No. 10-708

IN THE

Supreme Court of the United States

FIRST AMERICAN FINANCIAL CORPORATION, Successor in Interest to The First American Corporation, and FIRST AMERICAN TITLE INSURANCE COMPANY,
Petitioners,

v.

DENISE P. EDWARDS, Individually and on behalf of all others similarly situated,
Respondent.

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

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

MARC ROTENBERG
Counsel of Record
JOHN VERDI
ELECTRONIC PRIVACY
INFORMATION CENTER (EPIC)
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140

October 18, 2011

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

CONSTITUTIONAL PROVISIONS

INTEREST OF THE *AMICI CURIAE*

The Electronic Privacy Information Center (EPIC)[1] is a public interest research center in Washington, D.C., which 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 has participated as amicus curiae in several cases before this Court and other courts concerning the application and interpretation of federal privacy statutes, including *FCC v. AT&T*, 131 S. Ct. 1177 (2011) (Personal privacy exemption in the Freedom of Information Act); *Quon v. City of Ontario*, 130 S. Ct. 2811 (2010) (Electronic Communications Privacy Act); *Doe v. Chao*, 540 U.S. 614 (2003) (Privacy Act); *Reno v. Condon*, 528 U.S. 141 (2000) (Driver's Privacy Protection Act); *Kehoe v. Fid. Fed. Bank &*

---

[1] Letters of consent have not been lodged with the Court because on July 11, 2011, Petitioners lodged with the Court their "consent to the filing of amicus curiae briefs, in support of either party or of neither party," and on August 12, 2011, Respondent lodged with the Court their "consent to the filing of amicus curiae briefs, in support of either party or of neither party." 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 Alan Butler and EPIC Consumer Protection Fellow David Jacobs contributed to the preparation of this brief.

Trust, 421 F.3d 1209 (11th Cir. 2005), *cert. denied*, 126 S Ct. 1612 (2006) (Drivers Privacy Protection Act); and Harris v. Blockbuster Inc., 622 F. Supp. 2d 396 (N.D. Tex. 2009) (Video Privacy Protection Act).

At issue in this case is the constitutional standing to sue under Section 8 of the Real Estate Settlement Procedures Act ("RESPA"), which was enacted to combat abusive practices, such as kickbacks, in real estate settlements. But this case also raises the troubling prospect that the Court's consideration of that issue may adversely impact the statutory damages provisions, routinely established by Congress, that are central to the protection of privacy. Indeed, some amici in support of Petitioner have already made this argument.

EPIC supports the outcome reached by the Ninth Circuit. Enforcement provisions granting a private right of action, such as the one in RESPA at issue in this case, are found in almost every federal privacy statute. They are necessary not only because of the difficulty in quantifying harm in privacy cases but also because of the problems associated with establishing a causal link between poor data security practices and the injuries, such as identity theft and financial fraud, that result.

If Congress cannot establish statutory damages to enforce the privacy and security obligations of those who collect and use the personal data of others in the course of their business or agency functions, then such laws will be rendered ineffective.

SUMMARY OF THE ARGUMENT

In the modern era in which organizations build elaborate databases containing extensive details on their customers and the users of their services privacy is protected through federal statutes. These laws require organizations to safeguard personal information, to ensure that it is accurate and timely, and that its use is consistent with the purpose for which it was collected. Above all, these laws minimize the risk of harm to individuals that could result from the failure of organizations to protect the personal data that is within their control. The enforcement provisions established by Congress in these laws are the cornerstone of the statutory structure.

In passing privacy statutes such as the Privacy Act of 1974, the Electronic Communications Privacy Act of 1986, the Video Privacy Protection Act of 1988, and the Driver's Privacy Protection Act of 1994, Congress recognized individual rights of privacy related to the collection, use, and disclosure of personal information. Central to the effectiveness of these public laws are statutory damages provisions that provide the opportunity for individuals to enforce their rights against those entities that are subject to the Act. If individuals were required to prove harm in each such circumstance, it would become virtually impossible to enforce privacy safeguards in the United States.

As this Court has long recognized, a party may meet Article III's requirement of an injury-in-fact by showing a violation of a statute enacted by Congress that "creates legal rights, the invasion of which

creates standing." *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 578 (1992) (quotation marks omitted). When these rights are violated, the injury-in-fact relevant to the standing inquiry is the violation of the relevant provisions set out in the statute, and not the harmful consequences that may ultimately result. *See Havens Realty Corp. v. Coleman*, 455 U.S. 363 (1982); *Adarand Constructors, Inc. v. Pena*, 515 U.S. 200 (1995). This distinction between injury-in-fact and resulting harm is particularly significant in privacy matters because, in many cases, the ultimate harm is far removed from the initial violation of the statute. A computer criminal might wait days, weeks, or even months to profit from the negligent security practices that made it possible to obtain an individual's personal information, and it is quite likely that the individual will never be able to trace back to the source the violation of the statutory obligation that gave rise to the harm.

