

No. 26A308

In The
Supreme Court of the United States

September Term, 2026

**U.S. DEPARTMENT OF HOMELAND
SECURITY, ET AL.,**

Applicants,

vs.

LEAGUE OF WOMEN VOTERS, ET AL.,

Respondents.

**BRIEF OF *AMICUS CURIAE* OF THE SOCIETY
FOR THE RULE OF LAW IN OPPOSITION TO
APPLICATION TO STAY THE ORDER
OF THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

BALLARD SPAHR LLP

M. NORMAN GOLDBERGER

(Counsel of Record)

MATTHEW A. STOLOFF

LAURA K. GRANT

1735 Market Street, 51st Floor

Philadelphia, PA 19103-7599

215.864.8850

goldbergerm@ballardspahr.com

TABLE OF CONTENTS

	PAGE
INTEREST OF AMICUS CURIAE.....	1
SUMMARY OF ARGUMENT	1
ARGUMENT	4
I. Congress Enacted the Privacy Act to Protect Individuals from the Harm to Privacy in the Unchecked Collection and Dissemination of Personal Information	4
II. Compatibility Is Essential to the Privacy Act Framework.....	7
III. The Compatibility Analysis is Stringent.	12
IV. The Government Fails to Satisfy the Compatibility Analysis.	16
CONCLUSION	22

TABLE OF AUTHORITIES

Page(s)

Cases

<i>Advoc. Health Care Network v. Stapleton</i> , 581 U.S. 468, 137 S. Ct. 1652, 198 L. Ed. 2d 96 (2017)	9
<i>Ames v. United States Department of Homeland Security</i> , 861 F.3d 238 (D.C. Cir. 2017)	<i>passim</i>
<i>Britt v. Naval Investigative Serv.</i> , 886 F.2d 544 (3d Cir. 1989)	3, 8, 10, 11
<i>Chichakli v. Tillerson</i> , 882 F.3d 229 (D.C. Cir. 2018)	13, 14, 20
<i>Covert v. Harrington</i> , 876 F.2d 751 (9th Cir. 1989)	8
<i>Doe v. Chao</i> , 540 U.S. 614, 124 S.Ct. 1204, 157 L.Ed.2d 1122 (2004)	10
<i>Nielsen v. Preap</i> , 586 U.S. 392, 139 S. Ct. 954, 203 L. Ed. 2d 333 (2019)	9

<i>Roberts v. Sea-Land Services, Inc.</i> , 566 U.S. 93, 132 S.Ct. 1350, 182 L.Ed.2d 341 (2012)	10, 20
<i>Saunders v. Schweiker</i> , 508 F.Supp. 305 (W.D.N.Y. 1981)	11
<i>Stafford v. Social Sec. Admin.</i> , 437 F.Supp.2d 1113 (N.D. Cal. 2006)	12, 13, 18
<i>Townsend v. United States</i> , 236 F.Supp.3d 280 (D.C. 2017)	15
<i>Usher v. Secretary of Health and Human Services</i> , 721 F.2d 854 (1st Cir. 1983)	11
<i>USPS v. Nat’l Ass’n of Letter Carriers AFL-CIO</i> , 9 F.3d 138 (D.C. Cir. 1993)	8, 9
Statutes	
5 U.S.C. § 552a(a)(4)	19
5 U.S.C. § 552a(a)(7)	<i>passim</i>
5 U.S.C. § 552a(b)	7
5 U.S.C. § 552a(e)(4)(D)	8
Regulations	
20 C.F.R. § 401.150	18
90 FR 10026 (Feb 20, 2025)	16

Other Authorities

120 Cong. Rec. 36,894 (1974) (statement of Sen. Percy).....	11
DOJ, <i>Overview of the Privacy Act of 1974</i> (2020 ed.)	5
Report of the Secretary's Advisory Committee on Automated Personal Data Systems, DHEW Publication No. (OS) 73-94 (July 1973), https://www.justice .gov/opcl/docs/rec-com-rights.pdf (last accessed: Sept. 15, 2026)	6

INTEREST OF AMICUS CURIAE¹

Amicus The Society for the Rule of Law and Democracy, Inc., doing business as The Society for the Rule of Law (“SRL”), is a national non-profit, non-partisan membership organization of conservative, libertarian, and right-of-center lawyers, and others, who are dedicated to defending the constitutional principles of the rule of law, limited government, separation of powers, federalism, and other checks and balances regardless of politics or party affiliation.

