

**UNITED STATES DISTRICT COURT FOR
THE EASTERN DISTRICT OF NEW YORK**

MAKE THE ROAD STATES

301 Grove St
Brooklyn, NY 11237,

COMMON CAUSE

805 15th Street NW, Suite 800,
Washington, DC 20005,

and

**ELECTRONIC PRIVACY
INFORMATION CENTER,**

1519 New Hampshire Avenue, NW
Washington, DC 20036,

Plaintiffs,

v.

**U.S. DEPARTMENT OF HEALTH AND
HUMAN SERVICES,**

330 C Street SW,
Washington, D.C. 20201,

ROBERT F. KENNEDY JR., in his official
capacity as Secretary of U.S. Department of
Health and Human Services

330 C Street SW,
Washington, D.C. 20201,

**ADMINISTRATION FOR CHILDREN
AND FAMILIES,**

330 C Street SW,
Washington, D.C. 20201,

ALEX J. ADAMS, in his official capacity as
Assistant Secretary of the Administration for
Children and Families,

330 C Street SW,
Washington, D.C. 20201,

OFFICE OF FAMILY ASSISTANCE,

330 C Street SW
Washington, DC 20201,

Case No. ____-cv-_____

and

DAVID SWEGLE, in his official capacity as
Director, Office of Family Assistance,
330 C Street SW,
Washington, DC 20201,

Defendants.

COMPLAINT

INTRODUCTION

1. Temporary Assistance to Needy Families (“TANF”) is the federal government’s leading program for financial assistance to very low-income families with children. States administer the TANF program, and in doing so they are required to obtain, and periodically report to the Department of Health and Human Services’ (“HHS”) Administration for Children and Families (“ACF”), highly sensitive personal information about both recipients of TANF assistance and all others who live in their households—including their Social Security numbers, income, marital status, and immigration status.

2. Recognizing the sensitivity of that information, Congress safeguarded it from public dissemination and even sharing within the federal government through a series of protective provisions—in the TANF statute itself, in the Social Security Act, in 42 U.S.C. § 1306, in the Privacy Act of 1974 (the “Privacy Act”), and in the Computer Matching of Privacy Protection Act of 1988. And, in compliance with those statutes, Defendants have historically limited further disclosure of that information for very narrow uses.

3. TANF is a federal block grant program that helps fund state-run initiatives providing temporary cash assistance and non-cash benefits to low-income families with children and pregnant women, including child-care assistance, employment and training programs, services for children at risk of neglect or abuse, and after-school youth programs. TANF is one of the most significant forms of financial assistance for low-income American families and is a primary way that states assist families with children to achieve stability and become economically secure.

4. Congress placed calculated limits on the federal government’s authority to administer and oversee the program, instead granting states substantial flexibility and authority with the aim of reducing the bureaucracy and unwieldy federal oversight that had plagued TANF’s predecessor program.

5. States are required to share certain personal information TANF recipients provide about themselves and members of their households when enrolling in benefits with ACF, the office at HHS overseeing the TANF program, which then is authorized to use the information for narrow, statutorily prescribed purposes.

6. Congress took great pains to ensure that this sensitive personal information is protected by the state agencies administering the program and by the federal agencies funding it. States are required by federal statute to ensure that data collected from TANF recipients be made available “only to the extent necessary to assist in the valid administrative needs of the program receiving such information” and that such information “is adequately protected against unauthorized disclosure for other purposes.” 42 U.S.C. § 1320b-7(a)(5)(A), (B).

7. But Congress has never authorized Defendants to share this data about TANF recipients and members of their households, who may never have received benefits themselves, with any other federal or state agency or with private “entities” working with ACF. To the contrary, several federal statutes prohibit this sort of broad disclosure of data.

8. Defendants now seek to unlawfully bypass those protections in order to amass and share vast quantities of sensitive information about current and former TANF recipients and members of their households.

9. On August 11, 2026, Defendants can begin sharing vast quantities of this sensitive personal information with an undefined class of entities, including the U.S. Department of Homeland Security and other federal, state, or private “entit[ies] engaged by [Defendant Administration for Families and Children] (e.g., DHS or TANF program administrators) to assist [ACF] with” for vague and undefined “program integrity reviews or projects.” Privacy Act, System of Records, 91 Fed. Reg. 37409 (June 23, 2026) (hereinafter “TANF Notice”), available at <https://perma.cc/P4DV-3K9G>; see Exhibit A.