To ensure the effectiveness of privacy laws, Congress established statutory damage provisions to protect personal information. Statutory damage provisions help ensure that individuals can obtain relief when organizations fail to safeguard personal information; they also deter conduct that Congress has determined is likely to create significant privacy risks. An individual harmed by the improper disclosure of personal information could theoretically sue under a tort or contract theory, but common-law remedies are ill-suited for the modern era in which personal information is routinely collected and stored in vast databases far beyond the control of the individual whose interest are directly impacted by the use and disclosure of this information. As Chief

Justice Rehnquist stated "We are placed in the uncomfortable position of not knowing who might have access to our personal and business e-mails, our medical and financial records, or our cordless and cellular telephone conversations." *Bartnicki*, 532 U.S. 514, 541 (2001) (Rehnquist, C.J, dissenting). To avoid these obstacles to effective enforcement, Congress frequently provides statutory damages for privacy law violations. Privacy laws may also require notification and data correction procedures in an attempt to avoid harms before they occur.

Deferring to the need for Congress legislate effectively is particularly important as more and more information about Americans is held by companies and used in ways over which individuals have no meaningful control. Upholding Congress' authority to set out effective statutory schemes is important both to provide redress to consumers and to ensure that companies develop practices that do not place users at risk. "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*, 532 U.S. at 549 (Rehnquist, C.J., dissenting) (citing S. REP. NO. 1097, at 69 (1968), *reprinted in* 1968 U.S.C.C.A.N., 2112, 2156).

According to the Federal Trade Commission, identity theft has remained the number one concern of American consumers over the past decade. Federal Trade Commission, "FTC Releases List of Top Consumer Complaints in 2010; Identity Theft Tops

the List Again" (Mar. 8, 2011).[3] The Privacy Rights Clearinghouse reports that data breaches are on the rise. Privacy Rights Clearinghouse, "Chronology of Data Breaches: Security Breaches 2005 – Present."[4] This is not the time to limit the ability of Congress to safeguard the well-established right of privacy.

---

[3] *Available at* http://www.ftc.gov/opa/2011/03/topcomplaints.shtm

[4] *Available at* https://www.privacyrights.org/data-breach.

ARGUMENT

I. As This Court Has Recognized, Privacy Laws Serve an Important Purpose and Protect Individual Privacy Interests

As this Court made clear in *Sorrell v. IMS Health, Inc.*, protecting the privacy of personal information is an important governmental purpose. 131 S Ct. 2653, 2668 (2011) ("It may be assumed that, for many reasons, physicians have an interest in keeping their prescription decisions confidential."). In *Sorrell*, this Court emphasized that "[t]he capacity of technology to find and publish personal information, including records required by the government, presents serious and unresolved issues with respect to personal privacy and the dignity it seeks to secure. *Id.* at_2672. The Vermont statute in *Sorrell* was held unconstitutional in large part because it did not contain strong enough, across the board, privacy protections. *Id.* As this Court said, "[p]rivacy is a concept too integral to the person and a right too essential to freedom to allow its manipulation to support just those ideas the government prefers." *Id.*

This Court has highlighted the importance of privacy in other recent cases. In *National Aeronautics & Space Administration v. Nelson*, 131 S. Ct. 746 (2011), this Court recognized the "constitutional privacy 'interest in avoiding disclosure of personal matters,'" while it upheld NASA's hiring practices. 131 S Ct. 746, 751 (2011) (citing *Whalen v. Roe,* 429 U.S. 589, 599-600 (1977); *Nixon v. Administrator of General Services,* 433 U.S. 425, 457 (1977)). In *Doe v. Reed*, 130 S. Ct. 2811

(2010), concerning the disclosure of the identity of a petitioner signer, which may involve the release of "all kinds of demographic information, including the signer's race, religion, political affiliation, sexual orientation, ethnic background, and interest-group memberships," *id.* at 2824, Justice Alito wrote that "requiring such disclosures, however, runs headfirst into a half century of our case law, which firmly establishes that individuals have a right to privacy of belief and association.' *Id.* Justice Thomas further noted "[t]his Court has long recognized the 'vital relationship between' political association 'and privacy in one's associations.'" *Id.* at 2839 (Thomas, J., dissenting)(citing NAACP v. Alabama ex rel. Patterson, 357 U.S. 449 (1958)). Thus, the protection of privacy is a fundamental concern.

