ORAL ARGUMENT NOT YET SCHEDULED

Nos. 17-5217 & 17-5232 (Consolidated)

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

IN RE: U.S. OFFICE OF PERSONNEL MANAGEMENT
DATA SECURITY BREACH LITIGATION

On appeal from the United States District Court
for the District of Columbia, Case No. 15-1394 (ABJ)
The Honorable Amy Berman Jackson

BRIEF OF *AMICI CURIAE* ELECTRONIC PRIVACY INFORMATION CENTER (EPIC) AND FORTY-FOUR LEGAL SCHOLARS AND TECHNICAL EXPERTS IN SUPPORT OF APPELLANTS

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

May 17, 2018

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

All parties, interveners, and *amici* appearing before the district court and in this Court are set forth in the Brief for Appellants National Treasury Employees Union et al. EPIC previously filed a Corporate Disclosure Statement pursuant to Fed. R. App. P. 26.1 and D.C. Cir. Rules 27(a)(4) and 28(a)(1)(A) in its Notice of Intent to File.

B. Ruling under Review

References to the ruling at issue appear in the Brief for Appellants National Treasury Employees Union et al.

C. Related Cases

The cases on review has not previously been before this Court or any other court. EPIC is not aware of any related cases as defined by D.C. Circuit Rule 28(a)(1)(C).

TABLE OF CONTENTS

TABLE OF AUTHORITIES[1]

Cases

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

Statutes

Other Authorities

Constitutional Provisions

GLOSSARY

AFGE	American Federation of Government Employees
EPIC	Electronic Privacy Information Center
NTEU	National Treasury Employees Union
OPM	Office of Personnel Management
PII	Personally identifiable information
SSN	Social Security Number

STATUTES AND REGULATIONS

All applicable statutes, etc., are contained in the Brief for Appellants National Treasury Employees Union et al.

INTEREST OF AMICI[2]

The Electronic Privacy Information Center ("EPIC") 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 federal courts in cases about emerging privacy issues. *See* Notice by EPIC of Intent to File Amicus Br. in Support of Plaintiff-Appellants.

EPIC has a particular interest in the OPM data breach case because it is the first time this Court has considered the claim of informational privacy since its decision in *AFGE v. HUD*, 118 F.3d 786 (D.C. Cir. 1997). Much has happened in the years since, including the Supreme Court's mistaken reliance on the Privacy Act to safeguard personal data in *NASA v. Nelson*, 562 U.S. 134 (2011). Given the growing risk to Americans of data breach, identity theft, and financial fraud, EPIC seeks to protect the constitutional right to informational privacy and to defend the ability of individuals to seek legal redress after data breaches result. When personal data is collected by a government agency, that agency has a constitutional obligation to protect the personal data it has obtained. And if the government or a private company violates its obligation to safeguard that data, individuals should

[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.

be able to seek redress. EPIC's brief is joined by the following experts in privacy law and technology.

Legal Scholars and Technical Experts

Anita L. Allen
Henry R. Silverman Professor of Law and Philosophy, Vice Provost, University of Pennsylvania Law School

Alessandro Acquisti
Professor, Carnegie Mellon University

James Bamford
Author and Journalist

Ann M. Bartow
Director, Franklin Pierce Center for Intellectual Property and Professor of Law, University of New Hampshire School of Law

Francesca Bignami
Professor of Law, The George Washington University Law School

Christine L. Borgman
Distinguished Professor & Presidential Chair in Information Studies, UCLA

Ryan Calo
Lane Powell and D. Wayne Gittinger Associate Professor, University of Washington School of Law

Danielle Keats Citron
Morton & Sophia Macht Professor of Law, University of Maryland Francis King Carey School of Law

Julie E. Cohen
Mark Claster Mamolen Professor of Law and Technology, Georgetown Law

Simon Davies
Publisher, the Privacy Surgeon, Fellow of the University of Amsterdam, Founder of Privacy International and EPIC Senior Fellow

Dr. Whitfield Diffie

Laura K. Donohue
Professor of Law, Director of The Center for National Security and the Law, Georgetown University Law Center

Cynthia Dwork
Gordon McKay Professor of Computer Science, Harvard Radcliffe Alumnae Professor, Radcliffe Institute for Advanced Study

David J. Farber
Adjunct Professor of Internet Studies, Carnegie Mellon University

Addison Fischer
Founder and Chairman, Fischer International Corp.

Hon. David Flaherty
Former Information and Privacy Commissioner for British Columbia

A. Michael Froomkin,
Laurie Silvers & Mitchell Rubenstein Distinguished Professor of Law, University of Miami School of Law

Woodrow Hertzog
Professor of Law and Computer Science, Northeastern Univ. School of Law

Deborah Hurley
Harvard University and Brown University

Joichi Ito
Director, MIT Media Lab

Jerry Kang
Korea Times—Hankook Ilbo Chair in Korean Am. Studies and Law, UCLA

Chris Larsen
Executive Chairman, Ripple Inc.

Harry R. Lewis
Gordon McKay Professor of Computer Science, Harvard University

Anna Lysyanskaya
Professor of Computer Science, Brown University

Gary T. Marx
Professor Emeritus of Sociology, MIT

Mary Minow
Library Law Consultant

Eben Moglen
Professor of Law, Columbia Law School

Dr. Pablo Garcia Molina
Adjunct Professor, Georgetown University

Erin Murphy
Professor of Law, NYU School of Law

Dr. Peter G. Neumann
Chief Scientist, SRI International Computer Science Lab

Helen Nissenbaum
Professor, Cornell Tech Information Science

Frank Pasquale
Professor of Law, Univ. of Maryland Francis King Carey School of Law

Deborah C. Peel, M.D.
President of Patient Privacy Rights

Dr. Stephanie Perrin
President, Digital Discretion, Inc.