10. And since June 23, 2026, when the TANF Notice was published, Defendants have claimed an ability to substantially expand their statutorily limited role in overseeing the TANF program. They have also dramatically enlarged the scope of the information maintained in a system of records related to TANF recipients since June 23 to now include “verification information obtained from [TANF grantee] agencies, other HHS records, or other government agencies or entities,” which may include Social Security numbers, date of birth, county of residence, name, address, and detailed immigration status.

11. In so doing, Defendants have not identified a legally sound source of authority to take this unprecedented action with respect to TANF data. Nor have Defendants explained why this broad amassing and sharing of information is necessary when they have overseen the program for decades without it; nor have they given any indication that they had considered the interests of TANF recipients, who signed up for the program not knowing that their personal information—and their families’ personal information—would be widely disseminated as Defendants now intend. And Defendants ordered the new data sharing to take effect immediately at the *start* of the 30th day of a 30-day statutory comment period, not even pretending to allow themselves time to consider public comments submitted in response to such a dramatic development.

12. Defendants have no authority to amass and share this broad swath of data the way they assert, have failed to properly engage in the procedures set forth by the Privacy Act, and have failed to reasonably explain their actions or consider the interests of the millions of individuals whose information is subject to disclosure.

13. Make the Road States, Common Cause, and EPIC bring this lawsuit to stop Defendants’ amassing of vast amounts of personal information of millions of low-income children and families and the sharing of that information for unspecified and potentially boundless uses.

PARTIES

Plaintiffs

14. Plaintiff **Make the Road States** is a nonprofit, nonpartisan membership organization incorporated under the laws of the State of New York with offices and members in Pennsylvania, Nevada, Connecticut, New York, and New Jersey. Make the Road States is organized and operated as a membership organization and acts in this action on its own behalf. The organization's mission is to build the power of immigrant and working-class communities of color to achieve dignity and justice. Make the Road States is currently comprised of five organizations—Make the Road Connecticut, Make the Road Nevada, Make the Road New Jersey, Make the Road New York¹, and Make the Road Pennsylvania. Make the Road States's definition of a "member" is any individual who has signed on to a membership pledge, participated in its organizational activities and/or services and/or has paid membership dues. Currently, the organization has about 70,000 members, principally comprised of low-income people of color. Its membership includes immigrants and U.S. citizens of all ages. Its state-based organizations serve as community hubs for legal and supportive services. Make the Road States has members that reside in this district who are current or former TANF recipients (or their household members) and will be impacted by the TANF Notice.

15. Plaintiff **Common Cause** is a nonprofit nonpartisan membership organization incorporated under the laws of the District of Columbia with offices in 22 states and Washington, D.C. Common Cause has nearly 1 million members across the country, including in this judicial district. Its membership includes current and former recipients of TANF benefits, as well as family and household members of current and former TANF recipients, who will be impacted by

¹ In addition to being part of Make the Road States, Make the Road New York operates as its own non-profit organization.

the TANF Notice. Common Cause has a mission of creating an open, honest, and accountable government that serves the public interest; promoting equal rights, opportunity, and representation for all; and empowering people to make their voices heard in political and policymaking processes. Common Cause members comprise individuals who, within the past two years, made a financial contribution to the organization or have taken meaningful action in support of Common Cause's mission. As part of its work in promoting participation in democratic processes, Common Cause routinely files comments via Regulations.gov on federal rulemakings and SORNs. Common Cause also serves its membership through educating them about comment opportunities, coordinating comment campaigns, and inviting its individual members who want to file comments in their personal capacities. Moreover, it relies on public notices and records concerning the collection and use of personal information by federal agencies to understand and educate its members about their privacy interests in information collected about them. On July 31, 2026, Common Cause submitted a Comment Letter concerning the TANF SORN announced by Defendants. *See* Common Cause. Comment Letter on the Privacy Act System of Record Notice, 91 Fed. Reg. 37406 (June 23, 2026); John W. Young, III, *Common Cause's Opposition to the Privacy Act System of Records Notice*, Common Cause (July 1, 2026), <https://perma.cc/M7CN-X2D3> ("Common Cause Comment"). Moreover, Common Cause has invited its individual members to submit their own comments.

