach victims can be helpful" during data breaches. Dep't of Homeland Sec., Data Privacy and Integrity Advisory Comm., Report 2017-01, *Best Practices for Notifying Affected Individuals of a Large-Scale Data Breach* (2017).[35] In addition, a recent report from Experian advised businesses that credit monitoring is a "major component of identity protection because it can detect and notify key financial changes." Experian Data Breach Resolution, *Data Breach Response Guide* (2017).[36] State legislatures have even legally mandated this service. *See, e.g.*, H. 4806, 190th Gen. Court, 2017-2018 Sess. (Mass. 2019).[37]

It is notable that this Court found in *In re OPM* that the costs of credit monitoring and repair services constituted "actual damages" under the Privacy Act. *In re OPM*, ___ F.3d, slip op. at 32–35. The Supreme Court has made clear that damages under the Privacy Act are necessarily narrower than in other common law cases because of the doctrine of sovereign immunity. *See Doe v. Chao*, 540 U.S. 614 (2004) (holding that statutory damages are not available under the Privacy Act unless the plaintiff can prove "actual damages"); *FAA v. Cooper*, 566 U.S. 284 (2012) (denying recovery for harm caused by disclosure of HIV status because "actual damages" requires showing current economic harm for Privacy Act

[35] https://www.dhs.gov/sites/default/files/publications/DPIAC%20Recommendations%20Report%202017-01.pdf.
[36] http://www.experian.com/assets/data-breach/white-papers/experian-2017-2018-data-breach-response-guide.pdf.
[37] https://malegislature.gov/Laws/SessionLaws/Acts/2018/Chapter444.

claims); *see also* M. Ryan Calo, *Privacy Harm Exceptionalism*, 12 Co. Tech. L. J. 361, 361–63 (2014) (discussing the heightened standard for proof of harm that courts have previously applied in privacy cases).

* * *

In order to combat the growing data breach crisis, courts should recognize that any company collecting personal information has a duty to protect the data that they collect, and they should be held liable when they fail to do so. Courts should not dismiss data breach claims where plaintiffs allege that hackers have obtained their sensitive personal information, fraud has occurred, plaintiffs have incurred reasonable mitigation expenses, and defendants have failed to take reasonable measures to safeguard the personal data they chose to collect.

CONCLUSION

For the reasons explained above, *Amicus* respectfully requests this Court to reverse the judgment of the district court.

Respectfully submitted,

/s/ Marc Rotenberg
MARC ROTENBERG
ALAN BUTLER
MEGAN IORIO
Electronic Privacy Information Center
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140
rotenberg@epic.org

Dated: July 1, 2019

CERTIFICATE OF COMPLIANCE

I hereby certify that the foregoing brief complies with the typeface requirements of Federal Rule of Appellate Procedure 32(a)(5) and the type-style requirements of Federal Rule of Appellate Procedure 32(a)(6). The brief is composed in a 14-point proportional typeface, Times New Roman, and complies with the word limit of Federal Rule of Appellate Procedure 32(a)(7)(B) and D.C. Circuit Rule 32(e) because it contains 6,493 words, excluding the parts of the brief exempted under Federal Rule of Appellate Procedure 32(a)(7)(B)(iii) and D.C. Circuit Rule 32(e)(1).

/s/ Alan Butler
ALAN BUTLER

CERTIFICATE OF SERVICE

The undersigned counsel certifies that on this 1st day of July 2019, he caused the foregoing "Brief of *Amicus Curiae* Electronic Privacy Information Center (EPIC) in Support of Appellants" to be electronically filed using the Court's CM/ECF system, which served a copy of the document on all counsel of record in this case.

/s/ Alan Butler
ALAN BUTLER