Anita Ramasastry
Professor, University of Washington School of Law

Ronald L. Rivest
Institute Professor of Electrical Engineering and Computer Science, MIT

Bruce Schneier
Fellow and Lecturer, Harvard Kennedy School

Dr. Barbara Simons
IBM Research (retired)

Robert Ellis Smith
Publisher, Privacy Journal

Nadine Strossen
John Marshall Harlan II Professor of Law, New York Law School

Frank Tuerkheimer
Professor of Law Emeritus, University of Wisconsin Law School

Edward G. Viltz
President and Chairman, Internet Collaboration Coalition

Jim Waldo
Gordon McKay Professor of the Practice of Computer Science, John A. Paulson School of Engineering and Applied Sciences

Christopher Wolf
Board Chair, Future of Privacy Forum

(Affiliations are for identification only)

SUMMARY OF ARGUMENT

This case concerns the most significant data breach in the history of the United States government. The personal data of approximately 22 million government employees, their friends, and family members were disclosed without authorization. The records breached included the Standard Form 86, completed by those seeking national security positions, and over five million digitized fingerprints, collected precisely for the purpose of authenticating identity. The risks of identity theft, financial fraud, and extortion have increased significantly. The breach occurred just a few years after the Supreme Court mistakenly concluded in *NASA v. Nelson*, 562 U.S. 134 (2011), that the federal Privacy Act, 5 U.S.C. § 552a, sufficiently protected the personal information of federal employees.

Two constitutional questions are presented in this case. The first is whether the Constitution provides a basis to sue a federal agency that fails to safeguard personal data. The second is whether violating an obligation to safeguard personal data provides standing under Article III. EPIC urges this Court to answer both questions in the affirmative.

ARGUMENT

Before this Court is a case of extraordinary gravity. The personal data of the federal workforce has been compromised. The most sensitive details of employees

in national security agencies likely sit in the hands of foreign adversaries. The digital fingerprints of five million individuals, collected to improve authentication and now breached, pose a lifetime risk of identity theft. It may take years to assess the consequences of the breaches that occurred at the Office of Personnel Management. In *Whalen*, *Nixon*, and *Nelson*, the Supreme Court clarified that the Constitution protects a right to information privacy, but it left the scope of that right unresolved for prudential reasons. Those reasons no longer hold. The responsibility to answer the constitutional question now falls to this Court.

The Court should also reaffirm that Article III standing is well established for plaintiffs whose sensitive personal data has been breached. The lower court misapplied both *CareFirst* and *Spokeo.* The court also failed to understand that Social Security Numbers are routinely used by criminals to commit identity theft and financial fraud. The unauthorized disclosure of an individual's SSN is both a concrete and particularized injury, and therefore is reviewable under *Spokeo*.

I. This Court should make clear the right to informational privacy safeguards the personal data held by federal agencies.

A. After *Whalen*, *Nixon*, and *Nelson*, it is well recognized that the Constitution protects the right to informational privacy.

The Supreme Court has long recognized that individuals have a constitutionally protected interest in "avoiding disclosure of personal matters," *Whalen v. Roe*, 429 U.S. 589, 599 (1977); *see also NASA v. Nelson*, 562 U.S. at

147 ("As was our approach in *Whalen*, we will assume for present purposes that the Government's challenged inquiries implicate a privacy interest of constitutional significance."); *Nixon v. Adm'r of Gen. Servs.*, 433 U.S. 425, 455 (1977) ("[W]hen Government intervention is at stake [individuals] are not wholly without constitutionally protected privacy rights in matters of personal life unrelated to any acts done by them in their public capacity."). The right to informational privacy is "implicit in the concept of ordered liberty" that arises under the Fourteenth Amendment. *Whalen*, 429 U.S. at 599 n.23 (internal citations omitted). Both *Whalen* (prescription drug records) and *Nelson* (employment records) presented cases that specifically concerned government agencies' collection and use of personal data. And now before this Court is the breach of 22 million personnel records from a government agency.

Determining the scope of the right requires balancing the potential intrusion on privacy against the public interest served by the data's collection and retention. *See Nixon*, 433 U.S. at 458. As the Court explained, however, prudential considerations may counsel against conducting that inquiry where an applicable statutory regime provides adequate safeguards to protect the privacy interests at stake. *See Whalen*, 429 U.S. at 605–06; *see also Nixon*, 433 U.S. at 458–59.

