No. 13-1339

IN THE

Supreme Court of the United States

SPOKEO, INC.,

Petitioner,

v.

THOMAS ROBINS, ON BEHALF OF HIMSELF AND ALL OTHERS SIMILARLY SITUATED,

Respondent.

On Writ of Certiorari to the United States Court of Appeals for the Ninth Circuit

BRIEF OF *AMICI CURIAE* ELECTRONIC PRIVACY INFORMATION CENTER (EPIC) AND THIRTY-TWO TECHNICAL EXPERTS AND LEGAL SCHOLARS IN SUPPORT OF RESPONDENT

MARC ROTENBERG
Counsel of Record
ALAN BUTLER
T. JOHN TRAN
ELECTRONIC PRIVACY
INFORMATION CENTER (EPIC)
1718 Connecticut Ave. N.W.
Suite 200
Washington, DC 20009
(202) 483-1140
rotenberg@epic.org

September 8, 2015

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

OTHER AUTHORITIES

INTEREST OF THE *AMICI CURIAE*

The Electronic Privacy Information Center (EPIC) is a public interest research center in Washington, D.C.[1] 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.[2]

EPIC routinely participates as *amicus curiae* before this Court in cases concerning emerging privacy and civil liberties issues: *See, for example*, *City of Los Angeles, California v. Patel*, 135 S. Ct. 2443 (2015), *Riley v. California*, 134 S. Ct. 2473 (2014); *Sorrell v. IMS Health Inc.*, 131 S. Ct. 2653 (2011); *Doe v. Reed*, 561 U.S. 186 (2010); *Hiibel v. Sixth Judicial Dist. Ct. of Nevada*, *Humboldt County,* 542 U.S. 177 (2004); *Watchtower Bible & Tract Soc'y of N.Y., Inc. v. Stratton, Ohio*, 536 U.S. 150 (2002).

Technical Experts and Legal Scholars

Colin J. Bennett, Professor, University of Victoria

---

[1] Both parties consent to the filing of this brief. In accordance with Rule 37.6, the undersigned states that no monetary contributions were made for the preparation or submission of this brief, and this brief was not authored, in whole or in part, by counsel for a party.

[2] EPIC Appellate Advocacy Fellow Aimee Thomson and the following EPIC Clerks participated in the preparation of this brief: Britney Littles, Eogan Hickey, Jennifer Weekley, John Davisson, Kasey Wang, Michele Trichler, and Ximeng Tang.

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

Ryan Calo, Assistant Professor of Law, University of Washington School of Law

Dr. Peter G. Neumann, SRI International

Danielle Keats Citron, Lois K. Macht Research Professor of Law, University of Maryland School of Law

Dr. Whitfield Diffie, Visiting Scholar, Stanford Center for International Security and Cooperation

Laura K. Donohue, Professor, Director of the Center for National Security and the Law & Center on Privacy and Technology, Georgetown University Law Center

Cynthia Dwork, Distinguished Scientist, Microsoft Research

David J. Farber, Distinguished Career Professor of Computer Science and Public Policy, 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

Deborah Hurley, Institute for Qualitative Social Science, Harvard University

Ian Kerr, Canada Research Chair in Ethics, Law & Technology, University of Ottawa Faculty of Law

Chris Larsen, CEO, Ripple Labs 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

Dr. Pablo Molina, Adjunct Professor, Georgetown University

Helen Nissenbaum, Professor, Director of the Information Law Institute, New York University

Frank Pasquale, Professor of Law, University of Maryland Francis King Carey School of Law

Dr. Deborah Peel, M.D., Founder and Chair, Patient Privacy Rights

Chip Pitts, Chair, EPIC Board of Directors

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

Bruce Schneier, Security Technologist; Author, Schneier on Security (2008)

Barbara Simons, IBM Research (retired)

Robert Ellis Smith, Publisher, Privacy Journal

Nadine Strossen, John Marshall Harlan II Professor of Law, New York Law School, Former President, American Civil Liberties Union

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

Latanya Sweney, Professor of Government and Technology in Residence, Harvard University

Edward G. Vlitz, President and Chairman, Internet Collaboration Coalition

(Affiliations are for identification only)

SUMMARY OF THE ARGUMENT

Consumers in the United States today face unprecedented threats of financial fraud and identity theft arising from the misuse of their personal information. The newspapers are filled with reports of data breaches and identity theft. Nearly every adult in the United States with a credit card has received a notification that their account has been hacked, and advised to sign up for "credit monitoring" services. Consumers routinely report to the Federal Trade Commission that identity theft is their top concern.

