No. 16-36038

IN THE UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT

JANE DOES 1-10 and JOHN DOES 1-10

Plaintiffs-Appellees,

v.

DAVID DALEIDEN,

Defendant-Appellant,

UNIVERSITY OF WASHINGTON;
PERRY TAPPER, in his official capacity,

Defendants-Appellees.

On Appeal from the United States District Court for the Western District of Washington, Case No. 16-cv-1212-JLR, Honorable James L. Robart

Brief of Amicus Curiae Electronic Privacy Information Center (EPIC) in Support of Plaintiffs-Appellees

Marc Rotenberg
Alan Butler
John Davisson
Electronic Privacy Information Center
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140

Counsel for Amicus Curiae

March 16, 2017

CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rules of Appellate Procedure 26.1 and 29(c), Amicus Curiae Electronic Privacy Information Center ("EPIC") is a District of Columbia corporation with no parent corporation. No publicly held company owns 10% or more of EPIC stock.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

OTHER AUTHORITIES

INTEREST OF THE AMICUS[1]

The Electronic Privacy Information Center ("EPIC") is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and other constitutional values. EPIC is also a leading advocate for government transparency, frequently requesting records under the Freedom of Information Act ("FOIA") concerning government activities that affect privacy.

As *amicus curiae*, EPIC has routinely argued for both personal privacy and government transparency. *See* Br. of *Amici Curiae* EPIC and 16 Legal Scholars and Technical Experts in Support of Respondent, *Dep't of Treasury v. City of Chicago*, 537 U.S. 1229 (2003) (judgment vacated and remanded) (arguing that records can be disclosed in electronic format without revealing personally identifiable information); Br. of *Amicus Curiae* EPIC in Support of Appellant and Urging Reversal, *Chicago Tribune Co. v. Bd. of Trustees of the Univ. of Ill.*, 680 F.3d 1001 (7th Cir. 2012) (arguing that the federal student privacy law barred disclosure of certain educational records under the state open government law); Br. for EPIC and Technical Experts and Privacy Scholars, *Ostergren v. Cuccinelli*, 615

[1] The parties consent to the filing of this brief. In accordance with Rule 29, the undersigned states that no monetary contributions were made for the preparation or submission of this brief. Counsel for a party did not author this brief, in whole or in part.

F.3d 263 (4th Cir. 2010) (arguing that the state should limit disclosure of SSNs under the open records law, but that publishing of those records by a privacy advocate seeking to draw attention to the state's practices was protected by the First Amendment); *see also* Br. of *Amici Curiae* EPIC and Legal Scholars and Technical Experts in Support of Respondents, *NASA v. Nelson*, 562 U.S. 134 (2011) (arguing that the right to informational privacy is well recognized and that the Privacy Act would not sufficiently protect information that NASA sought to collect about JPL employees); Br. of *Amici Curiae* EPIC and Legal Scholars and Technical Experts in Support of Petitioners, *FCC v. AT&T*, 562 U.S. 397 (2011) (arguing that personal privacy protections under the federal open government laws were not intended to protect corporations); Br. of *Amici Curiae* EPIC in Support of Appellant and Urging Reversal, *Doe v. Luzerne County, PA*, 660 F.3d 169 (3d Cir. 2011) (arguing that disclosure of digital video and images of the plaintiff's body implicated the right to informational privacy and constituted personally identifiable information giving rise to constitutional privacy interests).

Open government laws and privacy laws are complimentary: the aim is to maximize both the public's access to information about the government and to safeguard personal privacy to the greatest extent feasible. This is reflected in the original language of the federal Freedom of Information Act as well as in cases concerning the constitutional right to informational privacy. In cases where courts

are asked to consider how to reconcile competing privacy and open government claims, courts should favor outcomes that advance both interests.

ARGUMENT

The District Court correctly protected both individual privacy and government transparency when it required the redaction of "all personally identifying information or information from which a person's identity could be derived with reasonable certainty." Imposing an injunction to limit disclosure of personally identifying information in the first instance is essential to protect the constitutional privacy rights of the individuals mentioned in the documents. In the open government context, it is widely accepted that release of personal information by the government should be limited where the public interest in disclosure is minimal in order to protect the privacy interests of the individual. *See generally* 5 U.S.C. §§ 552(b)(6); 552(b)(7)(C); *NARA v. Favish*, 541 U.S. 157 (2004).