This Court has also recognized that individuals have a legal interest in "avoiding disclosure of personal matters." *U.S. Dept. of Justice v. Reporters Comm. For Freedom of Press*, 489 U.S. 749, 762 (1989) (citing *Whalen v. Roe*, 429 U.S. 589, 598-600 (1977) (footnotes omitted)). The interest in avoiding disclosure becomes even more important when that information would not otherwise be freely available, because it was collected through a complex process. *Id.* at 764. Even where information "is not wholly 'private'," the individual retains an interest in "limiting disclosure or dissemination of the information." *Id.* at 770. These principles extend as well to statutes that seek to protect the privacy of communications. As this Court has said, "[i]n a democratic society privacy of communication is essential if citizens are to think and act creatively and constructively." *Bartnicki v. Vopper*, 532 U.S.

514, 533 (2001) (citing President's Commission on Law Enforcement and Administration of Justice, The Challenge of Crime in a Free Society 202 (1967)).

This Court has had many opportunities to review statutes designed to protect privacy interests; it has made clear that Congress plays a critical role in the protection of individual privacy. In *Reno v. Condon*, this Court upheld the Driver's Privacy Protection Act ("DPPA") as a "proper exercise of Congress' authority to regulate interstate commerce under the Commerce Clause." *Reno v. Condon*, 528 U.S. 141, 147 (2000). This Court has also recognized Congress' authority to create statutory privacy rights, as well as its ability to dictate recovery available for violations of those rights. *See, e.g., Doe v. Chao*, 540 U.S. 614 (2004).

In order to safeguard privacy interests, Congress has enacted modern privacy statutes built around the "Fair Information Practices" framework that allocates rights and responsibilities in the collection and use of personal information. Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy*, 2001 Stan. Tech. L. Rev. 1, ¶45 (2001). The concept of Fair Information Practices was first set out in the influential 1973 report *Records, Computers, and the Rights of Citizens*. U.S. Dep't of Health, Educ. & Welfare: Report of the Sec'y's Advisory Comm. on Automated Personal Data Sys., Records, Computers, and the Rights of Citizens (1973). The Code of Fair Information Practices describes basic privacy practices, such as:

- There must be no personal-data record-keeping systems whose very existence is secret.

- There must be a way for an individual to find out what information about him is in a record and how it is used.
- There must be a way for an individual to prevent information obtained about him for one purpose from being used or made available for other purposes without his consent.
- There must be a way for an individual to correct or amend a record of identifiable information about him.
- 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 reasonable precautions to prevent misuse of the data.

Id. at 41.

This framework formed the basis of the Privacy Act of 1974 and many privacy laws since. R. Turn and W.H. Ware, *Privacy and Security Issues in Information Systems*, in ETHICAL ISSUES IN THE USE OF COMPUTERS 133, 138 (Deborah G. Johnson & John W. Snapper eds. 1985). With the Privacy Act, Congress recognized that "in order to protect the privacy of individuals identified in information systems maintained by Federal agencies, it is necessary and proper for the Congress to regulate the collection, maintenance, use, and dissemination of information by such agencies." Pub. L. No. 93-579 § 2 (1974).

In the Privacy Act of 1974 Congress set out findings and purposes that help make clear the basis

of the statutory right of privacy. In the Findings, Congress said:

> (1) the privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies; (2) the increasing use of computers and sophisticated information technology, while essential to the efficient operations of the Government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use, or dissemination of personal information; (3) the opportunities for an individual to secure employment, insurance, and credit, and his right to due process, and other legal protections are endangered by the misuse of certain information systems; (4) the right to privacy is a personal and fundamental right protected by the Constitution of the United States; and (5) in order to protect the privacy of individuals identified in information systems maintained by Federal agencies, it is necessary and proper for the Congress to regulate the collection, maintenance, use, and dissemination of information by such agencies.