Anticipating that the collection and use of personal data in the modern economy would pose enormous risks to privacy, Congress enacted laws that establish rights for individuals and imposed obligations on the companies that profit from the collection and use of this data. This case presents a critical issue for the future of privacy in the United States—whether individuals whose personal information was misused by a firm in violation of an Act of Congress must also show an additional harm to seek redress. The defendant seeks to impose special pleading requirements on plaintiffs by requiring that they prove damages at the outset to establish the court's jurisdiction. That requirement is contrary to the Court's jurisprudence concerning the Article III "case and controversy" requirement, and it would remove the keystone of the Fair Credit Reporting Act and other privacy statutes—the ability

of consumers to seek redress when a company fails to safeguard their personal information as required by Congress.

ARGUMENT

I. Americans Face Unprecedented Threats to Personal Privacy

This is not the time for the Supreme Court to limit the ability of individuals to seek redress for violations of privacy rights set out by Congress. Americans consumers today face an epidemic of privacy harms, including data breaches, identity theft, and financial fraud. Many consumers are unable to obtain jobs or credit because of inaccurate or incomplete information made available by data brokers. These harms arise directly from the failure of companies that profit from the collection and use of the personal information of others to comply with the laws established by Congress to safeguard privacy. The willful violation of these laws threatens the economic and social opportunities of respondent Robins and millions of Americans consumers, whose personal information is collected and used by firms without their knowledge or consent. As Chief Justice Rehnquist warned, "All too often the invasion of privacy itself will go unknown. Only by striking at all aspects of the problem can privacy be adequately protected." *Bartnicki v. Vopper*, 532 U.S. 514, 549 (2001) (Rehnquist, C.J., dissenting).

A. Identity Theft and Consumer Fraud Have Skyrocketed as Data Brokers Put Consumers' Personal Information at Risk

For the fifteenth consecutive year, identity theft is the number one complaint among American consumers. Fed. Trade Comm'n, *Consumer Sentinel Network Data Book* 3 (2015). According to the most recent Department of Justice report, more than sixteen million Americans were the victims of identity theft in 2012 alone. *See* Erika Harrell, Ph.D. & Lynn Langton, Ph.D., Bureau of Justice Statistics, *Victims of Identity Theft* 1 (Dec. 12, 2013). That year, identity theft cost American consumers more than twenty-four billion dollars, ten billion more than the losses attributed to all other property crimes. *Id.* at 6 (outpacing fourteen billion in losses from burglary, automobile theft, and theft).[3]

As data brokers gather and store sensitive consumer data, the risk of data breaches necessarily increases. These valuable troves of personal information attract "identity thieves and other unscrupulous actors" to "the collection of consumer profiles that would give them a clear picture of consumers' habits over time, thereby enabling them to predict passwords, challenge questions, or other authentication credentials." Fed. Trade Comm'n, *Data Brokers: A Call for Transparency and*

[3] *Available at* http://www.bjs.gov/content/pub/pdf/vit12.pdf.

Accountability vi (2014) [hereinafter "FTC Data Broker Report"].[4]

In some instances, data brokers engage in practices that contribute directly to fraud and theft. The FTC determined that the data broker ChoicePoint had sold consumer profiles to identity thieves. *See* Stipulated Final J. and Order for Civil Penalties, Permanent Inj., and Other Equitable Relief, *United States v. ChoicePoint Inc.*, Feb. 15, 2006. The company caused so much damage that it paid, at the time, the largest fine in the FTC's history. Peter Lattman, *ChoicePoint Settles with FTC*, Wall St. J. (Jan. 27, 2006). Significantly, ChoicePoint's debacle was not an isolated incident. Subsequent reports revealed that the company also sold similar information on seven thousand people to identity thieves in 2002 with losses over one million dollars. David Colker & Joseph Menn, *ChoicePoint CEO Had Denied Any Previous Breach of Database*, L.A. Times (March 3, 2005).[5] *See also Identity Theft and Data Broker Services: Hearing Before the S. Comm. on Commerce, Sci., and Transp.*, 109th Cong. 1 (2005) (statement of Marc Rotenberg, Exec. Dir., EPIC).

