No. 09-530

IN THE

Supreme Court of the United States

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION, et al.,

Petitioners,

v.

ROBERT M. NELSON, et al.,

Respondents.

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

BRIEF OF *AMICI CURIAE* ELECTRONIC PRIVACY INFORMATION CENTER (EPIC) AND LEGAL SCHOLARS AND TECHNICAL EXPERTS IN SUPPORT OF THE RESPONDENTS

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

August 9, 2010

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

OTHER AUTHORITIES

INTEREST OF THE *AMICI CURIAE*[1]

The Electronic Privacy Information Center (EPIC) 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 privacy issues, new technologies, and Constitutional interests, including *Doe v. Reed*, 130 S. Ct. 2811 (2010); *Quon v. City of Ontario*, 130 S. Ct. 2619 (2010); *Flores-Figueroa v. United States*, 129 S. Ct. 1886 (2009); *Herring v. United States*, 129 S. Ct. 695 (2009); *Crawford v. Marion County Election Board*, 128 S. Ct. 1610 (2008); *Hiibel v. Sixth Judicial*

---

[1] Letters of consent to the filing of this brief have been lodged with the Clerk of the Court pursuant to Rule 37.3. On May 5, 2010, Respondents lodged with the Court their "consent to the filing of amicus curiae briefs, in support of either party or of neither party." EPIC files Petitioners' letter of consent contemporaneously with 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 the brief was not authored, in whole or in part, by counsel for a party.

[2] EPIC is grateful for the work of EPIC Clerks Musetta Durkee, Rachel Gozhansky, Cynthia Grady, Gautam Hans, Matthew Lijoi, Eric Lindgren, Laura Moy, Reuben Rodriguez, and Geoff Schotter, who contributed to the preparation of this brief.

Circuit of Nevada, 542 U.S. 177 (2004); *Doe v. Chao*, 540 U.S. 614 (2003); *Smith v. Doe*, 538 U.S. 84 (2003); *Department of Justice v. City of Chicago*, 537 U.S. 1229 (2003); *Watchtower Bible and Tract Society of N.Y., Inc. v. Village of Stratton*, 536 U.S. 150 (2002); *Reno v. Condon*, 528 U.S. 141 (2000); *National Cable and Telecommunications Association v. Federal Communications Commission,* 555 F.3d 996 (D.C. Cir. 2009)*; Bunnell v. Motion Picture Association of America*, No. 07-56640 (9th Cir. filed Nov. 12, 2007); *Kohler v. Englade*, 470 F.3d 1104 (5th Cir. 2006) 470 F.3d 1104 (5th Cir. 2006); *United States v. Kincade*, 379 F.3d 813 (9th Cir. 2004), *cert. denied* 544 U.S. 924 (2005); and *State v. Raines*, 857 A.2d 19 (Md. 2003).

EPIC has a particular interest in protecting individuals' right to informational privacy.

EPIC supports the right of individuals to keep confidential their personal health information. EPIC has filed several *amicus* briefs concerning the critical importance of limiting the collection and disclosure of sensitive medical data.[3] This right is particularly important in light of the incomplete privacy protections provided by NASA's implementation of the Privacy Act and the substantial risk of data breaches. EPIC argues in this brief that NASA should not compel scientists to disclose personal health information as a condition of employment.

---

[3] *See, e.g., IMS Health v. Ayotte*, 550 F.3d 42 (1st Cir. 2008) *cert. denied* 129 S. Ct. 2864 (2009)*, IMS Health Inc. v. Sorrell*, 631 F. Supp. 2d 429 (D. Vt. 2009), *appeal docketed*, No. 09-1913 (2d Cir. Aug. 1, 2009).

The Ninth Circuit's determination in the present case protects the informational privacy of scientists working at the Jet Propulsion Laboratory. If the Court overrules the Ninth Circuit, it will require these scientists to disclose sensitive, personal information that is insufficiently protected and at substantial risk of disclosure.

Technical Experts and Legal Scholars

Dr. Alessandro Acquisti, Associate Professor of Information Technology and Public Policy, Carnegie Mellon University; Co-editor, *Digital Privacy: Theory, Technologies and Practices* (2007)

Steven Aftergood, Senior Research Analyst, Federation of American Scientists

Grayson Barber, Grayson Barber, LLC

Christine L. Borgman, Professor & Presidential Chair in Information Studies, UCLA; Author, *Scholarship in the Digital Age: Information, Infrastructure, and the Internet* (2007)

Julie Cohen, Professor, Georgetown University Law Center; Author, *Configuring the Networked Self: Copyright, Surveillance, and the Production of Networked Space* (Forthcoming Yale University Press 2011)

Whitfield Diffie, Dr. sc. techn. (hc), Vice President for Information Security and Cryptography at ICANN; Co-author, *Privacy on the Line* (2007)