Since *Whalen* and *Nixon*, many federal courts have recognized the right to informational privacy.[3] Twenty years ago, this Court acknowledged the broad support across the federal judiciary for the right, noting that:

> [S]everal of our sister circuits have concluded based on *Whalen* and *Nixon* that there is a constitutional right to privacy in the nondisclosure of personal information. *See United States v. Westinghouse Electric Corp.*, 638 F.2d 570, 577-580 (3d Cir. 1980) (holding that there is a constitutional right to privacy of medical records kept by an employer, but that the government's interest in protecting the safety of employees was sufficient to permit their examination); *Plante v. Gonzales*, 575 F.2d 1119, 1132, 1134 (5th Cir. 1978), *cert. denied*, 439 U.S. 1129 (1979) (identifying a "right to confidentiality" and holding that balancing is necessary to weigh intrusions); *Barry v. City of New York*, 712 F.2d 1154, 1559 (2d Cir. 1983), *cert denied*, 464 U.S. 1017 (1983) (applying an intermediate standard of review to uphold a financial disclosure requirement). *See also, Hawaii Psychiatric Soc'y Dist. Branch v. Ariyoshi*, 481 F. Supp. 1028, 1043 (D. Hawaii 1979) (holding

[3] *Doe v. City of N.Y.*, 15 F.3d 264, 267 (2d Cir. 1994) (HIV status); *Hancock v. County of Rensselaer*, 882 F.3d 58, 65 (2d Cir. 2018) (medical records); *Matson v. Bd. of Educ. of City Sch. Dist. of N.Y.*, 631 F.3d 57, 63–64 (2d Cir. 2011) (serious medical condition); *United States v. Westinghouse Electric Corp.*, 638 F.2d 570 (3d Cir. 1980) (personal information and decisional privacy); *Fraternal Order of Police, Lodge No. 5 v. City of Philadelphia*, 812 F.2d 105 (3d Cir. 1987) (collection of medical history, gambling habits, alcohol consumption, financial status, memberships, and arrest records); *Doe v. Luzerne Cnty.*, 660 F.3d 169 (3d Cir. 2011) (sensitive images of the body); *Taylor v. Best*, 746 F.2d 220, 225 (4th Cir. 1984) (disclosure of personal matters); *Plante v. Gonzalez*, 575 F.2d 1119 (5th Cir. 1978) (personal financial information); *Pesce v. J. Sterling Morton High School, Dist. 201, Cook Cnty., Ill.*, 830 F.2d 789, 795–98 (7th Cir. 1987) (confidential private information); *Wade v. Goodwin*, 843 F.2d 1150, 1153 (8th Cir. 1988) (same); *Grummett v. Rushen*, 779 F.2d 491, 493–95 (9th Cir. 1985) (shielding naked body from public view); *A.L.A. v. West Valley City*, 26 F.3d 989, 990 (10th Cir. 1994) (confidential medical information); *Hester v. City of Milledgeville*, 777 F.2d 1492, 1497 (11th Cir. 1985) (compelled polygraph testing); *Borucki v. Ryan*, 827 F.2d 836, 839–49 (1st Cir. 1987) (psychiatric report); *U.S. Citizens Ass'n v. Sebelius*, 705 F.3d 588, 602 (6th Cir. 2013) (health information).

> that disclosure of psychiatric records implicates the constitutional right to confidentiality); *McKenna v. Fargo*, 451 F. Supp. 1355, 1381 (D.N.J. 1978) ("The analysis in Whalen . . . compels the conclusion that the defendant . . . must justify the burden imposed on the constitutional right of privacy by the required psychological evaluations.").

AFGE v. HUD, 118 F.3d 786, 792 (D.C. Cir. 1997). However, at the time, this Court declined to "enter the fray by concluding that there is no such constitutional right because in this case that conclusion is unnecessary." *Id.* at 793.

Since this Court's decision in *AFGE*, however, much has changed. There has been a dramatic rise in data breaches. The federal Privacy Act has failed to provide meaningful protection. Meanwhile, state courts, foreign courts, and scholars have reached a broad consensus on the significance of the right to informational privacy in modern society.

B. The Privacy Act does not adequately protect personal data collected by the government.

In *Whalen*, Justice Brennan warned, "The central storage and easy accessibility of computerized data vastly increase the potential for abuse of that information, and I am not prepared to say that future developments will not demonstrate the necessity of some curb on such technology." 429 U.S. at 607 (Brennan, J., concurring). Justice Brennan was persuaded that—given the "successful effort to prevent abuse and limit access to the personal information at issue" in the mid-1970s—computer storage of personal data did not amount to a "deprivation of constitutionally protected privacy interests . . . ." *Id.* Over time,

however, the sensitivity and vulnerability of data gathered by federal agencies has increased dramatically, while the protections afforded by the Privacy Act have not kept pace. The OPM data breach provides extraordinary evidence of this singular fact.

In the years since *AFGE* was decided, federal government data collection has expanded exponentially and much of the data collected includes extremely sensitive personal information. For example, the OPM breach included information in the SF-86, a 127-page form completed by every federal job applicant applying for a security clearance. This form requires the applicant to provide:

> psychological and emotional health history, policy records, illicit drug and alcohol use history, Social Security numbers, birthdates, financial histories and investment records, children's and relatives' names, foreign trips taken and contacts with foreign nationals, past residences, names of neighbors and close friends (such as college roommates and co-workers), and the Social Security numbers and birthdates of spouses, children, and other cohabitants.

JA 397.

Over the same period, the frequency and severity of data breaches also have grown. In *NASA v. Nelson*, the Supreme Court wrongly assumed that the Privacy Act provides sufficient protections such that it was unnecessary to reach the constitutional question. *See* 562 U.S. at 159. The Court may well have regretted that decision as both NASA and the federal government experienced numerous data breaches almost immediately afterword. In 2012, there was a breach of personally

identifiable information (PII) of approximately 2,300 NASA employees and students. Irene Klotz, *Laptop with NASA Workers' Personal Data is Stolen*, Reuters (Nov. 15, 2012).[4] NASA's Inspector General also acknowledged in 2012 that hackers had gained access to agency systems and the personal information of many NASA employees and contractors in 2011. *NASA Cybersecurity: An Examination of the Agency's Information Security: Hearing Before the Subcomm. on Investigations & Oversight of the H. Comm. on Science, Space, & Tech.*, 112th Cong. 5 (2012) (testimony of Paul K. Martin, Inspector Gen., Nat'l Aeronautics and Space Admin.).[5]

Breaches across other federal agencies also have been widely reported since *Nelson*. *See, e.g.*, Alan Rappeport, *Up to 100,000 Taxpayers Compromised in*

---

[4] https://www.reuters.com/article/us-space-nasa-security-idUSBRE8AE05F20121115.