Data breaches are on the rise. From 2013 to 2014, data breaches increased by twenty-three

---

[4] *Available at* https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

[5] http://articles.latimes.com/2005/mar/03/business/fi-choicepoint3.

percent. Symantec, *Internet Security Threat Report* 78 (2015).[6] In 2014 there were four "mega breaches," resulting in the exposure of "at least ten million" different individuals' personal data. *Id.* Those breaches exposed hundreds of millions of records, including names, birth dates, social security numbers, addresses, medical records, phone numbers, financial information, e-mail addresses, user names and passwords, and insurance information. *Id*. at 83.

Data breaches in 2015 have already exposed more than one hundred and forty million records of personally identifiable information. Identity Theft Res. Ctr., *Data Breach Reports* 5 (Aug. 25, 2015) (defining a data breach as "an incident in which an individual name plus a Social Security number, driver's license number, medical record or financial record (credit/debit cards included) is potentially put at risk because of exposure").[7] *See also Is the OPM Data Breach the Tip of the Iceberg?: Hearing Before the H. Comm. on Sci., Space, & Tech.*, 114th Cong. (2015) (statement of Chairman Lamar Smith (R-Tx)) ("National defense in the digital age no longer just means protecting ourselves against enemies who attack with traditional weapons. It now means protecting America from those who launch cyber-attacks against our computers and networks,

---

[6] *Available at* https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf.

[7] *Available at* http://www.idtheftcenter.org/images/breach/DataBreachReports_2015.pdf.

invading our privacy and probably endangering lives.").

Data breaches were "one of the main sources of fraud last year," and a recent report found that "one in three people who received notifications of a data breach" have discovered that they were subject to fraud. Blake Ellis, *Identity Fraud Hits New Victim Every Two Seconds*, CNN Money (Feb. 6, 2014).[8] Surveys indicate that more than forty percent of Americans have "experienced some form of payment card fraud in the last five years." *Skimming Off the Top*, Economist (Feb. 5, 2014).[9] The costs of these breaches have increased exponentially over the last few decades, and data brokers contribute to the problem by failing to follow their statutory obligations.

B. Data Brokers Sell Consumer Profiles on Millions of Americans Without Verifying the Accuracy or Completeness of the Records

Data brokers quantify, collect, and sell data on nearly every aspect of modern life. One company's database contains information on "1.4 billion consumer transactions and over 700 billion aggregated data elements." FTC Data Broker Report at 46. Starting with basic data elements such as name, gender, ethnicity, and income, data brokers make significant inferences about consumers. *Id.* at

---

[8] http://money.cnn.com/2014/02/06/pf/identity-fraud/.

[9] http://www.economist.com/news/finance-and-economics/21596547-why-america-has-such-high-rate-payment-card-fraud-skimming-top.

iv–v ("Potentially sensitive categories include those that primarily focus on ethnicity and income levels, such as 'Urban Scramble' and 'Mobile Mixers,' both of which include a high concentration of Latinos and African Americans with low incomes."). "The ability of a company—a company that you have no relationship with—to know where you live, your demographics, your interests, and how to contact you is unprecedented." Jeff Jonas, *The Surveillance Society and Transparent You*, *in Privacy in the Modern Age: The Search for Solutions* 93, 98 (Marc Rotenberg, Julia Horwitz, & Jeramie Scott eds., 2015).