16. Plaintiff **Electronic Privacy Information Center** (EPIC) is a nonprofit organization, headquartered in Washington, D.C., established in 1994 to focus public attention on emerging privacy and civil liberties issues. Central to EPIC's mission is oversight and analysis of government activities that impact individual privacy, along with public education and engagement in order to help people better protect their privacy from government overreach. EPIC is a membership organization. An individual member of EPIC is any person who

contributes to the advancement of EPIC’s mission, who acts in accordance with the core values and policies of EPIC, and who has been recognized and registered as a member by EPIC, by virtue of payment of annual dues or having been granted a dues waiver. This includes members of EPIC’s Advisory Board, who are distinguished experts in law, technology, and public policy. EPIC regularly exercises its right as an “interested person” under the Privacy Act “to submit written data, views, or arguments” concerning systems of records detailed in SORNs, including new “routine use[s]” of such information. 5 U.S.C. § 522a(e)(11).

Defendants

17. Defendant **U.S. Department of Health and Human Services (“HHS”)** is a federal agency within the meaning of the Privacy Act, 5 U.S.C. § 552a(a)(1), and the Administrative Procedure Act (“APA”), 5 U.S.C. § 551(1), headquartered in Washington, D.C. The TANF Notice was issued by an agency under HHS.

18. Defendant **Robert F. Kennedy Jr.** is the Secretary of HHS and is sued in his official capacity.

19. Defendant **Administration for Children and Families (“ACF”)** is a federal agency within the meaning of the Privacy Act, 5 U.S.C. § 552a(a)(1), and the APA, 5 U.S.C. § 551(1), headquartered in Washington, D.C. It is a component of HHS. The TANF Notice was issued by an office within ACF.

20. Defendant **Alex J. Adams** is the Assistant Secretary of ACF and is sued in his official capacity.

21. Defendant **Office of Family Assistance** is an agency within the meaning of the Privacy Act, 5 U.S.C. § 552a(a)(1), and the APA, 5 U.S.C. § 551(1), headquartered in Washington, D.C. OFA issued the TANF Notice.

22. Defendant **David Swegle** is the Director, Office of Family Assistance and is sued in his official capacity.

JURISDICTION

23. This Court has subject matter jurisdiction under 28 U.S.C. § 1331 because the claims in this action arise under federal law, namely the Administrative Procedure Act (APA), 5 U.S.C. §§ 702, 706.

VENUE

24. Venue lies with the Eastern District of New York because the defendants are agencies or officers of the United States sued in their official capacities, at least one plaintiff resides in this district, and no real property is involved. 28 U.S.C. § 1391(e)(1). Plaintiff Make the Road States is incorporated in and has its principal place of business in this judicial district and each of the Plaintiffs are membership-based associations with members who reside in this district.

LEGAL BACKGROUND

The Temporary Assistance to Needy Families Program

25. The federal TANF block grant program provides federal financial assistance to states that wish to offer financial assistance programs for low-income families with children. 42 U.S.C. §§ 601–619 (Title IV-A of the Social Security Act) (the “TANF Statute”).

26. Congress created TANF in the Personal Responsibility and Work Opportunity Reconciliation Act of 1996 (“PRWORA”), Pub L. No. 104-193, 110 Stat. 2105 (codified at 42 U.S.C. §§ 601–619).

27. Through the TANF program, Congress intended for the federal and state governments to:

“(1) provide assistance to needy families so that children may be cared for in their own homes or in the homes of relatives; (2) end the dependence of needy parents on government benefits by promoting job preparation, work, and marriage; (3) prevent and reduce the incidence of out-of-wedlock pregnancies and establish

annual numerical goals for preventing and reducing the incidence of these pregnancies; and (4) encourage the formation and maintenance of two-parent families.” *Id.*

28. TANF currently funds over \$16 billion per year in grants to all 50 states, the District of Columbia, and several territories and tribal governments. It is a primary way that the federal and state governments fund efforts to alleviate poverty and is a primary source of cash assistance for low-income families. *See* Gene Falk, *Temporary Assistance to Needy Families (TANF) Block Grant: A Primer*, Cong. Rsch. Serv., R48413 (Dec. 18, 2025), <https://perma.cc/2VLK-RJZB> (CRS TANF Primer).

29. In addition to providing cash assistance, the TANF program helps fund a range of state-administered benefits and services for very low-income families with children, including childcare assistance, employment and training programs, services for children at risk of neglect or abuse, and after-school youth programs.