[5] NASA's Inspector General testified:

> NASA reported 5,408 computer security incidents that resulted in the installation of malicious software or unauthorized access to its systems. These incidents spanned a wide continuum from individuals testing their skill to break into NASA systems, to well-organized criminal enterprises hacking for profit, to intrusions that may have been sponsored by foreign intelligence services seeking to further their countries' objectives. Some of these intrusions have affected thousands of NASA computers, caused significant disruption to mission operations, and resulted in the theft of export-controlled and otherwise sensitive data, with an estimated cost to NASA of more than $7 million.

Id.

Fafsa Tool Breach, I.R.S. Says, N.Y. Times (Apr. 6, 2017);[6] Lily Hay Newman, *All the Ways US Government Cybersecurity Falls Flat*, Wired (Aug. 24, 2017);[7] Chief of Naval Personnel Public Affairs, U.S. Navy, *Security Breach Notification of Sailors' PII*, No. NNS161123-13 (Nov. 23, 2016);[8] *see also* U.S. Gov't Accountability Office, GAO-14-478T *Federal Agencies Need to Enhance Responses to Data Breaches* (Apr. 2, 2014).[9] And this case presents to this Court the most significant breach of personal data in the history of the United States government.

Even the year after the OPM breach, in 2016, government agencies reported 30,899 information security incidents, 16 of which met the threshold for being considered a major incident. *Cybersecurity: Actions Needed to Strengthen U.S. Capabilities: Hearing Before the Subcomm. on Research & Tech. of the H. Comm. on Science, Space, & Tech.*, 115th Cong. (2017) (testimony of Gregory C. Wilshusen, Dir., Info. Sec. Issues, U.S. Gov't Accountability Office) [hereinafter Wilshusen Testimony].[10] In none of these instances did the Privacy Act prevent the unwarranted disclosure of personal information.

---

[6] https://www.nytimes.com/2017/04/06/us/politics/internal-revenue-service-breach-taxpayer-data.html.
[7] https://www.wired.com/story/us-government-cybersecurity.
[8] http://www.navy.mil/submit/display.asp?story_id=97820.
[9] https://www.gao.gov/products/GAO-14-487T.
[10] http://www.gao.gov/assets/690/682756.pdf.

According to one report, the federal government experienced a twenty percent increase in the number of data breaches in the last year alone. Thales, *Data Threat Report, Trends in Encryption and Data Security* 6 (2018).[11] In 2017, 57 percent of federal respondents experienced a data breach, up from 34 percent in 2016. *Id.* at 14. The most recent report issued by the White House found that "71 of 96 agencies (74 percent) participating in the risk assessment process have cybersecurity programs that are either at risk or high risk." Office of Mgmt. & Budget, *Federal Cybersecurity Risk Determination Report and Action Plan* 3 (2018);[12] *See also* Wilshusen Testimony, *supra* ("GAO has consistently identified shortcomings in the federal government's approach to ensuring the security of federal information systems and cyber critical infrastructure as well as its approach to protecting the privacy of personally identifiable information (PII)"). As government databases continue to expand, this problem will only get worse.

This Court now confronts the same issue that was before the Supreme Court more than 40 years ago—how to protect individuals given the federal government's increasing collection and retention of personal data. Today, the personal data stored by federal agencies is also subject to attack by foreign

[11] http://go.thalesesecurity.com/rs/480-LWA-970/images/2018-Data-Threat-Report-Global-Edition-ar.pdf.
[12] https://www.whitehouse.gov/wp-content/uploads/2018/05/Cybersecurity-Risk-Determination-Report-FINAL_May-2018-Release.pdf.

adversaries, a scenario that was unimaginable when the Privacy Act was enacted. And although the law affords remedies to citizens, the Supreme Court has limited the Act's remedial provisions. *See Doe v. Chao*, 540 U.S. 614 (2004) (holding that statutory damages are not available 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). Now federal agencies that collect personal information lack both adequate guidance on necessary security precautions and adequate incentive to develop such guidance on their own.

In sum, much has changed in the collection and use of personal data by federal agencies. The threats to the security of personal data collected by the government increase daily, and the law has failed to keep up. This Court should carry forward the right established by the Supreme Court in *Whalen*, *Nixon*, and *Nelson* and should find that right implicated by the government's failure to adequately safeguard the personal data at issue in this case.

C. There is widespread consensus on the importance and scope of the fundamental right to informational privacy.

Long before *Whalen* and *Nixon*, Samuel Warren and Louis Brandeis described the foundation of privacy as rights not "arising from contract or from special trust, but [r]ights as against the world." Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193, 213 (1890). Since the publication of

that seminal article, the right to privacy has been broadly adopted in international declarations and enshrined in constitutions in the United States and around the world.

> As privacy experts Simon Davies and David Banisar explain:
>
> > Privacy is a fundamental human right recognized in the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and in many other international and regional treaties. Privacy underpins human dignity and other values such as freedom of association and freedom of speech. It has become one of the most important human rights issues of the modern age . . .