Addison Fischer, Former owner, RSA Data Security, Co-founder, Verisign

Dr. David Flaherty, former Information and Privacy Commissioner, British Columbia, Canada; Author, *Protecting Privacy in Surveillance Societies* (1989)

Philip Friedman, Friedman Law Offices, PLLC

Deborah Hurley, Consultant

Jerry Kang, Professor of Law, UCLA; Author, *Communications Law and Policy* (3d ed., 2008)

Ian Kerr, Associate Professor, Canada Chair of Ethics, Law, and Technology, University of Ottawa; Co-Author, *Managing the Law: The Legal Aspects of Doing Business* (2d ed., 2005)

Chris Larsen, CEO and Co-Founder, Prosper Marketplace, Inc.

Gary Marx, Professor Emeritus, Massachusetts Institute of Technology; Author, *Undercover: Police Surveillance in America* (1989)

Mary Minow, LibraryLaw.com; Co-Author, *The Library's Legal Answer Book* (2003)

Pablo Molina, Chief Information Officer, Georgetown University Law Center

Dr. Peter G. Neumann, Fellow of AAAS, ACM, IEEE, SRI International; Author, *Computer Related Risks* (1994)

Helen Nissenbaum, Professor, New York University, Media, Culture, and Communication & Computer Science, Senior Faculty Fellow, Information Law Institute; Author, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (2009)

Deborah C. Peel, MD, Founder and Chair, Patient Privacy Rights

Chip Pitts, President, Bill of Rights Defense Committee, former Chairman, Amnesty International USA; Author, *Corporate Social Responsibility: A Legal Analysis* (2009)

Ron Rivest, Andrew and Erna Viterbi Professor of Electrical Engineering and Computer Science, Massachusetts Institute of Technology; Editor, *Introduction to Algorithms* (3rd ed. 2009)

Pamela Samuelson, Professor, Berkeley Law School & School of Information; Author, "*The New Economy, and Information Technology Policy*," *American Economic Policy in the 1990s,* Editors Jeffrey A. Frankel, Peter R. Orszag, MIT Press, 2002

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

Robert Ellis Smith, Publisher, *Privacy Journal*; Author, *Ben Franklin's Web Site: Privacy and Curiosity from Plymouth Rock to the Internet* (2000)

Dr. Latanya Sweeney, Distinguished Career Professor of Computer Science, Technology and Policy, Carnegie Mellon University; Author, *Computational Disclosure Control: A Primer on Data Privacy Protection* (1997)

Edward G. Viltz, President and Founder, Internet Collaboration Coalition

Christopher Wolf, partner, Hogan Lovells; Author, *Proskauer on Privacy: A Guide to Privacy and Data Security Law in the Information Age* (2006)

(Affiliations are for identification only)

SUMMARY OF THE ARGUMENT

The right to informational privacy protects critical Constitutional values. Since the Court's 1977 analysis in *Whalen*, scholars and international courts have described the importance of the right to informational privacy and opined on the right's vital role in safeguarding individuals from data collection and disclosure. The Ninth Circuit decision at issue in this case protects NASA scientists' right to informational privacy. Constitutional privacy safeguards are particularly important in this case because NASA's failure to meet its obligations under the Privacy Act and the agency's poor data security practices pose substantial risks to the scientists' personal information.

ARGUMENT

I. The Right to Informational Privacy is Well-Recognized

The parties have briefed U.S. courts' treatment of the right to informational privacy. Informational privacy rights have not been often litigated in this Court since *Whalen* and *Nixon*.[4] However, federal courts have interpreted informational privacy rights to protect individuals' freedom to withhold personal, sensitive health information from the government.[5] This interpretation supports Respondents ("the Scientists") in this case, and is consistent with the conclusions reached by scholars and international courts.

A. Scholars Recognize the Importance of the Right to Informational Privacy

Before *Whalen* and *Nixon*, Warren and Brandeis described the broad legal foundation of the right to privacy, describing privacy rights as "not rights arising from contract or from special trust, but are rights as against the world."[6] And Justice Brandeis famously described the right of privacy as "the most comprehensive of rights and the right most valued by

---

[4] *Whalen v. Roe*, 429 U.S. 589 (1977); *Nixon v. Administrator of General Services*, 433 U.S. 425 (1977).

[5] *E.g. Tucson Woman's Clinic v. Eden*, 379 F.3d 531, 537 (9th Cir. 2004); *Hawaii Psychiatric Soc'y v. Ariyoshi*, 481 F. Supp. 1028 (D. Haw. 1979).