30. During an average month in fiscal year 2024, about 1.5 million children and about 569,600 adults received TANF cash assistance. Off. of Fam. Assistance, *Characteristics and Financial Circumstances of TANF Recipients, Fiscal Year 2024*, (Apr. 24, 2026), <https://perma.cc/Z4UX-8NF2>.

31. Among these, about 41% of cases involved child-only families in which no adult received TANF assistance. These “child-only” cases arise in a number of situations, for example if a child’s parent received disability benefits, if a child lives with a guardian other than a parent or stepparent, like a grandparent, or if only the child in the household has a qualifying immigration status to receive benefits. *Id.* In some of these cases, the non-recipients have income to help support the child, but in all child-only cases, only the child receives the benefit.

Congress gave states significant authority in administering the TANF program

32. Through PRWORA, Congress granted state governments a great deal of flexibility in the administration of the TANF program. *See* CRS TANF Primer, *supra* p. 8, ¶ 28.

33. Under the TANF Statute, states are permitted to spend TANF funds “in any manner that is reasonably calculated to accomplish the purpose of this part.” 42 U.S.C. § 604(a)(1).

34. The details of each state’s TANF operations and programming are contained in a plan submitted to the Secretary of HHS, which the states are required to submit regularly within a 27-month period. *Id.* § 602(a). Each state’s TANF plan includes a written overview of eligibility for the state’s assistance program and work requirements, as well as certifications regarding child support enforcement, foster care, and adoption assistance programs. *Id.* § 602(a).²

35. In addition to these requirements, a state must certify that it has protections in place “to ensure against program fraud and abuse.” *Id.* § 602(b)(6).

36. Under PRWORA, states are also required to certify that TANF benefits only go to “qualified” immigrants, and in certain cases, that they have been in that “qualified” status for five years. 8 U.S.C. §§ 1611(a), 1613(a), 1641. “Qualified” immigrants include lawful permanent residents, refugees, and other narrowly defined statuses of immigrants. 8 U.S.C. § 1641. U.S. citizen children of unqualified immigrant parents are eligible for TANF benefits. Ctr. on Budget & Pol’y Priorities, *Policy Basics: Temporary Assistance for Needy Families*, (Mar. 1, 2022), <https://perma.cc/R2QW-W5T6>.

² TANF encompasses a spending formula that requires states to match the allocated federal funds spent on benefits and services to needy families with their own funds. 42 U.S.C. § 609(a)(7). The state matching funds are generally known as “maintenance of effort” (“MOE”) funds. Some states provide separate state-funded assistance benefits (“SSP-MOE”) to individuals and families who are not eligible for TANF and count the funds spent on these benefits towards their MOE.

Congress Limited the Federal Government’s Role in Overseeing TANF Program

37. The federal government’s role in administering the TANF program, on the other hand, is “narrowly circumscribe[d]” by Congress’s intentional design. *Pa. Dep’t of Pub. Welfare v. Sebelius*, 674 F.3d 139, 147 (3d Cir. 2012). Congress designed TANF in this way to avoid some of the problems it perceived attendant in TANF’s predecessor statute, Aid to Families with Dependent Children (“AFDC”). AFDC, unlike TANF, authorized HHS to establish a “quality control system” under which it could review each state’s implementation of AFDC, determine its “error rate,” and assess a corresponding penalty. *See* Omnibus Budget Reconciliation Act of 1989, Pub. L. No. 101-239, § 8004, 103 Stat. 2454 (1989) (codified at 42 U.S.C. § 608).

38. In contrast, Congress sharply limited top-down federal control of the TANF program. Congress repealed the HHS’s authority to share recipient information to assist “any audit or similar activity ... in connection with the administration of [AFDC] by any other governmental entity . . .” 42 U.S.C. § 602(a)(9) (1994); 45 C.F.R. § 205.50(a)(1)(i)(E) (2025). And, in a section of the TANF Statute entitled “Limitation of Federal Authority,” Congress stated that “[n]o officer or employee of the Federal Government may regulate the conduct of States under this part or enforce any provision of this part, except to the extent expressly provided in this part.” 42 U.S.C. § 617. These exceptions are limited.

39. *First*, the TANF Statute allows ACF, the agency administering TANF within HHS, to confirm that State-submitted plans concerning their state TANF programs contain statutorily required information. *Id.* § 602(a).