David Banisar & Simon Davies, *Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments*, 18 Marshall. J. Computer & Info. L. 1, 3 (1999).

Numerous state constitutions explicitly recognize the fundamental right to privacy. For example, the Constitution of Hawaii states, "The right of the people to privacy is recognized and shall not be infringed without the showing of a compelling state interest." Ha. Const. art. I, § 6. *See also*, Ak. Const. art. I, § 22 ("The right of the people to privacy is recognized and shall not be infringed."); Ar. Const. art. II, § 2 ("All men are created equally free and independent, and have certain inherent and inalienable rights; amongst which are those of . . . . protecting property, and reputation . . ."); Ca. Const. art. I, § 1 ("All people are by nature free and independent and have inalienable rights" such as "privacy"); Fl. Const. art. I, § 23 ("Every natural person has the right to be let alone and free from governmental

intrusion into the person's private life . . ."); Ill. Const. art. I, § 6 ("The people shall have the right to be secure in their persons, houses, papers and other possessions against unreasonable searches, seizures, invasions of privacy or interceptions of communications . . ."); La. Const. art. I, § 5 (Every person shall be secure in his person, property, communications, houses, papers, and effects against unreasonable searches, seizures, or invasion of privacy."); Ma. Const. art. II, § 10 ("The right of individual privacy is essential to the well-being of a free society and shall not be infringed without the showing of a compelling state interest."); Pa. Const. art. I, § 1 ("All men are born equally free and independent, and have certain inherent and indefeasible rights, among which are . . . protecting property and reputation . . ."); SC Const. art. I, § 10 ("The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures and unreasonable invasion of privacy shall not be violated . . .").

Courts outside of the United States have also recognized the right to informational privacy. The *Whalen* decision was followed shortly after by a decision of the German Constitutional Court in *Census* which established *informationelle Selbstbestimmung***,** the "right of informational self-determination." *In re: Census Act*, 30 BVerfGE 1, 42-43 (Dec. 15, 1983). This right to informational self-determination, as set out by the German court, is two-fold: (1) it "protects the individual from borderless collection, storage, application, and

transmission of personal data" and (2) "prevents any processing of personal data that leads to an inspection of or an influence upon a person that is capable of destroying an individual capacity for self-governance." Paul Schwartz, *The Computer in German and American Constitutional Law: Toward an American Right of Informational Self-Determination*, 37 Am. J. Comp. L. 675, 689–90 (1989). The *Census* case "compels the State to organize data processing so that personal autonomy will be respected." *Id.* at 690

The Supreme Court decision in *Whalen* and the decision of the German Constitutional court in *Census* influenced international privacy jurisprudence, resulting in the widespread recognition of the right to informational privacy. As Professor Bignami has explained, the right "has spread to virtually every corner of European governance." Francesca Bignami, *The Case of Tolerant Constitutional Patriotism: The Right to Privacy Before the European Courts*, 41 Cornell Int'l L.J. 211, 248 (2008). Privacy is protected under Article 7 of the European Charter of Fundamental Rights and the right to personal data protection is recognized under Article 8 of the European Charter of Fundamental Rights. Both the European Court of Human Rights (ECtHR) and the Court of Justice of the European Union (CJEU) have also recognized the right to privacy under Article 8 of the European Convention of Human Rights. *See, e.g., Amann v. Switzerland*, 30 Eur. Ct. H.R. 843, 858 (2000). "The constitutional frame has shaped both the jurisprudence of

other constitutional courts—in particular the European Courts of Human Rights and the Court of Justice of the European Union—as well as positive lawmaking in Germany and at the European level." Francesca Bignami & Giorgio Resta, *Transatlantic Privacy Regulation: Conflict and Cooperation*, 78 L. & Contemporary Problems 231, 233 (2015).

Most recently, in 2017, the Supreme Court of India unanimously recognized a right to informational privacy under Article 21 of the Indian constitution. *Puttaswamy v. Union of India*, Writ Petition (Civil) No. 494 of 2012 (India) (Aug. 7, 2017).[13] The high court of India found that the right was rooted in the right to life and liberty and also enshrined in other fundamental rights, including the right to equality and the fundamental freedoms. *Id.* Justice Chandrachud emphasized, "The best decisions on how life should be lived are entrusted to the individual . . . . The duty of the state is to safeguard the ability to take decisions—the autonomy of the individual—and not to dictate those decisions." *Id.*; *see also* Jayna Kothari, *The Indian Supreme Court Declares the Constitutional Right to Privacy*, Oxford Human Rights Hub (Oct. 4, 2017);[14] Emma Claybrook, *After the Groundbreaking Supreme Court Decision in India to Make Privacy a Fundamental Human Right,*

---

[13] *Available at* https://supremecourtofindia.nic.in/pdf/jud/ALL%20WP(C)%20No.494%20of%202012%20Right%20to%20Privacy.pdf.

[14] http://ohrh.law.ox.ac.uk/the-indian-supreme-court-declares-the-constitutional-right-to-privacy/.

How Can the World Follow Suit?, New Europe (Feb. 7, 2018) (quoting Malavika Jayaram, stating "[o]ne of the great things about this judgment is showing that privacy is a right that less wealthy countries are allowed to have.").[15]

There is widespread consensus among scholars and courts that the fundamental right to privacy protects several vitally important personal and societal interests. International privacy expert David Flaherty has explained:

> The ultimate protection for the individual is the constitutional entrenchment of rights to privacy and data protection. One can make a strong argument, even in the context of primarily seeking to promote data protection, that having an explicit entrenched constitutional right to personal privacy is a desirable goal in any Western society that has a written constitution and a bill of rights.