Id. § 2(A). Congress also set out the purposes of the Act, necessary for the protection of individual privacy:

The purpose of this Act is to provide certain safeguards for an individual against an invasion of personal privacy by requiring Federal agencies, except as otherwise provided by law, to--(1) permit an individual to determine what records pertaining to him are collected, maintained, used, or disseminated by such agencies; (2) permit an individual to prevent records pertaining to him obtained by such agencies for a particular purpose from being used or made available for another purpose without his consent; (3) permit an individual to gain access to information pertaining to him in Federal agency records, to have a copy made of all or any portion thereof, and to correct or amend such records; (4) collect, maintain, use, or disseminate any record of identifiable personal information in a manner that assures that such action is for a necessary and lawful purpose, that the information is current and accurate for its intended use, and that adequate safeguards are provided to prevent misuse of such information; (5) permit exemptions from the requirements with respect to records provided in this Act only in those cases where there is an important public policy need for such exemption as has been determined by specific statutory authority; and (6) *be subject to civil suit for any damages which occur as a result of willful or*

> *intentional action which violates any individual's rights under this Act.*

Id. § 2(B). (Emphasis added).

To further these purposes, the Privacy Act provides a private right of action to any individual who (1) requests an amendment to their record under § 552a(d)(3) that is denied or improperly reviewed; (2) is refused access to records under § 552a(d)(1); (3) is subject to an adverse determination as a result of failure to properly maintain a record; or (4) suffers an adverse effect as a result of the governments failure to comply with any provision of § 552a. 5 U.S.C. § 552a(g)(1) (2006). Without such rights, established by statute, there would be no effective means to address the concerns identified by Congress or to pursue the objectives Congress sought to achieve.

Many other statutes reflect purposes similar to those of the Privacy Act, assign responsibilities associated with the collection and use of personal information to those who collect data, and give rights to individuals, the "data subjects," such as the right to inspect and correct information. These statutes typically grant a private right of action for statutory damages when their provisions are violated. The Cable Communications Policy Act of 1984 prevents cable operators from collecting "personally identifiable information concerning any subscriber without the prior written or electronic consent of the subscriber concerned." 47 U.S.C. § 551(b)(1) (2006). The Act provides that "[a]ny person aggrieved by any act of a cable operator in violation of this section may bring a civil action in a United States district court." 47 U.S.C. §551(f)(1) (2006). The Video Privacy Protection Act, which creates liability against "a

video tape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer of such provider," 18 U.S.C. § 2710(b)(1) (1988), contains a similar provision. 18 U.S.C. §2710(c)(1). The 1994 Driver's Privacy Protection Act prevents disclosure of any "personal information . . . about any individual obtained by the department in connection with a motor vehicle record." 18 U.S.C. § 2721(a)(1) (2006). This Act specifies that "[a] person who knowingly obtains, discloses or uses personal information, from a motor vehicle record, for a purpose not permitted under this chapter shall be liable to the individual to whom the information pertains, who may bring a civil action in a United States district court." 18 U.S.C. § 2724 (1994).

Congress enacted these and other privacy laws to protect and promote the privacy interests of individuals. Modern informational privacy, in particular, concerns "an individual's control over the processing--*i.e.*, the acquisition, disclosure, and use--of personal information." Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 Stan. L. Rev. 1193, 1203 (1998). Informational privacy laws accordingly provide mechanisms to increase individuals' control over the information that government or private organizations gather and disseminate about them. These enforcement mechanisms are critical to the protection of individual privacy.

Congress continues to enact privacy laws in response to developments in technology and to new business practices. Consumers face a number of complex and difficult trade-offs in the area of online

data protection that require special attention. Consumer decisions related to the collection and protection of personal data on the Internet are inhibited by information asymmetries and other behavioral barriers. *Understanding Consumer Attitudes About Privacy: Hearing Before the Subcomm. on Commerce, Manufacturing, and Trade of the House Comm. on Energy and Commerce* (Oct. 13, 2011) (testimony of Prof. Alessandro Acquisti).[5] As Professor Acquisti describes, "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." *Id.*

As Professor Acquisti suggests, privacy laws also help to restore information symmetry and promote economic efficiency by requiring transparency in data collection practices and imposing liability on the entity in control of the information. Businesses that maintain consumer data are in a better position to safeguard the data. The data collectors are the "least cost avoiders" and can more efficiently protect the data in their possession than could the data subject who has transferred control over their personal information. *See generally* GUIDO CALABRESI, THE COST OF ACCIDENTS (1970). Thus, privacy laws allocate rights and responsibilities in the collection

---

[5] *Available at* http://republicans.energycommerce.house.gov/Media/file/Hearings/CMT/101311/Acquisti.pdf.

and use of personal data both to protect the interests of the individual and to efficiently safeguard personal data.