[6] Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 213 (1890).

civilized men."[7] "To protect that right," Brandeis wrote, "every unjustifiable intrusion by the government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment."[8]

Since *Whalen* and *Nixon*, *The Right to Privacy* article, and the *Olmstead* dissent, scholars and advocates have worked to advance the claim of informational privacy. The academic consensus describes a robust, vital Constitutional right. 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. Legislating for informational privacy, in turn, requires a different kind of attention to the categories that have dominated the discussion about data privacy protection. Effective data privacy protection must delineate the appropriate boundary between ownership and speech, specify the parameters for effective consent, and impose meaningful procedural and substantive protections on information practices.[9]

---

[7] *Olmstead v. U.S.*, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

[8] *Id.*

[9] Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1435 (2000).

As Professor Pamela Samuelson explains, "In addition, it may be important to realize that our concept of information privacy, and in particular, our understanding of what is appropriate and inappropriate to do with personal information, is evolving over time."[10] Professor Anita Ramasastry stresses privacy's role in freedom: "As our society becomes less private, even with our consent at each step, the sum of all those steps may mean it also becomes less free."[11]

Privacy contributes to personal and social development, as many scholars have described. Professor Jeffrey Rosen states:

> There is also an important case for privacy that has to do with the development of human individuality. . . .
> We are trained in this country to think of all concealment as a form of hypocrisy. But we are beginning to learn how much may be lost in a culture of transparency: the capacity for creativity and eccentricity, for the

---

[10] Pamela Samuelson, Privacy As Intellectual Property, 52 STAN. L. REV. 1125, 1170-72 (2000).

[11] Anita Ramasastry, *Tracking Every Move You Make: Can Car Rental Companies Use Technology to Monitor Our Driving? A Connecticut's Court's Ruling Highlights an Important Question*, Findlaw News, Aug, 23, 2005, *available at* http://writ.news.findlaw.com/ramasastry/20050823.html.

> development of self and soul, for understanding, friendship, even love.[12]

Professor Anita Allen has written:

> 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. It is not simply that people need opportunities for privacy; the point is that their well-being, and the well-being of the liberal way of life, requires that they in fact experience privacy.[13]

Professor Gary T. Marx notes: "We assume, or at least morally expect, that under ordinary circumstances behavior behind closed doors, in darkness and at a distance will be protected from the eavesdropping of third parties."[14]

Professor Jerry Kang, a prominent legal scholar writing on communications, has described several purposes served by informational privacy. First, informational privacy helps individuals avoid the embarrassment that accompanies the disclosure of

---

[12] Jeffrey Rosen, *Why Privacy Matters*, WILSON Q., Autumn 2000, at 38.

[13] Anita Allen, *Coercing Privacy*, 40 WM. & MARY L. REV. 723, 756 (1999).

[14] Gary T. Marx, Commentary, *At-Home Spying: Privacy Wanes as Technology Gains; Surveillance May be Legal, But is that the Only Standard?*, L.A. Times, May 28, 2002, at 11.

certain personal details. Second, informational privacy helps individuals construct intimacy with others by preserving a body of personal information, which can be selectively shared to communicate trust. Third, informational privacy helps individuals avoid damaging misuses of information that may expose them to unnecessary prejudices. Finally, informational privacy helps to preserve human dignity.[15]

Scholars have also recognized the specific need to impose limits on data collection, that privacy is not simply the limit on the disclosure of personal information. Professor Helen Nissenbaum, a culture and communications scholar, has argued that "strict limits on incursions into the private lives of citizens" constitute a critical check against a potentially overreaching government. According to Nissenbaum:

> The checks and balances that constitute the right to privacy against government, such as limiting surveillance and placing restrictions on access to personal records, function to curtail such evils as government intimidation and totalitarian-style incursions into private life.[16]

Given the specific threats posed to privacy by the emergence of modern information systems,[17] it is also

---

[15] Jerry Kang, *Info. Privacy in Cyberspace Transactions,* 50 STAN. L. REV. 1193, 1212–16, 1260 (1998).

[16] Helen Nissenbaum, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 92 (2010).

[17] "So long as databases identify individuals by a universal identifier, such as a name or a government-issued identity

not surprising that experts in computer security have contributed to the formulation of the modern privacy right:

> Privacy is at the very soul of being human. . . . Privacy is the right to autonomy, and it includes the right to be let alone. Privacy encompasses the right to control information about ourselves, including the right to limit access to that information. The right to privacy embraces the right to keep confidence confidential and to share them in private conversation. Most important, the right to privacy means the right to enjoy solitude, intimacy, and anonymity.[18]

---

number, records can easily be propagated and merged, and thus they can be employed for secondary purposes to the individual's detriment." Philip E. Agre, *Beyond the Mirror World: Privacy and the Representational Practices of Computing*, *in* TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE 29, 53 (Philip E. Agre & Marc Rotenberg eds., 1997). *See also* Jerry Kang, *Cyberspace Privacy: A Primer and Proposal*, 26 HUM. RTS. 3 (1999) ("[P]ersonal data can be used to commit identity theft, in which an impostor creates fake financial accounts, runs up enormous bills, and disappears leaving only a wrecked credit report behind.").