40. *Second*, the TANF Statute authorizes ACF to penalize states for their failure to comply with certain specified statutory requirements, *id.* § 609, such as their failure to submit the statutory required reports, *id.* § 609, or their “[f]ailure to participate in” the income and eligibility verification system. *Id.* § 609(a)(7).

41. *Third*, PRWORA allows ACF to collect demographic information about TANF recipients in order to prepare reports regarding the effectiveness of the program. States collect household-level data about TANF recipients and their families on a monthly basis from state TANF programs and report “disaggregated case record information” to HHS each quarter. 42 U.S.C. § 611(a)(1)(A). Through regulation, HHS requires states to also share recipients’ Social Security numbers, immigration status, and dates of birth. *See* 45 C.F.R. § 265.3(b)(1) (2025); Admin. For Children & Families, *ACF-199 TANF and ACF-209 SSPMOE Data Reporting Instructions* (OMB Control No. 0970-0338, approved through Oct. 31, 2026), <https://perma.cc/C936-Y955> (“TANF Data Reporting Instructions”). HHS, through ACF, relies on this data to produce mandated “[a]nnual reports to Congress”³ describing the demographic characteristics of TANF recipients and assessing states’ success in meeting the program’s objectives. 42 U.S.C. § 611(b).

42. No provision of the TANF Statute (or any other statute) provide Defendants the authority to conduct “program integrity reviews” or generally “ensure and confirm grantee compliance with TANF program requirements” as the TANF Notice states. 91 Fed. Reg. at 37407. To the contrary, ACF is only permitted to penalize states either for failing to comply with a narrow set of statutorily delineated requirements, or if an independent auditor, pursuant to the Single Audit Act, finds that the TANF funds have “been used [by a state] in violation of this part.” 42 U.S.C. § 609(a)(1)(A); 31 U.S.C. §§ 7501–7506.

Collection of Data from TANF Recipients and Household Members

43. When individuals apply for TANF benefits, either for themselves or their children (or both), they must provide a substantial amount of highly sensitive personal information to state agencies that administer the TANF programs, sometimes referred to as TANF grantee agencies.

³ *See State TANF Data and Reports*, HHS (June 5, 2026), <https://perma.cc/WVW4-VWA9>.

While there is variation among states, grantee agencies collect, among other information, employment statuses, incomes, home addresses, marital status, Social Security numbers, and citizenship or immigration statuses for TANF recipients, as well as for members of their households.

44. Because PRWORA extends TANF eligibility to certain categories of noncitizens, *see supra* ¶ 36, states are statutorily required to verify a noncitizen applicant’s alien registration number through an automated or other system to confirm the noncitizen’s immigration status. 42 U.S.C. § 1320b-7(d).

45. Upon receipt of that documentation, states use “the individual’s alien file or alien admission number to verify with [U.S. Citizenship and Immigration Services] the individual’s immigration status” through the current immigrant eligibility verification system (“IEVS”), the Systematic Alien Verification for Entitlements (“SAVE”) program. *Id.* § 1320b(d)(3).

46. States are required to transmit copies of the individual’s documentation to USCIS for official verification, where they are unable to verify an applicant’s status on the SAVE database. *See id.* § 1320b-7(d)(4)(B)(i).

States are Required to Safeguard Information They Collect

47. Congress has required states to maintain eligibility verification systems that protect information they collect. *See* 42 U.S.C. § 1320b-7(a)(5)(A), (B). They must ensure that the information “is made available *only to the extent necessary* to assist in the valid administrative needs of the program receiving such information” and that such “information is adequately protected *against unauthorized disclosure for other purposes*, as provided in regulations established by the Secretary of [HHS].” *Id.* (emphases added).

48. And in the statutory provision requiring the states to submit plans to HHS pertaining to their TANF programs, each state must describe how it will “[t]ake such reasonable steps as the

State deems necessary to restrict the use and disclosure of information about individuals and families receiving assistance under the program attributable to funds provided by the Federal Government.” 42 U.S.C. § 602(a)(1)(A)(iv).

49. States are further required to “protect[] the individual’s privacy to the maximum degree possible.” *Id.* § 1320b-7(d)(3)(B). Through regulation, states have the “authority to implement and enforce the provisions for safeguarding information about applicants and recipients.” 45 C.F.R. § 205.50(a)(1)(ii) (2025).