II. Privacy Laws Depend Upon Congress' Power to Define Injuries in Fact and to Provide for Statutory Damages.

As this Court has recognized, a party may meet Article III's requirement of an injury-in-fact by showing a violation of a statute, enacted by Congress, that "creates legal rights, the invasion of which creates standing." *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 578 (1992) (quotation marks omitted). Congress has exercised this power by passing laws regulating the collection, use, and disclosure of personal information in a variety of contexts, thereby providing standing for individuals whose privacy rights are violated. Because privacy harms are often unquantifiable or intangible, Congress provided statutory damages to ensure that privacy violations were adequately deterred and remedied.

A. The Violation of a Privacy Law Produces an Immediate Injury in Fact Sufficient to Confer Standing Under Article III.

Article III, § 2 of the United States Constitution limits the judicial power to "Cases" and "Controversies." Part of the "irreducible constitutional minimum of standing" required by Article III is an "injury-in-fact—an invasion of a legally protected interest" that is both "concrete and particularized" and "actual or imminent." *Lujan v. Defenders of Wildlife*, 504 U.S. at 560-61. This Court has recognized the important role that Congress

plays in protecting the legal rights of individuals, stating that an injury in fact "may exist solely by virtue of 'statutes creating legal rights, the invasion of which creates standing.'" *Warth v. Seldin*, 422 U.S. 490, 500 (1975) (citation omitted). Congress' power to affect standing allows it to "define injuries and articulate chains of causation that will give rise to a case or controversy where none existed before." *Massachusetts v. EPA*, 549 U.S. 497, 516 (2007) (quoting *Lujan*, 504 U.S., at 580) (Kennedy, J., concurring) (emphasis added). In creating new rights, however, "Congress must at the very least identify the injury it seeks to vindicate and relate the injury to the class of persons entitled to bring suit." *Id.*

In enacting privacy laws, Congress has complied with the above requirements. Privacy laws define a range of injuries relating to the improper collection, handling, and disclosure of personal information, and relate these injuries to specific classes of persons entitled to bring suit. For example, in the Wiretap Act, 18 U.S.C. § 2511 *et seq.* (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." Pub. L. 90-351, § 801 (1968). Finally, 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). Thus,

the Wiretap Act is not like the Endangered Species Act at issue in *Lujan*, which gave "any person" the right to enjoin the United States for any "violation of any provision" 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.

Likewise, after the public disclosure of Supreme Court nominee Robert Bork's video rental records, *see* S. Rep. No. 100–599, at 4-5 (1988), Congress passed the Video Privacy Protection Act, 18 U.S.C. § 2710 (2006). Congress defined the injury to privacy as the "knowing[] disclos[ure], to any person, [of] personally identifiable information concerning any consumer of [a video tape service] provider . . . ." 18 U.S.C. § 2710(b) (2006). Congress specified that "any person aggrieved by an act of a [video tape service provider] in violation of this section may bring a civil action" in court. *Id.* at § 2710(c). Thus, the class of individuals entitled to sue is equal to the class of individuals suffering the statutory violation.

Congress has passed many other statutes protecting specific classes of individuals against privacy injuries.[6] Under these laws, plaintiffs

---

[6] *See* Telephone Consumer Protection Act, 47 U.S.C. § 227 (2006); Cable Communications Privacy Act, 47 U.S.C. § 551 (2006); Fair Credit Reporting Act, 15 U.S.C. § 1681n (2006); Truth in Lending Act, 15 U.S.C. § 1640 (2006); Fair and Accurate Credit Transactions Act 15 U.S.C. § 1681n (2006); Stored Communications Act, 18 U.S.C. § 2707(c) (2006); Foreign Intelligence Surveillance Act, 50 U.S.C. § 1828 (2006); Privacy Protection Act, 42 U.S.C. §

bringing suit assert their own rights against the unlawful intrusion, the misuse of their data, the inadequate security practices, and so forth, and not the rights of others. Thus, privacy plaintiffs possess 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. at 517.

Because Congress can define injuries by statute, "the invasion of which creates standing," *Warth*, 422 U.S., at 500, 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 a current Justice of this Court, 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.[7] It is only logical that injury in fact be

---

2000aa (2006); Right to Financial Privacy Act, 12 U.S.C. § 3417 (2006).

[7] *See Havens Realty Corp. v. Coleman*, 455 U.S. 363 (1982) (holding that African-American testers had standing to enforce the Fair Housing Act even though the challenged violation could not have harmed them because

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.