[18] Whitfield Diffie & Susan Landau, PRIVACY ON THE LINE: THE POLITICS OF WIRETAPPING AND ENCRYPTION 126 (1998).

In a seminal article on the future of privacy, computer scientist David Chaum wrote:

> The choice between keeping information in the hands of individuals or of organizations is being made each time any government or business decides to automate another set of transactions. In one direction lies unprecedented scrutiny and control of people's lives, in the other, secure parity between individuals and organizations. The shape of society in the next century may depend on which approach predominates.[19]

Peter G. Neumann, a renowned computer scientist who specializes in computer-related risks, has also argued that "[s]acrificing privacy does not necessarily result in greater security." He warned that "serious inroads to privacy protection . . . may be very difficult to reverse."[20]

The protection of informational privacy remains central to the American experience. U.S. privacy commentator Robert Ellis Smith has said:

> [P]rivacy 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. Without privacy, there is no safe haven to know oneself. There is no space for

---

[19] David Chaum, *Achieving Electronic* Privacy, SCI. AM., Aug. 1992, at 96.

[20] Peter G. Neumann, *The Big Picture,* COMM. OF THE ACM, Sept. 2004, at 112.

> experimentation, risk-taking, and making mistakes. There is no room for growth. Without privacy there is no introspection; there is only group activity. Without privacy, everyone resembles everyone else. A number will do, everyone resembles everyone else. Without privacy, individuality perishes. Without individuality, there can be no group culture, or at least no group culture with any merit.[21]

The claim of informational privacy is not limited to the decisions and scholarship in the United States. As noted 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. The purpose of creating a constitutional right to privacy is not to leave data protection solely to the court except for the interpretation of the necessary statutes in statutes cases of conflict, but to allow

---

[21] Robert Ellis Smith, OUR VANISHING PRIVACY AND WHAT YOU CAN DO TO PROTECT YOURS 4 (1993), citing *Doe v. Bolton*, 410 U.S. 179 (1973).

> individuals to assert privacy claims that extend beyond the act. . . .
>
> All Western societies require constitutional standing for both data protection and information self-determination in accord with the census decision of the German Federal Constitutional Court. As Simitis has written: "Since this ruling at the latest, it has been an established fact in this country that the Constitution gives the individual the right to decide when and under what circumstances his personal data may be processed."[22]

The right to informational privacy has been broadly adopted in international treaties and declarations. Privacy experts Simon Davies and David Banisar have written:

> 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. . . .
>
> Privacy has roots deep in history. The Bible has numerous references to privacy. There was also substantive protection of

---

[22] David H. Flaherty, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES 376 (1998) (internal citation omitted).

privacy in early Hebrew culture, classical Greece and ancient China.[23]

The right to informational privacy "has spread to virtually every corner of European governance."[24]

B. International Courts Recognize the Right to Informational Privacy

Whalen v. Roe recognized the right to informational privacy as "the individual interest in avoiding disclosure of personal matters."[25] In 1983, the German Constitutional Court recognized the right of "informational self-determination."[26] The *Census* Case held that certain questions on the census survey exceeded the scope of government authority. In ruling for the citizens bringing the complaint, the German Constitutional Court found that the right of personality, already recognized in Articles I and II of the German Constitution, also entails "the right to information self-determination." This right to informational self-determination is two-fold: (1) it "protects the individual from borderless collection, storage, application, and transmission of

---

[23] David Banisar & Simon Davies, *Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments,* 18 J. MARSHALL. J. COMPUTER & INFO. L. 1, 6 (1999).

[24] Francesca Bignami, *The Case for Tolerant Constitutional Patriotism: The Right to Privacy Before the European Courts*, 41 CORNELL INT'L L.J. 211 (2008).

[25] *Whalen*, 429 U.S. at 599.

[26] *In re: Census Act*, 30 BVerfGE 1, 42-43 (Dec. 15, 1983).

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."[27] The *Census* case "compels the State to organize data processing so that personal autonomy will be respected."[28]

Whalen and the *Census* Case influenced international privacy jurisprudence, resulting in the widespread recognition of the right to informational privacy. International courts have invoked the right to informational privacy to protect individuals' interests in their personal medical information, as well as employees' interests in refusing to disclose sensitive information to employers.

In 2008, 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.[29] Two UK citizens requested destruction of their fingerprints and DNA samples after they were acquitted of criminal charges, but the UK police refused. Police

---

[27] Paul Schwartz, *The Computer in German and American Constitutional Law: Toward an American Right of Informational Self-Determination*, 37 AM. J. COMP. L. 675, 690 (1989).