SUMMARY OF ARGUMENT

The Privacy Act of 1974 was enacted to address concerns that the federal government’s growing

¹ No counsel for any party authored this brief in whole or in part, and no person or entity, other than SRL and its counsel, made a monetary contribution to fund the brief’s preparation or submission. The views of SRL do not necessarily reflect the views of all its individual members.

capacity to collect, store, and disseminate personal information posed a serious threat to individual privacy.

A key component of the Privacy Act is a simple but powerful principle: personal records collected by a federal agency for one purpose may not be disclosed for an incompatible purpose. The Privacy Act permits disclosure for a “routine use,” but only when that use is “compatible with the purpose for which [the record] was collected.” 5 U.S.C. § 552a(a)(7).

To ensure that a federal agency’s disclosure is compatible for a routine use, the government must show that there is a genuine nexus between the purpose of collection and the purpose of disclosure to another federal agency. As the Third Circuit put it, the statutory requirement of compatibility requires “a dual inquiry into the purpose for the collection of the

record in the specific case and the purpose of the disclosure.” *Britt v. Naval Investigative Serv.*, 886 F.2d 544, 548 (3d Cir. 1989). Compatibility is the “meaningful degree of convergence” between the two purposes, not mere relevance or utility for such disclosure. *Id.* at 549.

In its Application for Stay, the government fails to demonstrate that the Social Security Administration’s purpose in *collecting* the social security data is compatible with the purpose in *disclosing* it to the Department of Homeland Security. Instead, the government focuses on the ubiquity of Social Security numbers as identifiers. This does not meet the compatible analysis. The risk to individual privacy will be magnified if the government is permitted to disregard the compatible analysis.

ARGUMENT

I. Congress Enacted the Privacy Act to Protect Individuals from the Harm to Privacy in the Unchecked Collection and Dissemination of Personal Information

The Privacy Act of 1974 was born of a specific legislative concern. Congress found that “the increasing use of computers and sophisticated information technology . . . has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use, or dissemination of personal information.” Privacy Act of 1974, Pub. L. No. 93-579, § 2(a)(2), 88 Stat. 1896, 1896. As Congress was drafting the Privacy Act, it “relied on a recently published and widely read report,” Records, Computers, and the Rights of Citizens: Secretary’s Advisory Committee on Automated Personal Data Systems, published by what was then the Department

of Health, Education & Welfare (the “HEW Report”).² The HEW Report was a “comprehensive study of the risks to privacy presented by the increasingly widespread use of electronic information technologies[.]”³

The HEW Report addressed the establishment and use of personal data systems by government agencies in a chapter titled “Recommended Safeguards for Administrative Personal Data Systems”:

Formalized administrative procedures and requirements should be followed to assure that questions about the purposes, scope, and utility of systems are raised and confronted before systems are established or enlarged. Members of the public should also have an opportunity to comment on systems before they are created.

² DOJ, *Overview of the Privacy Act of 1974*, at 1 (2020 ed.), <https://perma.cc/6SB9-XAEK>.

³ *Id.*

It is especially important that such procedures be followed whenever data collection, imposed by any Federal department or agency on States, other grantees, or regulated organizations, are likely to result in the creation or enlargement of personal data systems. In our view, any such data collection requirement should be established by regulations adopted after the public has been given an opportunity to comment, rather than by less formal means, such as program guidelines or manuals. Adoption of a regulation also forces a federal agency to go through a formal process of internal justification and executive review. In the case of Federal data-collection requirements, the notice of any proposed regulation should contain a clear explanation of why each item of data is to be collected and why it must be collected and stored in identifiable form, if such is proposed.⁴

The HEW Report recognized the dangers inherent in the collection and dissemination of personal data by government agencies, and urged lawmakers to enact

⁴ Records, Computers, and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems, DHEW Publication No. (OS) 73-94 (July 1973) (hereinafter HEW Report), <https://www.justice.gov/opcl/docs/rec-com-rights.pdf> (last accessed: Sept. 15, 2026).

safeguards that required transparency and opportunity for comment by the individuals whose data was being collected and potentially shared.