Precautionary and remedial measures also impose heavy costs on consumers. *See* Frank Pasquale, *We're Being Stigmatized by 'Big Data' Scores We Don't Even Know About*, L.A. Times (Jan 15, 2015) ("Naturally, just as we've lost control of data, a plethora of new services offer 'credit repair' and 'reputation optimization' to remedy the stigmatization of secret digital judgments.").[10] For example, credit repair companies charge initial fees ranging from $49 to $99 in addition to monthly payments. *See How Much Do Credit Repair Services Cost?*, Lexington Law (2015).[11] But a credit repair

---

[10] http://www.latimes.com/opinion/op-ed/la-oe-0116-pasquale-reputation-repair-digital-history-20150116-story.html.

[11] https://www.lexingtonlaw.com/faq/costs. *See also Credit Repair*, Sky Blue Credit Repair, https://www.skybluecredit.com (last visited July 2, 2015); *How It Works*, Ovation (2015), http://www.ovationcredit.com/WhatWeDo (last visited July 2, 2015).

service is not a guaranteed fix of a credit score. The National Association of Insurance Commissioners reports that the typical cost of identity theft insurances ranges from $25 to $60 per year. *A Rise in Identity Theft Spurs New Type of Insurance*, Nat'l Ass'n of Ins. Comm'rs (Sept. 2009).[12] Online reputation management services can cost between $250 and $8000 initially plus monthly maintenance charges, which can range from $20 to upwards of $2000 per month. *See Pricing*, BrandYourself;[13] *How Reputation Management Works*, Reputation.com (2015).[14] Social media monitoring software can cost a consumer between $100 and $500 per month. *Pricing*, Trackur (2014).[15]

Although the total impact of inaccurate reports, data breaches and identity theft in the United States is staggering, the ability for an individual to prove harm is particularly difficult.. Unlike physical crimes, harms arising from inadequate data protection are often concealed. *See, e.g.*, *Law Enforcement*, Identity Theft Res. Center (last visited Sept. 3, 2015) ("Most identity theft crimes are multi-jurisdictional, time consuming, and difficult to solve.").[16] In addition, the harms caused

---

[12] http://www.naic.org/documents/consumer_alert_idtheft.htm.

[13] https://brandyourself.com/info/about/howItWorks/headStart (last visited July 2, 2015).

[14] http://www.reputation.com/personal/how-reputation-management-works (last visited July 2, 2015).

[15] http://www.trackur.com/options.

[16] http://www.idtheftcenter.org/id-theft/law-enforcement.html.

by such privacy violations are not easily quantified, though the consequences of a lost job, the weeks spent fixing an inaccurate credit report, or changing credit cards are very real.

Well aware of the enormous challenge of safeguarding privacy in the modern age, Congress has enacted laws that impose obligations on commercial firms to minimize the risk of the misuse of personal information and provided for statutory damages when companies fail to comply with these requirements. *See, e.g.*, Consumer Credit Reporting Reform Act of 1996, Pub. L. No. 104-208, Div. A., Title II, Subtitle D, § 2412(b), 110 Stat. 3009–446 (1996) (codified at 15 U.S.C. § 1681n(a)(1)(A)) (amending FCRA to include a statutory damages provision); Video Privacy Protection Act of 1988, Pub. L. No. 100-618, 102 Stat. 3195 (codified at 18 U.S.C. § 2710). Congress has recognized that consumers cannot be expected to wait until after they suffer monetary damage to seek redress for a company's failure to meet its privacy obligations.

II. Privacy Laws Establish Individual Rights for Data Subjects and Impose Legal Obligations on Data Processors

Modern privacy laws, such as the Fair Credit Reporting Act, place obligations on companies that collect personal information and give rights to individuals whose information is collected and disseminated. The allocation of responsibilities and rights is sensible, particularly because the entity in possession of the data that controls its subsequent use. It is economically efficient for the entity in possession of personal data to bear the consequences for its subsequent misuse.