There are also significant constitutional interests that should limit the disclosure of personal information in this case. The first is the right to associational privacy, which has long protected from government disclosure the names of individuals who engage in protected speech and association. *See NAACP v. Alabama ex. rel. Patterson*, 357 U.S. 449 (1958). The second is the constitutional right to informational privacy, which protects an "individual's interest in avoiding

disclosure of personal matters." *Nixon v. Adm'r of Gen. Servs.*, 433 U.S. 425, 457 (1977); *see also Whalen v. Roe*, 429 U.S. 589, 600 (1977).

I. Redaction of names and other personally identifying information promotes both the right to privacy and government transparency.

Open government requires the promotion of transparency and the protection privacy. Redacting names and other personally identifying information in government records is a well established mechanism for protecting personal information while still ensuring public to access government records. *See Dep't of Air Force v. Rose*, 425 U.S. 352, 380–81 (1971) ("redaction is a familiar technique in other contexts"); *Department of Justice Guide to the Freedom of Information Act: Exemption 6*, at 82 (2016).[2]

Over the last twenty years, EPIC has pursued hundreds of public records requests and obtained hundreds of thousands of pages of documents related to a wide range of government activities; EPIC has also litigated cases concerning the unlawful withholding of agency records. *See generally* EPIC, *FOIA Cases* (2017);[3] EPIC, *FOIA Gallery* (2016).[4] Of the hundreds of thousands of pages of government records obtained by EPIC and released to the public, many contain redactions to prevent unwarranted disclosure of personally identifying information

[2] *Available at* https://www.justice.gov/sites/default/files/oip/legacy/2014/07/23/exemption6_0.pdf.
[3] http://epic.org/foia/.
[4] https://epic.org/foia/gallery/2016/.

of employees, private individuals, and others whose identities are not a matter of public interest. But redacting personally identifying information does not typically detract from the ability of an open government litigator to obtain useful information about the government's activities, policies, and priorities. Only when the official conduct of a specific individual is at issue would the disclosure of identity become relevant.

For example, EPIC routinely requests contracts and statements of work related to government programs that involve surveillance or data collection. The names and identifying information of the individuals who submitted these proposals are typically redacted, but that does not prevent public scrutiny of the government programs. *See, e.g.*, Letter from Fred W. Allen, Chief Counsel, U.S. Dep't of the Army, to Julia Horwitz, EPIC FOIA Counsel, at 7 (Aug. 19, 2014).[5] EPIC also routinely requests records of communications concerning government surveillance programs, which include many redacted names and titles in official email exchanges. *See, e.g.*, EPIC, *Freedom of Information Act Documents: Tenth Release, EPIC v. FBI – Stingray / Cell Site Simulator* (May 31, 2013).[6]

While EPIC has worked to promote government transparency and to obtain government records on behalf of the public, we have simultaneously sought to

[5] http://epic.org/foia/army/EPIC-FOIA-Interim-Release-19-Aug-2014.pdf.
[6] http://epic.org/foia/fbi/stingray/FBI-FOIA-Release-05312013-s2-OCR.pdf.

ensure that individuals do not suffer unwarranted invasions of privacy as a result of government disclosures. For example, following a ruling in a FOIA case filed by a city to obtain gun sale records maintained by the federal agency charged with tracking such sales, *City of Chicago v. U.S. Dep't of Treasury*, 287 F.3d 628 (7th Cir. 2002), EPIC filed an *amicus curiae* brief at the certiorari stage arguing that the lower court had properly identified a technologically feasible method of coding the data such that release would safeguard individual privacy interests. Br. of *Amici Curiae* EPIC and 16 Legal Scholars and Technical Experts in Support of Respondent, *Dep't of Treasury v. City of Chicago*, 537 U.S. 1229 (2003) (No. 02-322) (vacating and remanding the lower court's judgment in light of a new statute passed by Congress).

Privacy interests are especially strong in the context of university records, where the exposure of personal information, including medical and financial records, implicates fundamental privacy interests and can chill the free exchange of ideas. In *Chicago Tribune Co. v. Bd. of Trustees of the Univ. of Ill.*, 680 F.3d 1001 (7th Cir. 2012), EPIC filed an *amicus curiae* brief in a case brought by a news organization for access to university application records as part of an investigative series. EPIC recognized the important press interest in pursuit of the investigation but argued that the University was right to withhold records of specific students, which are also protected under federal law. Br. of *Amici Curiae* EPIC and Legal

Scholars and Technical Experts in Support of Petitioners, *FCC v. AT&T*, 562 U.S. 397 (2011) (No. 09-1279).