David H. Flaherty, *Protecting Privacy in Surveillance Societies* 376 (1998) (internal citations omitted).

Professor Jerry Kang has described the personal interests that the right protects. *See* Jerry Kang, *Info. Privacy in Cyberspace Transactions*, 50 Stan. L. Rev. 1193, 1212–18, 1260 (1998). First, informational privacy helps individuals avoid the embarrassment that accompanies the disclosure of certain personal details. *Id.* Second, as Professor Kang explains, "an individual's capacity to disclose personal information selectively also supports her ability to modulate intimacy." *Id.* at 1212. Third, informational privacy helps individuals avoid

[15] https://www.neweurope.eu/article/india-could-become-data-protection-leader-after-supreme-court-ruling-establishes-right-to-privacy/.

damaging misuse of information that may unnecessarily expose them to prejudice. *Id.* at 1214. Fourth, informational privacy helps to preserve human dignity. *Id.* Finally, "information privacy allows one to have thoughts, beliefs, conditions, and behaviors without the knowledge of others, thereby making it easier to have public personae distinct from private ones." *Id.* at 1218. *See also* Jeffrey Rosen, *Why Privacy Matters*, Wilson Q., Autumn 2000, at 38 ("we are beginning to learn how much may be lost in a culture of transparency: the capacity for creativity and eccentricity, for the development of self and soul, for understanding, friendship, even love."); Anita L. Allen, *Coercing Privacy*, 40 Wm. & Mary L. Rev. 723, 756 (1999) ("There is both empirical evidence and normative philosophical argument supporting the proposition that paradigmatic forms of privacy (e.g., seclusion, solitude, confidentiality, secrecy, anonymity) are vital to well-being.").

Privacy also serves important societal interests. As Professor Julie E. Cohen has written, "Informational privacy is an essential building block for the kind of individuality, and the kind of society, that we say we value." Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 Stan. L. Rev. 1373, 1435 (2000). As Professor Cohen explains, "the liberal self and the liberal democratic society are symbiotic ideals. Their inevitably partial, imperfect realization requires habits of mind, of discourse, and of self-restraint that must be learned. Those are the very same habits that support a mature, critical subjectivity,

and they require privacy to form." Julie E. Cohen, *What Privacy Is For*, 126 Harv. L. Rev. 1904, 1918 (2013); s*ee also* Robert Ellis Smith, *Our Vanishing Privacy and What You Can Do to Protect Yours* 4 (1993) ("Privacy is vital to our national life. Otherwise our culture is debased, belittled, and perverted. It is equally crucial to the lives of each one of us.").

There is widespread consensus that the fundamental right to privacy has a broad temporal scope. The right covers the collection of personal data, along with the disclosure of that data. As Professor Khiara Bridges explains:

> [M]any times, individuals who have challenged laws that require them to divulge certain information—whether that information is sensitive or not—are not simply concerned about that information landing in the wrong hands; rather, they have been offended by the fact that the government poses the question in the first place. In other words, they want to prevent the government from collecting certain information because, even if no unauthorized person ever gains access to the information, it is degrading when the government asks the question and collects the information in the first instance.

Khiara Bridges, *The Poverty of Privacy Rights* 162 (2017). Professor Danielle Keats Citron has further explained:

> Indeed, there are some aspects of a person's life in which the government has no legitimate interest and whose collection undermines self-respect and autonomy. Individuals have the right *not to be known* if the state's questions would demean and humiliate them for no good reason. Privacy honors human dignity by conferring "respect for individual choice" and "respect for individuals because they have the capacity for choice."

Danielle Keats Citron, *A Poor Mother's Right to Privacy: A Review*, 98 B.U. L. Rev. (forthcoming 2018) (manuscript at 12) (on file with authors) (internal citations omitted); *see* also Danielle Citron & David A. Super, *We Don't Need a National Data Center of the Poor*, Slate (May 8, 2018).[16] This point is underscored by the work of Bignami and Resta:

> The right [recognized by the German Constitutional Court] came into being at the time of collection—at the moment that the individual was asked to give up the information—and not simply once it was used or misused by state actors and other types of data processors.

Bignami & Resta, *supra*, at 233.

Courts outside of the United States have invoked the right to informational privacy to protect individuals' interests in preventing or limiting collection of their personal medical information and employment-related information. In 1999, the Spanish Constitutional Court held that the right to informational privacy bars collection of health-related data absent a specific statutory mandate or individual consent. STC 202/1999, of Nov. 8 [Spanish Constitutional Court], cited in Javier Thibault Aranda, *Information Technology and Workers' Privacy: A Comparative Study: Part II: National Studies: Information Technology and Workers' Privacy: The Spanish Law*, 23 Comp. Lab. L. & Pol'y J. 431 (2002). The Court held that a database called "absent on medical grounds" was unconstitutional. The database

[16] https://slate.com/technology/2018/05/the-national-food-stamp-database-proposed-by-house-republicans-is-a-potential-nightmare.html.