[28] *Id.*

[29] *Case of S. and Marper v. The United Kingdom*, Applications nos. 30462/04 and 30566/04, Eur. Ct. H.R., Dec 4, 2008.

had collected the samples when the citizens were first charged. The court held that "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."[30]

Case of S. and Marper followed a 2004 European Court of Human Rights decision barring the Ukraine government from obtaining and disclosing confidential medical information without patients' consent.[31] The government obtained confidential information concerning psychiatric treatment of Mr. Panteleyenko, a citizen who was engaged in a civil lawsuit against the government.[32] This information was subsequently disclosed, without consent, at a public hearing.[33] The European Court of Human Rights found that the Ukraine government violated Mr. Panteleyenko's right to informational privacy by collecting and disclosing personal health information without consent.

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.[34] The Court held that

---

[30] *Id.* at ¶ 125.

[31] *Panteleyenko v. Ukraine*, App. No. 11901/02, Eur. Ct. H.R. 43 (2004).

[32] *Id.*

[33] *Id.*

[34] STC 202/1999, of Nov. 8 [Spanish Constitutional Court], cited in Javier Thibault Aranda, *Information Technology*

a database called "absent on medical grounds" was unconstitutional. The database 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 for the purpose of preserving the health of employees.

Other international courts have also applied the right to informational privacy to safeguard employment-related information.[35]

---

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).

[35] *E.g.* Joined Cases C-465/00, C-138-01, and C-139/01, *Rechnungshof v. Österreichischer Rundfunk and Others*, 2003 E.C.R. (May 20, 2003), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62000J0465:EN:HTML (holding 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); *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"); Case C-28/08 P, *Commission v. Bavarian Lager*, Court of Justice of the European Union, June 29, 2010 (holding that

II. The Privacy Act Would Not Sufficiently Protect Respondents' Information

NASA argues that the "informational privacy interests in this case are limited" because "information gathered in the background-check process is protected by the Privacy Act and other safeguards."[36] Attempting to narrow the scope of the Scientists' privacy interests, NASA ignores data collection and focuses on disclosure, alleging that "the essence of the privacy interest . . . is 'keeping personal facts away from the public eye.'"[37] NASA contends that it may collect sensitive information from the Scientists because the Privacy Act, 5 U.S.C. § 552a, will safeguard the data.[38]

However, the Privacy Act does not adequately protect the Scientists' privacy. The Privacy Act prohibits federal agencies from disclosing personal information in some circumstances. However, NASA has willfully disclosed employees' sensitive health information in the past, and subsequently argued that its disclosures were lawful. NASA has already announced its intent to exempt itself from Privacy Act obligations concerning the Scientists' SF-85 information in this case.

Even if the Scientists' information is ostensibly protected by the Privacy Act, it might be disclosed

---

disclosure of the identities of civil servants involved in regulatory investigations would violate their right to informational privacy).

[36] Pet. Br. at 18.

[37] *Id.* at 18, 24.

[38] *Id.* at 18.

through a data breach. The risks of such a disclosure are not, as petitioners claim, a "remote possibility." Instead, the risk of disclosure is substantial: Independent investigators recently highlighted the agency's vulnerability to data breaches.

A. NASA's Narrow Interpretation of "System of Records" Would Not Sufficiently Protect Respondents' Information

NASA has previously disclosed employees' sensitive health information. In *Randall v. NASA*, information about a NASA employee's psychiatric care was placed in a workers' compensation file and later disclosed by a NASA staff doctor at a staff meeting.[39] The employee sued, alleging that NASA violated the Privacy Act by disclosing the data. In its defense, "NASA claimed that Henson had failed to allege that the information divulged came from a record within a system of records."[40]

The Privacy Act states, "No agency shall disclose any record which is contained in a system of records . . . except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains . . ."[41] Regardless of content, information is only legally protected when it is organized within a "system of records."

"System of records" means "a group of any records under the control of any agency from which

---

[39] *Randall v. NASA*, 14 F.3d 1143, 1145 (6th Cir. 1994).

[40] *Id.* at 1146.

[41] 5 U.S.C. § 552a(b) (2010).

information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual . . . ."[42]

In *Randall*, NASA denied that the Privacy Act protected the agency employees' personal health records. NASA argued that the medical documents were not within a "system of records," and thus fell outside the statute's disclosure protections. Whether an organizational system is a "system of records" depends entirely on the method by which information is retrieved, rather than how or what information is stored.[43] In order to qualify as a system of records, information in a database must actually be retrieved by an individual's name or unique identifier. Even if an agency has a group of records from which information *may be* retrieved by name or identifier, courts do not consider such a group of records a "system of records" when the controlling agency "does not *in practice* use its system to retrieve information

---

[42] 5 U.S.C. § 552a(a)(5) (2010).