HHS is Required to Keep Confidential TANF Data Collected from the States

50. HHS is required to keep TANF data it receives from state TANF agencies confidential.

51. Under 42 U.S.C. § 1306(a)(1), no disclosures shall be made of “any file, record, report, or . . . information, obtained at any time by . . . any officer or employee of [HHS] in the course of discharging the duties of the head of [HHS] under this chapter [42 U.S.C. ch. 7, §§ 301 to 1397mm, including the TANF subchapter] . . . except as the head of [HHS] may by regulations prescribe and except as otherwise provided by Federal law.”

52. And information provided pursuant to that statute is obtained by HHS officers and employees “in the course of discharging the duties” of the HHS Secretary. *See* 42 U.S.C. § 611(a)(1)(A) (“Each eligible state shall . . . report *to the Secretary* on a quarterly basis, the following disaggregated case information . . .”) (emphasis added). Thus, this information may be “disclos[ed]” only as the Secretary “may by regulations prescribe” and “as otherwise provided by Federal law.” 42 U.S.C. § 1306(a)(1).

53. In the absence of any regulation or statute authorizing the disclosure of information in Defendants’ possession, Defendants may not share the TANF data collected by the states. 42 U.S.C. § 1306(a)(1).

54. And pursuant to the Social Security Act, under 42 U.S.C. § 405(c)(2)(B)(viii)(I), “[s]ocial security account numbers and related records that are obtained or maintained by authorized persons pursuant to any provision of law enacted on or after October 1, 1990, shall be confidential, and no authorized person shall disclose any such social security account number or related record.” The TANF data collected by the states and maintained in the TANF System of Records are “obtained or maintained” pursuant to PRWORA, which was passed in 1996. Pub. L. No. 104-193, 110 Stat. 2105, 2110. HHS personnel with access to those records are “authorized persons” within the meaning of the statute. *See* 42 USC § 405(c)(2). And the TANF System of Records contains Social Security numbers and “related” records about TANF recipients and members of their households. *See* 42 U.S.C. § 405(c)(2)(B)(viii)(I).

Privacy Act

55. Congress enacted the Privacy Act of 1974 because of concerns about the centralization and amassing of personal information of American people in the wake of the Watergate and Counterintelligence Program scandals, both accepted today as threats to American democracy. Meghan M. Stussey, Cong. Rsch. Serv. R47863, *The Privacy Act of 1974: Overview and Issues for Congress* (Dec. 7, 2023), <https://perma.cc/R3QE-7TSX>. In developing the Privacy Act, Congress recognized that “good government and efficient management require that basic principles of privacy, confidentiality and due process must apply to all personal information programs and practices of the Federal Government.” S. Rep. No. 93-1183, at 6929 (1974). Congress’s objective was to “prevent [] de facto national data banks on individuals free of the restraints on Federal power established by Constitution and statutes” and the “creation of data banks and new personal information systems without statutory authorization from Congress and without proper regard for privacy of the individual, confidentiality of data, and security of the system.” S. Rep. No 93-1183.

56. The Act “regulate[s] the collection, maintenance, use, and dissemination of information by such agencies,” Pub. L. No. 93-579, § 2(a)(5), 88 Stat. 1896 (1974), and “prescribes how the government is to store agency records with individually identifying information, who may access information on individuals, and when the government may use or disclose it.” Stussey, *The Privacy Act of 1974*, at 1.

57. Under the Privacy Act, when federal agencies “collect, maintain, use, or disseminate any record of identifiable personal information,” they must do so “in a manner that assures that such action is for a necessary and lawful purpose.” Pub. L. No. 93-579, § 2(b)(4). The Privacy Act defines a “record” broadly as encompassing “any item, collection, or grouping of information about an individual that is maintained by an agency, including . . . his name, or the identifying number, symbol, or other identifying particular assigned to the individual.” 5 U.S.C. § 552a(a)(4). A disclosure is “any means of communication.” *Id.* § 552a(b).