collected the results and diagnoses of employees' regular medical examinations. Some employees did not consent to the use of this data; nor were the records kept to preserve the health of employees. In *Rechnungshof v. Österreichischer Rundfunk and Others*, the Supreme Court of Austria held that "collection of data by name relating to an individual's professional income, with a view to communicat[e] it to third parties," violates the right to informational privacy. Joined Cases C-465/00, C-138-01, *Rechnungshof v. Österreichischer Rundfunk and Others*, 2003 E.C.R. (May 20, 2003);[17] *see also Arroyo v. Rattan Specialties, Inc.*, 117 P.R. Dec. 35 (1986), *cited in* Luis Anibal Aviles Pagan, *Articulo: Human Dignity, Privacy and Personality Rights in the Constitutional Jurisprudence of Germany, the United States and the Commonwealth of Puerto Rico*, 67 Rev. Jur. U.P.R. 343 (1998) (holding that mandatory polygraph tests violate employees' right to informational privacy because "[r]egardless of the degree of reliability that the polygraph test could reach, its intrusion upon the mind of the human being, with his thoughts, is such that he loses the freedom to control the disclosure of his own thoughts").

The right also extends to the retention of personal data lawfully collected. In *Case of S. and Marper v. The United Kingdom*, Application nos. 30462/04, Eur.

[17] Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62000CJ0465.

Ct. H.R., Dec. 4, 2008, two UK citizens requested destruction of their fingerprints and DNA samples after they were acquitted of criminal charges, but the UK police refused. The European Court of Human Rights held that the United Kingdom violated Article 8 of the European Convention for the Protection of Human Rights and Freedoms by failing to safeguard citizens' informational privacy rights in their fingerprints, DNA and cellular samples. It reasoned: "the blanket and indiscriminate nature of the powers of retention of fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences . . . fails to strike a fair balance between competing public and private interests." *Id.* at ¶ 125.

Last, and of particular importance for this case, the right encompasses the conditions under which personal data, lawfully collected, may be retained. As Professor Michael Froomkin explained, in an article cited by the lower court:

> When the State takes a person's data and holds it in a fashion outside the person's control, the State has done to that data exactly what Chief Justice Rehnquist said was necessary to trigger Due Process Clause protection: it has 'by the affirmative exercise of its power' taken the data and 'so restrain[ed]' it that the original owner is unable to exert any control whatsoever over how the government stores or secures it. The government's 'affirmative duty to protect' the data 'arises . . . from the limitation which it has imposed on his freedom to act on his own behalf to keep the data secure.

In re OPM Data Breach Security Litigation, 266 F. Supp. 3d 1, 45 (D.D.C. 2017) (citing Michael Froomkin, *Government Data Breaches*, 24 Berkeley Tech. L.J. 1019, 1049 (2009)).

Government collection of personal data implicates fundamental due process rights. When the state has failed to safeguard that information, the state has violated those rights. The prudential reasons for "not entering the fray" in *AFGE* no longer hold. In 1997, the *AFGE* court said that the plaintiffs "could cite no case in which a court has found a violation of the constitutional right to privacy where the government has collected, but not disseminated, the information." *AFGE v. HUD*, 118 F.3d at 793. But that finding preceded the wave of data breaches federal agencies experienced since that time. Discussing *Whalen*, the *AFGE* court also said

> the state had enacted security provisions protecting the privacy of patients, and that there was no record evidence that the security provisions would prove insufficient. Accordingly, the Court held that unsubstantiated fear of public disclosure was not a sufficient reason for invalidating the statute.

Id. But evidence now shows that the security provisions are insufficient and the risk of identity theft and financial fraud is no longer an "unsubstantiated fear." According to the Federal Trade Commission, identity theft is among the top concerns of American consumers. Fed. Trade Comm'n, *FTC Releases Annual Summary of Complaints Reported by Consumers* (Mar. 1, 2018) ("Identity theft was the second biggest category, making up nearly 14 percent of all the consumer

complaints.).[18] And the *AFGE* court placed substantial weight on the protections purportedly provided by the Privacy Act, stating:

> the records are maintained under secure conditions. Those charged with maintaining the records are, themselves, subject to background checks. These measures, designed to protect the confidentiality of the information, substantially reduce the employees' privacy interests.

AFGE v. HUD, 118 F.3d at 793. That is precisely the same mistake that the Supreme Court made in *Nelson*, discussed *supra*. The Privacy Act did not prevent the breach of 22 million records of government employees, their families, and friends, which is the case now before this Court.

II. Standing to challenge data breaches is well-established under *CareFirst.*

The lower court's analysis of Article III standing was also flawed in two important respects. First, the court misunderstood the key role that Social Security Numbers play in identity theft and financial fraud, and misapplied the rule in *Carefirst*. And second, the court misstated the holding and outcome in *Spokeo*.

In *Attias v. CareFirst, Inc.*, this Court found that Plaintiffs "cleared the *low bar* to establish their standing" because they were victims of a data breach. 865 F.3d 620, 622 (D.C. Cir. 2017) (emphasis added). The Court emphasized that "an unauthorized party has already accessed personally identifying data on CareFirst's servers, and it is much less speculative—at the very least, it is plausible—to infer

[18] https://www.ftc.gov/news-events/press-releases/2018/03/ftc-releases-annual-summary-complaints-reported-consumers

that this party has both the intent and the ability to use that data for ill." *Id.* at 628. Furthermore, "a substantial risk of harm exists already, simply by virtue of the hack and the nature of the data that the plaintiffs allege was taken." *Id.* at 629.