The rights and responsibilities that provide the basis of privacy laws have come to be known as "Fair Information Practices" ("FIPs"). *See* EPIC, *The Code of Fair Information Practices*.[17] "Fair information Practices provide the central conceptual framework for privacy rights in the digital age." Marc Rotenberg, *EPIC: The First Twenty Years*, *in Privacy in the Modern Age: The Search for Solutions* 1, 5 (Marc Rotenberg, Julia Horwitz, & Jeramie Scott eds., 2015). The Privacy Act of 1974, 5 U.S.C. § 552a (2012), incorporated the FIPs as outlined by the HEW Report in 1973, *see* U.S. Dep't. of Health, Education and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, *Records, Computers, And The Rights of Citizens* (1973), and this structure has been adopted in every major privacy law. The FIPs include five obligations for all organizations that collect personal data:

1. There must be no personal data record-keeping systems whose very existence is secret.
2. There must be a way for a person to find out what information about the person is in a record and how it is used.
3. There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent.
4. There must be a way for a person to correct or amend a record of identifiable information about the person.

---

[17] http://epic.org/privacy/consumer/code_fair_info.html.

5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data.

Id. at viii. These obligations are central for the data broker industry, where "it would be impractical to premise data collection and use . . . based solely on traditional implementations of notice and choice." Christopher Wolf, *Envisioning Privacy in the World of Big Data*, *in Privacy in the Modern Age: The Search for Solutions* 204, 205 (Marc Rotenberg, Julia Horwitz, & Jeramie Scott eds., 2015).

Congress passed the FCRA to make clear the fiduciary duties that arise from the decision of companies to profit from the collection and use of personal information. As this Court recently explained, "Congress enacted FCRA in 1970 to ensure fair and accurate credit reporting, promote efficiency in the banking system, and protect consumer privacy." *Safeco Ins. Co. of America v. Burr*, 551 U.S. 47, 52 (2007). The rights set out in the FCRA and other privacy laws arise directly from these fiduciary responsibilities established by Congress.

For example, FCRA not only limits the disclosure of information contained in credit reports, but it also places on the credit reporting agency an obligation to ensure that the information is correct and timely, 15 U.S.C. § 1681e(b) (2012), and it provides the subject of the credit report the opportunity to inspect the record and correct it if necessary, § 1681g. The law also requires that "any person [who] takes any adverse action with respect to

any consumer that is based in whole or in part on any information contained in a consumer report" must notify the affected consumer. *Safeco*, 551 U.S. at 53 (citing 15 U.S.C. § 1681m(a) (2012)).

These responsibilities help ensure that data collectors use personal information for its intended purposes and that financial institutions base determinations, such as whether a person qualifies for a car loan or can obtain a home mortgage, are based on accurate information. *See* 15 U.S.C. § 1681(b) (2012) (defining the purpose of the FCRA as "requiring that consumer reporting agencies adopt reasonable procedures" to ensure that credit reporting is "fair and equitable to the consumer, with regard to the confidentiality, accuracy, relevancy, and proper utilization" of consumer information). When the Court in *Safeco* articulated the rights and obligations created by the FCRA, it never questioned the standing of an individual to bring suit based on the violation of those rights.[18]

---

[18] If the Court were to adopt the test that Spokeo proposes in this case, it would have to reconsider all prior opinions in which it presumed standing for claims based on the violation of a legally protected interest without any proof of consequential harm. *See*, *e.g.*, *Zivotofsky v. Kerry*, 135 S. Ct. 2076 (2015) (considering a challenge brought by a minor child for declaratory and injunctive relief based on a challenge to the listed place of birth on his U.S. passport); *Havens Realty Corp. v. Coleman*, 455 U.S. 363, 374 (1982) (upholding the right of Fair Housing Act testers to receive "truthful information concerning the availability of housing," even in the absence of further harm).

Congress also established individual rights to deter the collection or disclosure of personal information by unknown third parties, which would violate an individual's privacy. For example, in the Wiretap Act, 18 U.S.C. §§ 2510–22 (2006), the injury occurs with the "interception" of a "wire, oral, or electronic communication." *Id*. § 2511(1)(a)–(e). The harm is the unlawful intrusion itself, irrespective of any subsequent or consequential damages. Congress passed the Wiretap Act to remedy "extensive wiretapping carried on without legal sanctions, and without the consent of any of the parties to the conversation." Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. 90-351, § 801, 82 Stat. 197, 211. The class of persons entitled to sue consists only of those who have suffered the injury: "any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used" in violation of the Act. 18 U.S.C. § 2520(a) (2006).