Indeed, the distinction between injury-in-fact and resulting harm is especially important in the context of privacy laws, because individuals rarely experience the harmful consequences concurrently with the statutory violation. For example, the Driver's Privacy Protection Act ("DPPA") prohibits any person from unlawfully obtaining or disclosing personal information from a motor vehicle record. 18 U.S.C. § 2722(a). Congress passed DPPA to prevent harms similar to those that affected Rebecca Schaeffer, a young actor who was stalked and murdered after her killer obtained her home address from the California Department of Motor Vehicles. 139 Cong. Rec. S15762 (Nov. 16, 1993) (statement of Sen. Boxer). The congressional record is filled with the stories of other victims who have been murdered, stalked, threatened, or robbed as a result of the disclosure of

---

they never intended to rent from the discriminatory realtor); *Heckler v. Matthews*, 465 U.S. 728 (1984) (male plaintiff had standing to challenge a gender-based social security classification despite the fact that invalidating the classification would not affect the amount of benefits he received); *Adarand Constructors, Inc. v. Pena*, 515 U.S. 200 (1995) (holding that nonminority contractors had standing to challenge a government program that that gave preference to minority contractors without the need to show that they would have received the contracts in the absence of discrimination).

their personal information. *See id.* at S15765 (statement of Sen. Robb). In these cases, the injury in fact occurs at the moment an individual's driving records are disclosed in violation of the statute. The resulting harm, however, may not occur until days, weeks, or even months later, when the victim is robbed, raped, or murdered. It is clear that robbery, rape, and murder constitute injuries sufficient to give a plaintiff standing under Article III; it is equally clear that by the time these harms materialize it is simply too late.

The recognition that the relevant injury occurs when the statute is violated, and not when the harm ultimately results, has led many courts to find standing for statutory violations of the DPPA. *See Graczyk v. West Pub. Co.*, 2011 WL 4469953, at *2 (7th Cir. Sept. 28, 2011) (holding that plaintiffs have standing to sue when their information was disclosed in violation of DPPA); *Parus v. Cator*, No. 05–C–0063–C, 2005 WL 2240955, at *5 (W.D. Wis. Sept. 14, 2005) ("It is true that plaintiff has not alleged that he suffered injury as a *result* of defendant Kreitlow's obtaining his personal information. However, under the statute, improperly obtaining plaintiff's information was an injury.") (emphasis in original); *Roberts v. Source for Public Data*, 2008 WL 5234675, at *5 (W.D. Mo. Dec. 12, 2008) ("The Complaint's allegations that the Defendants unlawfully obtained Plaintiffs' highly restricted personal information, in violation of their privacy rights under the DPPA, suffice to establish injury-in-fact."); *Johnson v. West Pub. Corp.*, 2011 WL 3422756, at *19 (W.D. Mo. Aug. 3, 2011) ("In fashioning the DPPA, Congress created

a right to privacy, the invasion of which creates an injury sufficient to create standing.").

The Federal Trade Commission's enforcement action against LexisNexis provides another crucial example of the distinction between injury in fact and resulting harm. *In the Matter of Reed Elsevier Inc. and Seisint Inc.*, FTC File No. 052-3094 (Mar. 27, 2008).[8] The FTC brought a complaint against LexisNexis after the company violated the FTC Act by collecting personal information, including social security numbers, from public and nonpublic sources, then failing to "provide reasonable and appropriate security" for this information. *Id.* at 3. Criminals exploited these inadequate security measures by accessing the database and gaining sensitive information about over 300,000 customers. In some cases, the criminals used the sensitive information to open credit accounts in the names of consumers whose information was disclosed and then made purchases using these accounts. *Id.* In other cases, criminals used the sensitive information to activate new credit cards that they had stolen from consumers. As above, the injury in fact occurred immediately, when LexisNexis allowed personal information to be disclosed, and not later, when the consumers learned that they had suffered financial harm from the unauthorized purchases.[9]

---

[8]http://www.ftc.gov/os/caselist/0523094/080327complaint.pdf

[9] A similar problem arose in the FTC's investigation of Choicepoint, a data broker that disclosed personal information of 163,000 American consumers to a criminal