Given the holding in *CareFirst*, the lower court should have simply held that plaintiffs "cleared the low bar." Instead, the court mistakenly interpreted *CareFirst* as requiring proof of "theft of credit card information" to establish standing. That is not the test, and credit card theft is not even the most damaging or impactful form of identity theft and financial fraud. When a criminal gains access to an individual's SSN they can commit many types of financial fraud, including tax refund fraud, government benefit fraud, medical fraud, employment fraud, and can even commit crimes in the victim's name. *See* Social Security Admin., *Identity Theft and Your Social Security Number*, Pub. No. 05-10064 (2017);[19] Office of Inspector Gen., U.S. Dep't of Health & Human Serv., *Medical Identity Theft* (2018);[20] Internal Revenue Serv., *Taxpayer Guide to Identity Theft* (2018);[21] Internal Revenue Serv., *Guide to Employment-Related Identity Theft* (2018).[22] Even worse, a stolen SSN, unlike a stolen credit card, cannot be easily cancelled or replaced.

---

[19] https://www.ssa.gov/pubs/EN-05-10064.pdf.
[20] https://oig.hhs.gov/fraud/medical-id-theft/index.asp.
[21] https://www.irs.gov/newsroom/taxpayer-guide-to-identity-theft.
[22] https://www.irs.gov/identity-theft-fraud-scams/employment-related-identity-theft.

The unauthorized use of a credit card is only one example of the financial damage caused by a data breach. Individuals who lose control of their SSNs, like the plaintiffs in this case, face a much more significant risk. As the Federal Trade Commission explains, a thief can cause many types of damage when they obtain personal information (including, most important, the SSN):

> An identity thief can use your name and information to:
>
> - buy things with your credit cards
> - get new credit cards
> - open a phone, electricity, or gas account
> - steal your tax refund
> - get medical care
> - pretend to be you if they are arrested

Fed. Trade Comm'n, *Avoiding Identity Theft* (2018);[23] *see also* Fed. Trade Comm'n, *Security in Numbers: SSNs and ID Theft* 2 (Dec. 2008).[24] No other identifier plays a more significant role in record-linkage, or poses a greater risk to personal privacy than the SSN. *See* EPIC, *Social Security Numbers* (2018).[25] Unfortunately, the SSN is used as both an identifier and an authenticator. *Id.* In other words, the SSN is both the username and password for an individual's identity. *Id.* As a result, when a person's SSN is disclosed, the risk of financial fraud and identity theft is magnified.

---

[23] https://www.consumer.gov/articles/1015-avoiding-identity-theft.
[24] https://www.ftc.gov/sites/default/files/documents/reports/security-numbers-social-ssecurity-numbers-and-identity-theft-federal-trade-commission-report/p075414ssnreport.pdf.
[25] https://epic.org/privacy/ssn/.

New account fraud is an especially damaging type of identity theft that criminals, armed with SSNs, can commit because many financial institutions rely on the numbers to verify new customers. *See* Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Credit.com (Nov. 2, 2017);[26] Ass'n of Certified Fraud Examiners, *Financial Institution Fraud* (2013).[27] The Bureau of Justice Statistics found that "[v]ictims experiencing the opening of a new account or the misuse of personal information had greater [out-of-pocket] loss than those experiencing misuse of an existing credit card or bank account." *See* Bureau of Justice Statistics, Office of Justice Programs, U.S. Dep't of Justice, NCJ 248991, *Victims of Identity Theft, 2014* 7 (Sept. 2015) (revised Nov. 13, 2017).[28] These identity theft victims are also more likely to have unresolved problems more than a year later. *Id.* at 13. The breach of SSNs therefore creates the very risk of harm that this Court recognized in *CareFirst* that gives rise to standing. 865 F.3d at 629.

The lower court also misstated the Supreme Court's holding in *Spokeo* and the application of the "concrete injury" test post-*Spokeo*. Specifically, the lower court held that the plaintiff's claim in *Spokeo* was "found to be insufficient"

[26] http://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/.
[27] http://www.acfe.com/uploadedFiles/Shared_Content/Products/Self-Study_CPE/Financial%20Institution%20Fraud%202013_Chapter%20Excerpt.pdf.
[28] https://www.bjs.gov/content/pub/pdf/vit14.pdf.

without "a further showing that real harm, albeit even intangible harm, would follow." JA 416–17. Bhe Supreme Court made clear in *Spokeo* that the basis for reversal was the Ninth Circuit's failure "to fully appreciate the distinction between concreteness and particularization" and that the lower court's "standing analysis was incomplete." *Spokeo v. Robbins*, 136 S. Ct. 1540, 1550 (2016). On remand, the Ninth Circuit conducted the necessary concreteness analysis and determined that the plaintiff's claims were sufficient to establish standing. *Spokeo v. Robbins*, 867 F.3d 1108 (9th Cir. 2017). The Supreme Court declined Spokeo's request to review that decision. 138 S. Ct. 931 (2018).

There is no "real harm" requirement in Article III, only a requirement that a plaintiff allege a concrete and particularized *injury*. The lower court's analysis of standing post-*Spokeo* was incorrect.

CONCLUSION

For the reasons explained above, *Amici* respectfully request this Court reverse the judgment of the district court.

Respectfully submitted,

/s/ Marc Rotenberg

MARC ROTENBERG
ALAN BUTLER
NATASHA BABAZADEH
Electronic Privacy Information Center
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140
rotenberg@epic.org

Dated: May 17, 2018

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 established in this Court's briefing Order because it contains 6,855 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/ Marc Rotenberg

MARC ROTENBERG

CERTIFICATE OF SERVICE

The undersigned counsel certifies that on this 17th day of May 2018, 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/ Marc Rotenberg

MARC ROTENBERG