[43] *Savarese v. U.S. Dep't of Health, Education & Welfare*, 479 F. Supp. 304 (N.D. Ga. 1979) (holding that because personal information was "not keyed for retrieval by name or name-related identifiers" and "the only manner of retrieval would be a manual search of the entire file," defendant's disclosure of information about plaintiff was not unlawful under the Privacy Act); *Baker v. Dep't of Navy*, 814 F.2d 1381, 1384 (9th Cir. 1987), *cert. denied*, 484 U.S. 963 (1987) (stating that "the definition of 'system of records' makes coverage under the Act dependent upon the method of retrieval of a record rather than its substantive content").

keyed to individuals."[44] Although some provisions of the Privacy Act apply to "records" in general, most protections, including the protection against unauthorized disclosure, apply only to records maintained in "systems of records." As a result, many records containing sensitive information about individuals fall outside the protections of the Privacy Act.

In *Randall*, the district court agreed with NASA, dismissing the employee's claim. But the Sixth Circuit overruled.[45] Although NASA ultimately lost, this case demonstrates the agency's willingness to use a narrow interpretation of the Privacy Act's "system of records" definition to attempt to evade liability. Furthermore, the district court's decision agreeing with NASA highlights the specious nature of the agency's claim that the Privacy Act protects the Scientists' personal information.

Nearly from its inception, narrow interpretations of the Privacy Act's "system of records" definition have been criticized. The Privacy Protection Study Commission ("PPSC") issued a report on the Privacy Act in 1977.[46] This report concluded that, while the Privacy Act was a great step forward, narrow

---

[44] *Henke v. U.S. Dep't of Commerce*, 83 F.3d 1453, 1456 (D.C. Cir. 1996) (emphasis added); *see also Artz v. U. S.*, 275 F. App'x 569 (8th Cir. 2008) (holding that because records were retrieved by date, they did not come from a "system of records").

[45] *Id.* at 1149.

[46] U.S. Privacy Protection Study Comm'n, *Personal Privacy in an Information Society* (1977).

interpretations of "systems of records" were problematic.[47] The PPSC determined that narrowly construing "system of records" "undermines the Act's objective of allowing an individual to have access to the records an agency maintains about him, and . . . unnecessarily limits the Act's scope."[48]

Concern over agencies' narrow implementation of the Privacy Act has only grown since 1977. Because modern computer databases allow for retrieval of "records" by any number of means, commentators have argued for Congressional action to clarify the definition of a "system of records" to reflect these changes in technology.[49] Whereas the functionality of older databases provided few retrieval methods, modern databases allow for retrieval by any number of fields. For example, it would be trivial to retrieve a set of all records in which a Scientist answered "yes" to SF-85's drug use question. Under NASA's narrow interpretation of "system of records," the Privacy Act would not protect records retrieved by this method, since the agency's search was not "keyed for retrieval by name or name-related identifiers."[50]

---

[47] *Id.*

[48] *Id.*

[49] Julianne M. Sullivan, Comment, *Will The Privacy Act of 1974 Still Hold up in 2004? How Advancing Technology Has Created a Need for Change in the "System Of Records" Analysis*, 39 CAL. W.L. REV. 395 (2004).

[50] *Savarese*, 479 F. Supp. at 304.

B. The Privacy Act Includes Broad Exceptions that Permit Disclosure of Sensitive Documents by NASA

There are twelve exceptions to the Privacy Act's general prohibition against disclosure, some of which are extraordinarily broad.[51] If an agency determines that disclosure is permitted by an exception, it merely needs to keep an accounting of the date, nature, and purpose of the disclosure as well as the name and address of the person or agency to whom the disclosure is made.[52]

As a result of these exceptions, a record covered by the Privacy Act is not necessarily protected; Information can flow quite freely within, between, and outside agencies. For example, the PPSC noted that in the law enforcement context, "[t]he Privacy Act does not place an effective burden on, or barriers to, the free flow of information within the law enforcement and investigative community."[53]

There is substantial risk that NASA would disclose the Scientists' personal information pursuant to the "routine use" exception. This exception allows agencies to disclose records for any purpose "compatible" with the purpose for which the record was originally collected, as long as the agency publishes the routine use in the Federal Register.[54] Agencies have unlawfully used the "routine use"

---

[51] 5 U.S.C. § 552a(b)(1-12) (2010).

[52] 5 U.S.C. § 552a(c)(1) (2010).

[53] PPSC, *supra* note 46 at 516–21.

[54] 5 U.S.C. § 552a(b)(3) (2010).

exception as a purported basis for disclosing employees' sensitive information.[55]

It is important to note that agencies define their own routine uses. This gives agencies the opportunity to essentially create their own new exceptions to the Privacy Act's disclosure prohibition.