Because standing depends on the existence of an injury in fact, and not the eventual occurrence of harmful consequences, the only circuits to have analyzed the question of standing in identity-theft cases have recognized that the injury occurs at the time of the breach. In *Pisciotta v. Old Nat. Bancorp*, the Seventh Circuit held that a class of consumers had standing to sue a bank whose poor security procedures resulted in the disclosure of their personal information. 499 F.3d 629 (7th Cir. 2007). Once the plaintiffs in *Piscotta* established that a breach occurred, "the fact that the plaintiffs anticipate[d] that some greater potential harm might follow the defendant's act d[id] not affect the standing inquiry." *Id.* at 634. In *Krottner v. Starbucks Corp.*, several employees sued Starbucks, claiming that the company's negligence caused the theft of a laptop containing social security numbers of approximately 97,000 Starbucks employees. 628 F.3d 1139 (9th Cir. 2010). The court held that plaintiffs had standing, even though some of them had suffered no "anxiety and stress," did not have to spend money for credit monitoring services, and had not suffered identity theft or fraudulent purchases. *Id.* at 1142-43. *See also Ruiz v. Gap, Inc.*, 380 Fed. App'x. 689 (9th Cir. 2010) (holding that a plaintiff had standing to sue over the alleged negligent disclosure of his social

---

ring engaged in identity theft. The FTC's action against the company was predicated on the improper disclosure, not on the harm that resulted. *See ChoicePoint Inc.*, FTC File No. 052-3069 (Jan. 26, 2006), http://www.ftc.gov/os/caselist/choicepoint/choicepoint.htm.

security number, even though he had "failed to establish a genuine issue of material fact on whether he suffered damages" resulting from the injury).

B. Statutory Damages Are Critical to the Structure of Modern Privacy Law

In ensuring that privacy laws would be effective, Congress relied on more than its ability to create standing. Indeed, without statutory damage provisions, privacy laws would create rights with no remedies. Statutory damage provisions ensure that individuals can seek compensation for and deter privacy violations. Privacy violations have long been redressable at common law, *see* Restatement (Second) of Torts §652A(1) (1977) ("One who invades the right of privacy of another is subject to liability for the resulting harm to the interests of the other."); *see*, *e.g.*, *Pavesich v. New England Life Ins. Co.*, 122 Ga. 190 (1905). However, Congress recognized that common-law tort and contract remedies do not adequately protect individual privacy. Harms suffered as a result of privacy violations are often difficult to quantify. Personal information is now routinely collected and stored in vast databases beyond individual control. Those individuals' interests are directly impacted by the use and disclosure of their information. Adopting the general framework of Fair Information Practices, Congress created statutory damage provisions to ensure adequate enforcement of privacy interests.

The nature of privacy dictates that privacy injuries are broader and more important than simple pecuniary loss. As Professor, and later Solicitor General, Charles Fried wrote, "privacy is not just one

possible means among others to insure some other value, [it is] necessarily related to ends and relations of the most fundamental sort: respect, love, friendship and trust." Charles Fried, *Privacy,* 77 Yale L.J. 475-93 (1968), reprinted in PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY 203, 205 (ed. Ferdinand D. Schoeman 1984). He concludes:

> The concept of privacy requires, as we have seen, a sense of control and a justified acknowledged power to control aspects of one's environment . . . we at once put the right to control as far beyond question as we can and at the same time show how seriously we take this right.

Id. at 219. Privacy laws seek to restore this control and the civil remedies provided are the means by which the "justified acknowledged power," in Professor Fried's phrase, is realized.

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, PRIVACY LAW AND SOCIETY 4 (2007). 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).

Privacy laws also guard against an increased risk of identity theft, financial loss, erroneous credit information, and even bodily harm. As with mental

and emotional distress or loss of reputation and trust, the harm that this increased risk represents is difficult to quantify. Even though an increased risk of future harm may confer standing, such a risk is typically insufficient to allow for recovery under common-law claims. *See, e.g., Pisciotta v. Old Nat. Bancorp*, 499 F.3d 629 (7th Cir. 2007) ("Without more than allegations of increased risk of future identity theft, the plaintiffs have not suffered a harm that the law is prepared to remedy."); *Ruiz v. Gap, Inc.*, 380 Fed. App'x. 689 (9th Cir. 2010) (denying recovery under breach of contract and invasion of privacy theories based on increased risk of identity theft); *Stollenwerk v. Tri-West Health Care Alliance*, 254 Fed. Appx. 664, 667 (9th Cir. 2007) (denying a claim for credit monitoring damages because plaintiffs did not show that their information was misused in any way, or that credit monitoring was necessary, "given that Plaintiffs could place fraud alerts with the major credit agencies and receive copies of their credit reports free of charge."). Perhaps the court in *In re JetBlue Airways Corp. Privacy Litigation* provides the bluntest illustration of the inadequacy of common-law remedies, denying a breach of contract claim because "[t]here is . . . no support for the proposition that an individual passenger's personal information has or had any compensable value in the economy at large." 379 F. Supp. 2d 299, 328 (E.D.N.Y. 2005). Thus, even when individuals are able to establish standing for privacy injuries, the increased risk of harm that individuals suffer will go unremedied without statutory damages.