At the time of the introduction of the Video Privacy Protection Act in 1988, Senator Chuck Grassley explained the important interests served by federal privacy laws:

> Privacy is something we all value. The right of privacy is not, however, a generalized undefined right. It is a specific right, one which individuals should understand. And it is the role of the legislature to define, expand, and give meaning to the concept of privacy.

134 Cong. Rec. 5400–01 (May 10, 1988).

When it enacted the FCRA, Congress provided for statutory remedies to ensure protection of personal data. The need for statutory remedies is

due, in part, to the complicated nature of harms resulting from privacy violations. Echoing the views expressed by Chief Justice Rehnquist in *Bartnicki v. Vopper*, 532 U.S. 514, 549 (2001) (Rehnquist, C.J., dissenting), privacy scholars have explained why the harms resulting from privacy invasions are especially difficult to quantify and trace. The underlying interests protected by federal privacy laws are as complex and varied as they are important.

Privacy rights serve at least three separate purposes. First, privacy helps individuals avoid the embarrassment that accompanies the disclosure of certain personal details. Second, privacy helps to preserve human dignity, respect, and autonomy. Finally, privacy helps individuals construct intimacy with others. Jerry Kang, *Information Privacy in Cyberspace Transactions,* 50 Stan. L. Rev. 1193, 1212–16, 1260 (1998).

Privacy violations negatively impact the lives of Americans, and the "embarrassment that results from privacy incursions is uniquely detrimental to humans, with irreparable effects on individuals." Ann Bartow, *A Feeling of Unease About Privacy Law*, 155 U. Pa. L. Rev. 52 (2007). Cognitive psychology research also demonstrates that embarrassment from lack of privacy stunts social development and growth, neither of which is fungible or replaceable in human beings. *See* Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 Stan. L. Rev. 1373, 1425 n.195 (2000).

The exposure or misuse of privacy information also "poses special threats to individuals' ability to structure their lives in unconventional ways." Jeffrey Rosen, *The Purposes of Privacy: A Response*, 89 Geo.

L.J. 2117, 2121 (2001). Privacy further enables personal autonomy and freedom:

> [I]nsofar as privacy, understood as a constraint on access to people through information, frees us from the stultifying effects of scrutiny and approbation (or disapprobation), it contributes to material conditions for the development and exercise of autonomy and freedom in thought and action.

Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* 82 (2010).

The interests of personal autonomy, dignity, and freedom are especially important values in American law. "Even in a world in which, thanks to technology, acquiring knowledge about others is virtually effortless, personal autonomy must be respected." Francesca Bignami, *The Case for Tolerant Constitutional Patriotism: The Right to Privacy Before the European Courts*, 41 Cornell Int'l L.J. 211, 223 (2008). Personal autonomy "concerns the individuals' ability to maintain a sphere of immunity from social norms and regulations." Jeffrey Rosen, *The Purposes of Privacy: A Response*, 89 Geo. L.J. 2117, 2121 (2001). Privacy interests are not only essential to freedom and autonomy, they go to the core of self definition.

Privacy laws in the United States protect individuals from a wide range of harms, including intrusions upon their physical, informational, decisional, proprietary, and associational interests. Anita L. Allen & Marc Rotenberg, *Privacy Law And Society* ___ (2016) (forthcoming). These intrusions

might be intentional or mistaken; they might be caused by government or private organizations. Freedom from such intrusions serves to foster a free and open society, promote human dignity and individuality, and limit threats to individual autonomy. *Id*. at 7 (summarizing values as described in privacy literature).

The individual rights set out in the FCRA and other federal privacy laws are not the administrative schemes outlined in the Endangered Species Act. In *Lujan v. Defenders of Wildlife*, 504 U.S. 555 (1992), the Court found that plaintiffs did not have standing based on a provision giving "any person" the ability to enjoin the United States for a "violation" of the Act—in effect allowing anyone to sue to enforce the public's "nonconcrete interest in the proper administration of the laws." 504 U.S. at 516–17. In contrast, plaintiffs in federal privacy cases seek to enforce the obligations owed to them by entities that misuse their personal data. These plaintiffs have a sufficiently "personal stake in the outcome of the controversy as to assure that concrete adverseness which sharpens the presentation of issues upon which the court so largely depends for illumination." *Massachusetts v. EPA*, 549 U.S. 497, 517 (2007).