58. Federal agencies are prohibited from disclosing records covered by the Privacy Act to any other person or agency unless “the individual to whom the record pertains” consents in writing or if one of thirteen statutory exceptions for disclosure without prior consent applies. *Id.*

59. One of these exceptions permits an agency to disclose information for a “routine use.” *Id.* § 552a(b)(3). “[T]he term ‘routine use’ means, with respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected.” *Id.* § 552a(a)(7). This exception prevents “personal data collected by one organization for a stated purpose” from being “used and traded by another organization for a completely unrelated purpose,” which could “seriously threaten[]” Americans’ “individual rights.” *Britt v. Naval Investigative Serv.*, 886 F.2d 544, 550 (3d Cir. 1989) (quoting 120 Cong. Rec. 36,894 (1974) (statement of Sen. Charles H. Percy)). Federal agencies are required “to the greatest extent practicable” to collect information directly from individuals. 5 U.S.C. §

552a(e)(2). When they collect individuals' data from a third party, however, it is the purpose for which the information was collected from the *individual*, not from the third party, that governs the purposes from which routine uses can be crafted. *See Covert v. Herrington*, 667 F. Supp. 730, 738–39 (E.D. Wash. 1987) *aff'd on other grounds sub nom. Covert v. Harrington*, 876 F.2d 751 (9th Cir. 1989).

60. When an agency plans to change a system of records or use it in a new way, including through a new routine use, it must adhere to certain safeguards. *See* 5 U.S.C. §§ 552a(a)(5), (e). The Act requires agencies to follow specific procedures before they “maintain, collect, use, or disseminate” any covered information. *Id.* §§ 552a(a)(3), (e)–(f). When an agency “establish[es] or revis[es]” a “system of records” containing retrievable information about individuals, it must “publish in the Federal Register ... a notice of the existence and character of the system of records.” *Id.* §§ 552a(e)(4), (a)(5) (defining “system of records”).

61. This notice, commonly referred to as a System of Records Notice (“SORN”), must identify, *inter alia*, the name and location of the system; the categories of individuals whose records are maintained in the system; the categories of records maintained in the system; the policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of records; and the procedures by which individuals can request notification of and access to information pertaining to them. *Id.* § 552a(e)(4).

62. The SORN must also identify “each routine use of the records contained in the system, including the categories of users and the purpose of such use.” *Id.* § 552a(e)(4)(D). And a “routine use” must be one that is “compatible with the purpose for which [the information] was collected.” *Id.* § 552a(a)(7).

63. The Act includes additional protections if an agency wants to create and rely upon a new routine use, including after the publication of the original notice. “[A]t least 30 days prior to

publication of information under” a routine use, the agency must “publish in the Federal Register notice of any new use or intended use of the information” and must provide an opportunity for interested parties to submit “written data, views, or arguments to the agency.” *Id.* § 552a(e)(11); *see also id.* § 552a(e)(4)(D).

64. If an agency fails to provide the requisite notice and opportunity for comment regarding a new routine use, it is “precluded from making necessary interagency transfers until it has complied with” those requirements. Privacy Act Implementation: Guidelines and Responsibilities, 40 Fed. Reg. 28948, 28966 (July 9, 1975); *see also* Off. of Mgmt. & Budget Circular, No. A-108, Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act 7 (2016), <https://perma.cc/N9QK-SDLE> (OMB Circular No. A-108) (“In no circumstance may an agency use a new or significantly modified routine use as the basis for a disclosure fewer than 30 days following *Federal Register* publication.”).

65. The Privacy Act is designed to ensure that the agency has sufficient time “to review those comments,” 40 Fed. Reg. at 28966, and “to determine whether any changes to the SORN are necessary” in light of them. OMB Circular No. A-108, at 7, 12 (“If an agency receives public comments on a published SORN, the agency shall review the comments to determine whether any changes to the SORN are necessary.”). And a court recently emphasized that the Privacy Act’s notice-and-comment procedures require both the “opportunity for meaningful input” *as well as* the “consideration of comments.” *League of Women Voters v. U.S. Dep’t of Homeland Sec.*, No. 25-3501 (SLS), 2026 WL 1784297, at *26 (D.D.C. June 22, 2026).

66. Prior to disseminating any information under a new routine use, an agency also must provide actual notice of the new use to any individual whose information may be disclosed. *Bechhoefer v. DOJ*, 179 F. Supp. 2d 93, 101 (W.D.N.Y. 2001) (an agency must “inform each individual whom it asks to supply information of the routine uses that may be made of the

information”); *U.S. Postal Serv. v. Nat’l Ass’n of Letter Carriers, AFL-CIO v. USPS*, 9 F.3d 138, 146 (D.C. Cir. 1993) (“the Privacy Act mandates that each [individual from whom information is collected] receive actual notice of the routine uses to which the private information provided by [the individual] is put . . . [and] an agency’s failure to provide [individuals] with actual notice of its routine use would prevent a disclosure from qualifying as a ‘routine use.’”). 5 U.S.C. § 552a(e)(3), (4), (11).