II. Compatibility Is Essential to the Privacy Act Framework.

Unless a government agency obtains consent from an individual, disclosure of an individual's records to another agency is not permitted unless there is an applicable exception. 5 U.S.C. § 552a(b). One exception arises when there is a "routine use," which requires disclosures to be "both (i) 'for a purpose which is compatible with the purpose for which it was collected' and (ii) within the scope of a routine use notice published by the agency." *Ames v. United States Department of Homeland Security*, 861 F.3d 238, 240 (D.C. Cir. 2017) (citing 5 U.S.C. §§ 552a(a)(7), 552a(e)(4)(D)).

The Privacy Act defines “routine use” to mean “the use of [a] record for a purpose which is compatible with the purpose for which it was collected.” 5 U.S.C § 552a(7). The Privacy Act does not define the word “compatible,” but two courts have proposed definitions that are consistent with the overarching purpose of the Privacy Act. *Britt v. Naval Investigative Serv.*, 886 F.2d 544, 549-50 (3d Cir. 1989); *USPS v. Nat’l Ass’n of Letter Carriers AFL-CIO*, 9 F.3d 138, 144 (D.C. Cir. 1993).

In *Britt*, the United States Court of Appeals for the Third Circuit characterized “compatible” as one in which there is a “concrete relationship or similarity, some meaningful degree of convergence, between the disclosing agency’s purpose in gathering the information and in its disclosure.” 886 F.2d at 549-50 (citing *Covert v. Harrington*, 876 F.2d 751, 755 (9th

Cir. 1989)).

Similarly, in *USPS*, the D.C. Court of Appeals defines “compatible” to mean “capable of existing together without discord or disharmony.” 9 F.3d at 144.

There is a presumption that each word Congress uses in a statute is there for a reason. *Advoc. Health Care Network v. Stapleton*, 581 U.S. 468, 477, 137 S. Ct. 1652, 1659, 198 L. Ed. 2d 96 (2017) (citing A. Scalia & B. Garner, *Reading Law: The Interpretation of Legal Texts* 174–179 (2012)). As this Court has observed, words should be “given the meaning that proper grammar and usage would assign them.” *Nielsen v. Preap*, 586 U.S. 392, 408, 139 S. Ct. 954, 965, 203 L. Ed. 2d 333 (2019) (*quoting* A. Scalia & B. Garner, *Reading Law: The Interpretation of Legal Texts* 140)).

At the same time, words must be read “in their context and with a view to their place in the overall statutory scheme.” *Roberts v. Sea-Land Services, Inc.*, 566 U.S. 93, 101, 132 S.Ct. 1350, 182 L.Ed.2d 341 (2012).

Compatibility is a keystone of the Privacy Act. “One of the goals of the [Privacy] Act was to prevent the federal government from maintaining in one place so much information about a person that that person could no longer maintain a realistic sense of privacy.” *Britt*, 886 F.2d at 550. *See also Doe v. Chao* (“Chao I”), 540 U.S. 614, 618, 124 S.Ct. 1204, 157 L.Ed.2d 1122 (2004) (observing that the Privacy Act is intended “to protect the privacy of individuals identified in information systems maintained by Federal agencies” and it is necessary “to regulate the collection, maintenance, use, and dissemination of information

by such agencies”) (*quoting* Privacy Act of 1974, Pub. L. No. 93-579, § 2(a)(5), 88 Stat. 1896). *See also Usher v. Secretary of Health and Human Services*, 721 F.2d 854, 856 (1st Cir. 1983) (“[T]he purpose of the statute is ‘to let citizens know why and for what reasons the United States is asking them questions.’”) (*quoting Saunders v. Schweiker*, 508 F.Supp. 305, 309 (W.D.N.Y. 1981)).