The Supreme Court has recognized that public interest in the disclosure of names and other identifying information is too attenuated to outweigh individual privacy interests where release of names would not "'shed light on an agency's performance of its statutory duties' or otherwise let citizens know 'what their government is up to.'" *Bibles v. Oregon Natural Desert Association*, 519 U.S. 355, 356 (1997). Also, some claims that information is subject to protection as personally identifiable are simply not correct as a matter of law. In *FCC v. AT&T*, 562 U.S. 397 (2011), EPIC argued in support of a federal agency that sought to disclose information about a corporation that was subject to investigation and subsequently claimed a personal privacy exemption. EPIC wrote that corporate entities do not have personal privacy interests and, thus, that disclosure of their information under the FOIA is entirely appropriate. Br. of Amici Curiae EPIC and Legal Scholars and Technical Experts in Support of Petitioners, *FCC v. AT&T*, 562 U.S. 397 (2011) (No. 09-1279). Chief Justice Roberts agreed and famously wrote, "The protection in FOIA against disclosure of law enforcement information on the ground that it would constitute an unwarranted invasion of personal privacy does not extend to corporations. We trust that AT&T will not take it personally." *Id*. 409–10.

Personally identifiable information is the key concept in all modern privacy laws, regulations, and industry standards. Indeed, under many privacy regimes, personally identifiable information is the jurisdictional or substantive trigger. *See, e.g.*, Nat'l Conf. State Legislatures, *Security Breach Notification Laws* (2015) (listing data breach notification laws triggered by breach of PII enacted in forty-seven states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands).[7] *See also* Christopher Wolf, *Envisioning Privacy in the World of Big Data*, *in Privacy in the Modern Age: The Search for Solutions* 204, 207 (Marc Rotenberg, Julia Horwitz, & Jeramie Scott eds., 2015) ("Personally identifiable information ('PII') is one of the central concepts in information privacy regulation.").

II. The right to informational privacy is widely recognized as a significant constitutional protection for individuals.

Writing nearly a century ago, Justice Louis Brandeis described the right to privacy as "the most comprehensive of rights and the right most valued by civilized men." 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting). "To protect that right," Brandeis wrote, "every unjustifiable intrusion by the government upon the privacy of the individual, whatever the means employed" must be held unconstitutional. *Id.*

[7] http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

Since the Court's ruling in *Olmstead* (and those in *Nixon*, *Whalen*, and *Nelson*), scholars and advocates have worked to elucidate the right to informational privacy. The academic literature describes a robust Constitutional right. *See, e.g.*, Nadine Strossen, *Beyond the Fourth Amendment: Additional Constitutional Guarantees That Mass Surveillance Violates*, 63 Drake L. Rev. 1143, 1164 (2015) ("A government measure that infringes on informational privacy is subject to the heightened scrutiny that the Court applies to any measure infringing on a substantive due process right."); Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* 92 (2010) ("The checks and balances that constitute the right to privacy against government, such as . . . placing restrictions on access to personal records, function to curtail such evils as government intimidation and totalitarian-style incursions into private life."); A. Michael Froomkin, *Government Data Breaches*, 24 Berkeley Tech. L.J. 1019, 1021 (2009) ("[T]here is a constitutional right, either free-standing or based in Due Process, against government disclosure of personal data lawfully acquired under legal compulsion[.]"); Grayson Barber, *Personal Information in Government Records: Protecting the Public Interest in Privacy*, 25 St. Louis U. Pub. L. Rev. 63, 84 (2006) ("The U.S. Supreme Court's decision in *Whalen v. Roe* has generated appellate precedent for the proposition that the state is not free to

disclose confidential information about its citizens. A majority of circuit courts have accepted the constitutional right to information privacy.").

As Professor Julie E. Cohen explains, "Informational privacy is an essential building block for the kind of individuality, and the kind of society, that we say we value." Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 Stan. L. Rev. 1373, 1435 (2000). This right is all the more essential in an era increasingly awash with personal data. It is "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." Pamela Samuelson, *Privacy As Intellectual Property*, 52 Stan. L. Rev. 1125, 1170-72 (2000). Professor Anita Ramasastry warns that "[a]s 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." Anita Ramasastry, *Tracking Every Move You Make: Can Car Rental Companies Use Technology to Monitor Our Driving?*, Findlaw News (Aug, 23, 2005).[8]

Scholars have detailed the ways in which informational privacy contributes to personal and social development. Professor Anita Allen writes:

> There is both empirical evidence and normative philosophical argument supporting the proposition that paradigmatic forms of privacy (e.g., seclusion, solitude, confidentiality, secrecy, anonymity)

[8] http://writ.news.findlaw.com/ramasastry/20050823.html.

> 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.

Anita Allen, *Coercing Privacy*, 40 Wm. & Mary L. Rev. 723, 756 (1999).

Professor Jeffrey Rosen expands on this view:

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

Jeffrey Rosen, *Why Privacy Matters*, Wilson Q., Autumn 2000, at 38.