Moreover, NASA has breached its statutory obligations regarding routine uses and SF-85 as well as Form 42. The Privacy Act requires agencies to "publish in the Federal Register . . . each routine use of the records contained in the system, including the categories of users and the purpose of such use."[56] Agencies must also "inform each individual whom it asks to supply information, on the form which it uses to collect the information . . . the routine uses which may be made of the information."[57] However, the routine uses published in the Federal Register concerning SF-85 are not identical to the routine uses listed on the SF-85 form itself.[58] Worse, Form 42 lists

---

[55] *E.g. Covert v. Herrington*, 876 F.2d 751, 752-56 (9th Cir. 1989) (Holding that the Department of Energy violated the Privacy Act when it disclosed employees' responses to a security clearance questionnaire. The DOE unsuccessfully argued that the disclosure was lawful pursuant to the "routine use" exception.).

[56] 5 U.S.C. § 552a(e)(4) (2010).

[57] *Id.*

[58] *See e.g.*, *Privacy Act of 1974; Privacy Act System of Records*, 74 Fed. Reg. 50,247, 50,251-53 (Sept. 30, 2009); *see also* Office of Pers. Mgmt., *Questionnaire for Non-Sensitive Positions* (SF-85), J.A. 88-95.

no routine uses at all.[59] By failing to adequately "inform each individual whom it asks to supply information" about its routine uses, petitioner undermines its own assertion that the Privacy Act provides meaningful privacy protection.

Several of NASA's listed routine uses demonstrate that the Privacy Act does not, in practice, sufficiently protect the Scientists' privacy. On SF-85, the sixth routine use permits disclosure to contractors, grantees, experts, consultants, or volunteers when necessary to perform a function or service related to the record for which they have been engaged.[60] This creates the risk that personal information about the Scientists' drug counseling will be sent outside NASA, and potentially outside the government altogether. The fourth enumerated routine use listed on SF-85 allows disclosure to any source from which information is requested in the course of an investigation concerning the hiring or retention of an employee or other personnel action to the extent necessary to identify the individual, inform the source of the nature and purpose of the investigation, and to identify the type of information requested.[61] This raises the specter that personal information will be inadvertently disclosed to individuals listed as references by the Scientists.

---

[59] INV Form 42, *Investigative Request for Personal Information*, J.A. 96-97.

[60] J.A. 89.

[61] *Id.*

C. The Privacy Act Does Not Protect Respondents' Information Against NASA's Data Breaches

If NASA is permitted to collect the Scientists' personal health information, there is a substantial risk that the data will be disclosed as a result of a data breach. Even the most rigorous statutory protections are no guarantee against exposure of personal information in data breaches. A June 2007 report (the "Data Breach Report") published by the United States Government Accountability Office ("GAO") describes the frequency and breadth of such breaches.[62] "While comprehensive data do not exist, available evidence suggests that breaches of sensitive personal information have occurred frequently and under widely varying circumstances."[63] Over 570 data breaches were reported in the media from January 2005 through December 2006.[64] A survey of federal agencies "identified more than 788 data breaches at 17 agencies from January 2003 to July 2006 . . . . Most of these breaches have compromised data that included personally identifiable information . . . ."[65] The breaches "varied in size—for example, several affected fewer than five records,

---

[62] U.S. Gov't Accountability Office, *Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown* (2007).

[63] *Id.* at 5.

[64] *Id.*

[65] *Id.*

while a breach at a VA affected 26.5 million records."[66]

NASA is Particularly at Risk

NASA has been singled out for criticism concerning its network and data security practices. In October 2009, the GAO released a report titled *NASA Needs to Remedy Vulnerabilities in Key Networks* (the "NASA Report").[67] The NASA Report reviewed and criticized NASA's data security practices at several of NASA's centers, including the Jet Propulsion Laboratory ("JPL").[68] "NASA did not consistently implement effective controls to prevent, limit, and detect unauthorized access to its networks and systems."[69] In particular, NASA did not implement sufficient access controls,[70] it did not keep

---

[66] *Id.*

[67] U.S. Gov't Accountability Office, *NASA Needs to Remedy Vulnerabilities in Key Networks* (2009).

[68] *Id.* at 2.

[69] *Id.* at unpaginated "Highlights" section.

[70] "NASA did not adequately identify and authenticate users in systems and networks supporting mission directorates." *Id.* at 14. None of the NASA centers reviewed "sufficiently restrict[ed] access and privileges to only those users that needed access to perform their assigned duties." *Id.* at 15. "Although NASA has implemented cryptography, it was not always sufficient or used in transmitting sensitive information." *Id.* at 16. NASA "did not always adequately control the logical and physical boundaries protecting its information and systems." *Id.* "[F]irewalls at the centers did not provide adequate protection for the organization's networks, since they could be bypassed." *Id.* at 17. NASA "neither enforced

its software or system configurations up-to-date,[71] and it had not sufficiently implemented its information security program[72] as required by the Federal Information Security Management Act ("FISMA").[73] Because of NASA's vulnerabilities and shortfalls, "increased and *unnecessary risk exists*

---

stringent physical access measures . . . nor did it maintain and review . . . a current list of personnel with access to all IT-intensive facilities and properly authenticate visitors to these facilities." *Id.* at 18. Moreover, "NASA did not adequately segregate incompatible duties," which "increases the risk that erroneous or fraudulent transactions could be processed . . . ." *Id.* at 17-18.