The compatibility requirement of the Privacy Act is designed to “limit[] interagency exchange of information.” *Britt*, 886 F.2d at 550. “When personal data collected by one organization for a stated purpose is used and traded by another organization for a completely unrelated purpose, individual rights could be seriously threatened.” *Id.* (*quoting* 120 Cong. Rec. 36,894 (1974) (statement of Sen. Percy)).

III. The Compatibility Analysis is Stringent.

In cases involving the routine use exception, courts have closely examined whether the disclosure was compatible with the purpose for collecting the information.

One illustrative case, which highlights the importance of the compatibility analysis in the Social Security data context, is *Stafford v. Social Sec. Admin.*, 437 F.Supp.2d 1113 (N.D. Cal. 2006). There, the plaintiff was suspected of child abuse, and a social worker who conducted the child abuse investigation contacted the Social Security Administration to determine why the plaintiff was receiving benefits. *Id.* at 1114-16. A Social Security Administration employee provided the requested information without plaintiff's authorization. *Id.* at 1116. The district court held that the routine use exception did not apply. *Id.*

at 1118. Specifically, the district held that because the social worker sought the information to determine if the plaintiff's child should be removed from the home, and not to determine eligibility for an income-maintenance program or related medical benefits, the disclosure "was not compatible with the purpose for which the information was collected." *Id.* at 1120-21.

By contrast, in *Chichakli v. Tillerson*, 882 F.3d 229, 231 (D.C. Cir. 2018), the Treasury Department's Office of Foreign Assets Control determined that Chichakli was acting on behalf of an arms-trafficker and placed Chichakli's name, social security number, date of birth, aliases, residential and business addresses, and country of origin, on a list that was transferred to the Department of State and the United Nations. *Id.* The United Nations then published Chichakli's personal information online. *Id.* The Court

of Appeals held that the State Department’s disclosures were compatible for the purposes for which the information was collected. “The purpose for collecting Chichakli’s identifying information—to investigate whether to designate him for economic sanctions and to implement the sanctions—is precisely aligned with the purpose of disclosure—to implement the sanctions by publishing the information to the public. This is true for OFAC, as well as the Department of State.” *Id.* at 233-234.

Similarly, in *Ames v. United States Dep’t of Homeland Sec.*, 861 F.3d 238, 239 (D.C. Cir. 2017), Ames was an employee at the U.S. Department of Homeland Security who improvidently granted two security clearances and made false statements during an investigation conducted by the Office of Inspector General. But before the Inspector General’s report

was completed, Ames left her position for another job at the Department of Defense. *Id.* When the Department of Homeland Security sent the Inspector General's report to the Department of Defense, Ames was terminated from her employment. *Id.* The court held that the disclosure of the Inspector General's report to the Department of Defense "was compatible with the purpose for which the report was collected" because the purpose of the report was to determine whether Ames committed wrongdoing that could affect her suitability for employment at other federal agencies. *Id.* at 240. *See also Townsend v. United States*, 236 F.Supp.3d 280, 319 (D.C. 2017) (collecting cases).

As these cases illustrate, the government must demonstrate a close nexus between *collection* and *disclosure* of information before compatibility will be

found. The government has failed to do so here.

IV. The Government Fails to Satisfy the Compatibility Analysis.

The Social Security Administration collects data for the purposes of work authorization and eligibility for Social Security benefits, including but not limited to: for various Old Age, Survivors, and Disability Insurance (OASDI), Supplemental Security Income (SSI), and Medicare/Medicaid claims purposes, as well as “for the general administration of the Social Security Act to ensure the accuracy of enumeration related information in other SSA systems,” and “to record accurate earnings information . . .” 90 FR 10026 (Feb 20, 2025).

The federal regulations for the Social Security Administration contain specific guidelines to determine compatibility before sharing information:

(1) Disclosure to carry out SSA programs. We disclose information for published routine uses necessary to carry out SSA's programs.

(2) Disclosure to carry out programs similar to SSA programs. We may disclose information for the administration of other government programs. These disclosures are pursuant to published routine uses where the use is compatible with the purpose for which the information was collected. These programs generally meet the following conditions:

(i) The program is clearly identifiable as a Federal, State, or local government program.