Professor Jerry Kang has identified several purposes served by informational privacy. Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 Stan. L. Rev. 1193 (1998). First, informational privacy helps individuals "avoid the simple pain of embarrassment" that accompanies the disclosure of certain personal details. *Id.* at 1212. Second, informational privacy helps individuals construct intimacy by allowing them to "selectively regulate the outflow of personal information to others." *Id.* at 1212–13.

Third—and most relevant to the instant case—informational privacy helps individuals avoid damaging misuses of information that may expose them to unnecessary prejudices. Professor Kang explains:

> [I]nformation can be misused by making us vulnerable to unlawful acts and ungenerous practices. After all, personal information is what the spying business calls "intelligence," and such "intelligence" helps

> shift the balance of power in favor of the party who wields it. To take a simple example, knowledge of our home phone number and address makes us more vulnerable to harassers and stalkers. . . .
>
> Individual vulnerability has social consequences. It chills individuals from engaging in unpopular or out-of-the-mainstream behavior. While uniform obedience to criminal and tort laws may deserve praise, not criticism, excessive inhibition—not only of illegal activity but also of legal, but unpopular, activity—can corrode private experimentation, deliberation, and reflection. The end result may be bland, unoriginal thinking or excessive conformity to unwarranted social norms.

Id. at 1214–15. This dimension of informational privacy extends well beyond one's name, address, and phone number to include a wide range of personally identifiable information. 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) (noting that "records can easily be propagated and merged, and thus they can be employed for secondary purposes to the individual's detriment"). Finally, Professor Kang notes that informational privacy also helps to preserve human dignity. Kang, *supra*, at 1260–65.

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

> [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 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.

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)).

Yet the recognition of a right to informational privacy is not limited to cases and articles in the United States. The right has been broadly adopted in international treaties and declarations and is deeply rooted in the history of many cultures. As privacy experts Simon Davies and David Banisar explain:

> Privacy is a fundamental human right recognized in the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and in many other international and regional treaties. Privacy underpins human dignity and other values such as freedom of association and freedom of speech. It has become one of the most important human rights issues of the modern age. . . .
>
> Privacy has roots deep in history. The Bible has numerous references to privacy. There was also substantive protection of privacy in early Hebrew culture, classical Greece and ancient China.

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). International privacy expert David Flaherty elaborates:

> 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 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."

David H. Flaherty, *Protecting Privacy in Surveillance Societies* 376 (1998) (internal citation omitted). Indeed, the right to informational privacy has spread "to virtually every corner of European governance" and well beyond. Francesca Bignami, *The Case for Tolerant Constitutional Patriotism: The Right to Privacy Before the European Courts*, 41 Cornell Int'l L.J. 211 (2008).

* * *

In *NASA v. Nelson*, 562 U.S. 134 (2011), Justice Alito, writing for the Court, noted that the mandatory collection of sensitive, personal information by the government "implicate[d] a privacy interest of constitutional significance." 562 U.S. at 147 (citing *Whalen v. Roe,* 429 U.S. 589, 599, 605 (1977)). In *Whalen*, the Court had said:

> We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files. The

> collection of taxes, the distribution of welfare and social security benefits, the supervision of public health, the direction of our Armed Forces, and the enforcement of the criminal laws all require the orderly preservation of great quantities of information, much of which is personal in character and potentially embarrassing or harmful if disclosed. The right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures.

Id. 605 (emphasis added).

The Court in *NASA v. Nelson* resolved the privacy matter on a statutory basis, finding that the Privacy Act provided sufficient protection for the claims asserted.

The Court here should either find that the statute provides an appropriate basis to exempt the personal information from the records that will otherwise be disclosed or recognize that there are privacy interests of "constitutional significance" and prevent disclosure on that basis.

CONCLUSION

EPIC respectfully requests that this Court affirm the lower court's preliminary injunction order.

March 16, 2017

Respectfully submitted,

/s/ Marc Rotenberg

Marc Rotenberg
Alan Butler
John Davisson
Electronic Privacy Information Center
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140

Counsel for Amicus Curiae

CERTIFICATE OF COMPLIANCE

This brief complies with the type-volume limitation of Fed. R. App. P. 29(a)(4) because it contains 3,458 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii). This brief also complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Office Word for Mac in 14 point Times New Roman style.

/s/ Marc Rotenberg
Marc Rotenberg

Dated: March 16, 2017

CERTIFICATE OF SERVICE

I hereby certify that on March 16, 2017, I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the CM/ECF system. I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the CM/ECF system.

/s/ Marc Rotenberg

Dated: March 16, 2017 Marc Rotenberg