III. In Privacy Cases, Plaintiffs Have Standing When a Company Misuses Their Personal Information in Violation of Federal Law

This Court has long held that "Congress may enact statutes creating legal rights, the invasion of which creates standing." *Warth v. Seldin*, 422 U.S. 490, 514 (1975) (citing *Linda R.S. v. Richard D.*, 410 U.S. 614, 617 n.3 (1973)). It follows that the injury

relevant to the standing inquiry is the statutory violation itself, not the harmful consequences that may ultimately result. In the words of Justice Scalia, legal injury is "by definition no more than the violation of a legal right; and legal rights can be created by the legislature . . . ." Antonin Scalia, *The Doctrine of Standing As an Essential Element of the Separation of Powers*, 17 Suffolk U. L. Rev. 881, 885 (1983) (emphasis added). This Court has recognized the distinction between injury-in-fact and resulting harm, holding that that plaintiffs suffering an injury-in-fact need not wait until the harmful consequences of that injury have materialized before enforcing their rights.[19] It is only logical that injury-in-fact be distinct from resulting harm. Requiring a plaintiff to produce a detailed audit of his damages merely to pass through the courthouse door would overturn the notice-pleading model of the civil justice system.

This rule is not only consistent with this Court's well-established precedent on Article III standing, it is simple and easy to administer. In contrast, petitioner Spokeo would have the Court allow the firm to willfully violate obligations to the plaintiff—established by Congress—and be immune from suit unless the plaintiff could also prove consequential harm. This would impose a special heightened pleading standard for privacy cases, which is precisely what Congress sought to avoid when it enacted the FCRA and other federal privacy laws. To rule in the petitioner's favor in this case

---

[19] *See Havens Realty Corp. v. Coleman,* 455 U.S. 363 (1982).

would be directly contrary to the will of Congress and to this Court's precedent.

The petitioner's proposed rule would not only effect a dramatic narrowing of the FCRA, it would undermine the ability of individuals to prevent the misuse of many types of sensitive personal information. For example:

- The Cable Communications Policy Act limits the ability of cable providers to disclose subscriber information. 47 U.S.C. § 551(a) (2012).
- The Driver's Privacy Protection Act punishes the unauthorized acquisition, disclosure, or use of information from motor vehicle records. 18 U.S.C. § 2721 (2012).
- The Electronic Communications Privacy Act prohibits the interception, disclosure, or use of wire, oral, and electronic communications. 18 U.S.C. § 2520(a)-(c) (2012).
- The Fair Debt Collection Practices Act prohibits debt collectors from contacting a consumer at work if the collector knows or has reason to know that the consumer's employer prohibits such contact. 15 U.S.C. § 1692c (2012).
- The Fair and Accurate Credit Transactions Act regulates the disclose of consumer credit reports and requires parties to properly dispose of consumer information. 15 U.S.C. §§ 1681b, 1681w(a) (2012).
- The Right to Financial Privacy Act generally prohibits government authorities

from accessing individuals' bank records without notice and an opportunity to object. 12 U.S.C. § 3402 (2012).

- The Telephone Consumer Protection Act prohibits unsolicited robo-calls and faxes. 47 U.S.C. § 227(b) (2012).
- The Video Privacy Protection Act prohibits video service providers from knowingly disclosing certain consumer information. 18 U.S.C. § 2710 (2012).

Were the Court to accept Spokeo's argument that violations of privacy rights established by Congress are insufficient to establish Article III standing absent specific proof of consequential harm, the Court would severely limit the deterrent effect of federal privacy laws and contribute to the growing problem of data breach and identity theft in the United States.

CONCLUSION

For the foregoing reasons, *amici* respectfully ask this Court to affirm the decision of the Ninth Circuit below.

Respectfully submitted,

MARC ROTENBERG
ALAN BUTLER
T. JOHN TRAN
ELECTRONIC PRIVACY
INFORMATION CENTER (EPIC)
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140
(202) 483-1248 (fax)
rotenberg@epic.org

September 8, 2015