(ii) The information requested concerns eligibility, benefit amounts, or other matters of benefit status in a Social Security program and is relevant to determining the same matters in the other program. For example, we disclose information to the Railroad Retirement Board for pension and unemployment compensation programs, to the Department of Veterans Affairs for its benefit programs, to worker's compensation programs, to State general assistance programs and to other income maintenance programs at all levels of government. We also disclose for health maintenance programs like Medicaid and Medicare.

(iii) The information will be used for appropriate epidemiological or similar research purposes.

20 C.F.R. § 401.150.

Here, as in *Stafford* the government has failed to demonstrate how the disclosure of Social Security data to the Department of Homeland Security “is compatible with the purpose for which the information was collected” by the Social Security Administration. *Stafford*, 437 F.Supp.2d at 1121. The government contends that “identification is the only use of the SSN” and summarily concludes this fact “is more than the necessary ‘meaningful degree of convergence’ between the collection purpose and disclosure purpose.” Application for Stay, at 22.

The government’s argument is conclusory and flawed for at least two reasons. *First*, the government overlooks the fact that an “identifying number,” such

as a Social Security number, is a “record” within the meaning of the Privacy Act. 5 U.S.C. § 552a(a)(4). *Second*, the government frames the compatibility inquiry around the general utility of Social Security numbers as identification tools, rather than examining the purpose for which Social Security Administration collected the specific information at issue. The government asserts that a “core ‘purpose’ of Social Security numbers . . . is to identify a particular individual.” Application for Stay at 23. The Privacy Act requires a different inquiry: whether the “purpose” for which the record was “collected” is “compatible with” the purpose for which it is being disclosed. 5 U.S.C. § 552a(a)(7). The subject of the inquiry is the agency’s *purpose in collecting* the record, not the general character of the data element itself. By failing to address this question, the

government has not offered any meaningful compatibility analysis sufficient to meet the requirements laid out in *Chichakli* and *Ames*. In short, the government has completely failed to show that the purpose for disclosure is compatible with the purpose for collection.

In his dissenting opinion, Judge Katsas makes two comments: First, Judge Katsas comments that there is no precise definition of compatibility. App. 147a. As discussed above, a precise definition is unnecessary so long as the term is understood “in their context and with a view to their place in the overall statutory scheme.” *Roberts*, 566 U.S.at 101.

Second, Judge Katsas opines that modified SAVE satisfies “any reasonable formulation of the compatibility test,” and that the disclosure of Social Security data to confirm voter eligibility “neither

conflicts with nor frustrates those initial purposes.” App. 147a-148a (*quoting Ames*, 861 F.3d at 240 n.1). But like the government, Judge Katsas does not explain how the Social Security Administration’s collection of Social Security data is compatible with the disclosure of such information for voter verification purposes. Judge Katsas’ assertion that a Social Security number is “a ‘nearly universal identifier’” (App. 148a) is not the issue. Rather, the issue is that the government has failed to show how the disclosure of Social Security data to confirm voter eligibility satisfies the compatibility analysis, which is a requirement of the Privacy Act. 5 U.S.C. § 552a(a)(7).

Permitting the government to disclose information, including Social Security identifying information, without satisfying the compatible

analysis presents a real threat to individual privacy—this is precisely what the Privacy Act was designed to prevent.

CONCLUSION

The government fails to offer a legally sufficient rationale to demonstrate how the disclosure of Social Security data is compatible with the purpose for which those records were initially collected by the Social Security Administration, namely, to administer social benefits programs. SSA's compatibility guidelines expressly limit sharing with other agencies that would use the information with respect to social benefit programs that they administer that are similar to those administered by SSA. The Court should deny the government's application for a stay.

Respectfully submitted,

BALLARD SPAHR LLP

M. NORMAN GOLDBERGER

(Counsel of Record)

MATTHEW A. STOLOFF

LAURA K. GRANT

1735 Market Street, 51st Floor,

Philadelphia, PA 19103-7599

215.864.8850

goldbergerm@ballardspahr.com