[71] "For example, all three NASA centers had not applied a critical operating system patch, . . . increasing the risk of exposing critical and sensitive unclassified data to unauthorized access." *Id.* at 20. Furthermore, NASA's e-mail systems were "vulnerable to attack because their systems allowed various file types as extensions," creating an "increased risk . . . that an attacker could . . . execute malicious code and gain control of or compromise a system." *Id.*

[72] "NASA had not fully assessed its risks." *Id.* at 23. "The agency did not have a policy for malware incident handling and prevention." *Id.* at 24. "NASA's policies do not adequately describe physical access controls . . . ." *Id.* "NASA had developed contingency plans for the five systems and networks we reviewed. However, shortcomings existed in several plans." *Id.* at 27. "Although NASA regularly monitored its unclassified network for security vulnerabilities, the monitoring was not always comprehensive." *Id.* at 17.

[73] FISMA was enacted as title III, E-Government Act of 2002, Pub. L. No. 107-347 (Dec. 17, 2002).

that sensitive information is subject to unauthorized disclosure, modification, and destruction . . . ."[74] The NASA Report made eight recommendations; NASA ultimately failed to dispute the report's conclusions.[75] Indeed, "NASA recognizes there are still significant gaps" in its technology security posture.[76]

The NASA Report details actual attacks leveled against the agency. "During fiscal years 2007 and 2008, NASA reported 1,120 security incidents . . . ."[77] This includes 839 "malicious code attacks," the "highest experienced by any of the federal agencies . . . account[ing] for over one-quarter of the total number of malicious code attacks directed at federal agencies during this period."[78] Over the same period of time, "NASA reported 209 incidents of unauthorized access" to sensitive data.[79] For at least one such breach, the "incident report does not indicate whether this lost data was unencrypted or encrypted or how the incident was resolved."[80]

---

[74] U.S. Gov't Accountability Office, *supra* note 67, at unpaginated "Highlights" section (emphasis added).

[75] *Id.* app. VI at 44-47 (Letter from Lori B. Garver, Deputy Administrator of NASA, to Gregory C. Wilshusen, Director, Information Security Issues, U.S. Gov't Accountability Office (Oct. 9, 2009)).

[76] *Id.* app. VI at 44.

[77] *Id.* at 32.

[78] *Id.* at 33.

[79] *Id.*

[80] *Id.* at 33.

The NASA Report was particularly critical of NASA's contract with JPL. Although the contract "specified adherence to certain NASA security policies, it did not require [JPL] to implement key elements of an information security program."[81] In addition, NASA failed to "incorporate provisions in the contract to allow it to perform effective oversight of [JPL]'s implementation of the security controls and program."[82] As a result, "NASA faces a range of risks from contractors and other users with privileged access to NASA's systems, applications, and data since contractors . . . can introduce risks to their information and information systems."[83]

The dramatic flaws in NASA's data storage networks place the Scientists' data at substantial risk. The risk of a data breach at NASA fatally undermines the agency's asserted distinction between collection and disclosure. NASA argues that "this case presents no realistic threat of public disclosure of information that comes into the

---

[81] *Id.* at 30-31. The NASA Report listed four FISMA and NASA requirements not met by the JPL contract: (1) "periodic testing and evaluation of the effectiveness of information security policies"; (2) a "process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in the information security policies"; (3) "[p]rocedures for detecting, reporting, and responding to security incidents"; and (4) "[p]lans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency."

[82] *Id.* at 31.

[83] *Id.*

government's possession."[84] Because there are "numerous statutory and regulatory protections for information obtained through the background-check process," NASA claims that its background-check program does not "implicate[] the principal concern for the privacy of personal information."[85] Even assuming, *arguendo*, that such statutory protections are meaningful in this case, the well-documented, ubiquitous, imminent threat of data breaches demonstrates that NASA's data collection does "implicate[] the principal concern for the privacy of [the Scientists'] personal information." The only way that NASA can in good faith assure the Scientists that their information will not be disclosed is not to collect it in the first place.

---

[84] Pet. Br. at 27.

[85] *Id.* at 30.

CONCLUSION

Amici respectfully ask this Court to deny Petitioners' motion and uphold the decision of the lower court.

Respectfully submitted,

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

August 9, 2010