III. Because New and Emerging Business Practices Pose a Particular Threat to Individual Privacy, Congress Must Maintain the Power to Define and Remedy Privacy Injuries.

Among amici for Petitioners are companies whose business practices implicate the very privacy interests that Congress' has sought to address through the enactment of federal privacy laws. These amici seek to avoid accountability for the collection and use of the personal information that they obtain. Facebook, et al. Br. 3. They hope to curtail Congress' long-established power to safeguard the privacy interests of American consumers. And they seek to set themselves apart from others—financial institutions, medical service companies, Internet service providers, telecommunications firms, cable operators, video rental service providers, educational institutions, and federal and state agencies—that are subject to federal privacy laws

The business practices of amici raise precisely the concerns that have typically given rise to action by Congress. In 2007, Facebook announced "Beacon", and began to routinely disclose information about the purchases of its users to the company's business partners without the consent of users. Beacon violated both the company's privacy policy, and, with respect to video rental information, the Video Privacy Protection Act. *See Harris v. Blockbuster Inc.*, 622 F. Supp. 2d 396 (N.D. Tex 2009); *Lane v. Facebook, Inc.,* 2009 WL 3458198 (N.D. Cal. Oct. 23, 2009). Facebook did not notify users of its change in business practices, nor did the company give users the ability

to opt out of the program. Instead, Facebook unilaterally decided to change the way it disclosed users' personal information. User protest eventually led Facebook to cancel Beacon. Jaikumar Vijayan, *Privacy advocates hail Facebook's plan to shutter Beacon*, COMPUTERWORLD (Sept. 28 2009).[10]

Google also dramatically changed its business practices by effectively requiring that users of Google's email service Gmail also subscribe to Google's social network service Buzz. Byron Acohido, *Google Buzz fuels rising privacy, security concerns*, USA TODAY (Feb. 16, 2010).[11] As a result, Google automatically disclosed pictures, video, text, and other data that users posted to websites such as Picasa and YouTube with the e-mail accounts of the users' frequent contacts. The company's disclosure of user data meant that, for example, the names of a doctor's patients, a journalist's contacts, or a lawyer's clients would be made public in violation of the confidentiality that normally attaches to those relationships. *See* Don Cruse, Lawyers (or Journalists) with Gmail Accounts: Careful with the Google Buzz, The Supreme Court of Texas Blog (Feb.

---

[10] *Available at* http://www.computerworld.com/s/article/9138373/Privacy_advocates_hail_Facebook_s_plan_to_shutter_Beacon.

[11] *Available at* http://content.usatoday.com/communities/technologylive/post/2010/02/google-buzz-facing-privacy-security-storm-1/1

11, 2010).[12] Eventually, the Federal Trade Commission undertook an investigation of Google Buzz and the program was discontinued. Federal Trade Commission, *FTC Charges Deceptive Privacy Practices in Google's Rollout of Its Buzz Social Network: Google Agrees to Implement Comprehensive Privacy Program to Protect Consumer Data* (Mar. 30, 2011).[13]

These emerging privacy risks, and the growing public concern about the misuse of personal data, make it especially important that Congress retain the power to respond to changing technology and new business practices by updating privacy laws to address new challenges. Although Petitioners' amici might prefer to avoid the responsibilities associated with the collection and use of personal information (even though many business in the United States are routinely subject to these obligations), they should not use this case to put their business activities beyond the reach of Congress. This Court has been vigilant in using the requirement of injury-in-fact to ensure that the Executive's duty to "take Care that the Laws be faithfully executed" is not infringed, *see Lujan*, 504 U.S. at 577 (quoting Art. II, § 3); it should be equally vigilant in guarding against transferring from Congress to the courts the vesting of "[a]ll legislative powers herein granted." Art. I, § 1.

---

[12] *Available at http://www.scotxblog.com/legal-tech/lawyer-privacy-on-google-buzz/.*

[13] *Available at* http://www.ftc.gov/opa/2011/03/google.shtm.

CONCLUSION

Amicus respectfully ask this Court to deny Petitioners' motion and uphold the decision of the Ninth Circuit and to remand to the district court with instructions to give full consideration to the merits of the plaintiff's claims.

Respectfully submitted,

MARC ROTENBERG
JOHN VERDI
ELECTRONIC PRIVACY
INFORMATION
CENTER (EPIC)
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140

October 18, 2011