Computer Matching and Privacy Protection Act

67. With the increased use of computer systems, Congress became concerned that there were not adequate controls for, and oversight of, agencies’ computer-matching of individuals’ private data, and that individuals’ due process rights were not adequately protected from adverse actions stemming from inaccurate information. *See* Natalie R. Ortiz, Cong. Rsch. Serv., R47325, Computer Matching and Privacy Protection Act: Data Integration and Individual Rights, at 2 (Dec. 6, 2022) (“CRS Rep. on CMPPA”). In light of these concerns, Congress passed the Computer Matching and Privacy Protection Act of 1988 (“CMPPA”), Pub. L. No. 100-503, 102 Stat. 2507, which amends provisions of the Privacy Act and operates within the Privacy Act’s statutory framework. *See id.*

68. CMPPA creates additional protections whenever data held in different systems of records are “matched” for various purposes, including for “establishing or verifying the eligibility of . . . recipients,” or the “continuing compliance with statutory and regulatory requirements by . . . providers,” of federal benefit programs. 5 U.S.C. § 552a(a)(8) (defining “matching program”); *see also id.* § 552a(o) (establishing substantive and procedural safeguards for matching programs).

69. A matching program may involve two or more federal agencies or a federal agency and a state or local government agency. *See id.* §§ 552a(a)(8)(A)(i), 552a(a)(10) (defining “non-federal agency”)

70. The CMPPA states that “[n]o record ... may be disclosed” for purposes of a matching program unless and until the agencies involved execute a detailed “written agreement” specifying how the matching program will operate and how the data involved will be protected. *Id.* § 552a(o).

71. The statute requires an agency to publish a notice in the Federal Register at least 30 days before conducting a new or revised matching program. *See id.* § 552a(e)(12).⁴ The matching notice “is not effective until at least 30 days after its publication in the *Federal Register*.” OMB Circular No. A-108, at 19. And “[i]f an agency receives public comments on a published matching notice, the agency shall review the comments to determine whether any changes to the matching notice are necessary,” and if so, “shall publish a revised matching notice and provide an additional 30-day public comment and review period.” *Id.*

FACTUAL BACKGROUND

Ongoing Efforts to Consolidate Data and Bypass Procedural Requirements

72. Since taking office in January 2025, the Trump-Vance Administration has been persistently moving to consolidate the personal, sensitive data of American people from across local, state, and federal governments. *See* Emile Ayoub, *The Dangers of the Trump*

⁴ Which agency must publish the notice depends on whether federal or state agencies are involved in the matching program. A federal agency receiving data for purposes of a matching program must publish the notice if it is conducting the matching program with another federal agency, and a federal agency producing data for purposes of a matching program must publish the notice if conducting a matching program with a non-federal agency. *See id.* § 552a(e)(12); *see also* OMB Circular No. A-108, at 19, <https://perma.cc/N9QK-SDLE>.

Administration's Data Consolidation Efforts, Brennan Center (July 9, 2026),
<https://perma.cc/QE99-A5TJ>.

73. The President signed multiple executive orders in 2025 that advance this goal. First, on January 20, 2025, President Trump signed Executive Order 14158, *Establishing and Implementing the President's "Department of Government Efficiency,"* ("DOGE EO"), in which he directed the federal government to broadly share personal data across agencies so that DOGE would have "full and prompt access to all unclassified agency records." Exec. Order No. 14158, 90 Fed. Reg. 8441, 8442 (Jan. 20, 2025).

74. Then, on March 20, 2025, President Trump signed Executive Order 14243, *Stopping Waste, Fraud, and Abuse by Eliminating Information Silos* (the "Data Consolidation EO"). Exec. Order No. 14243, 90 Fed. Reg. 13681 (Mar. 20, 2025). The Data Consolidation EO calls for the removal of "unnecessary barriers to Federal employees accessing Government data and promot[ion of] inter-agency data sharing" as steps to curtail duplication and inefficiency. *Id.* The Executive Order directs heads of federal agencies to "ensure the Federal Government has unfettered access to comprehensive data from all State programs that receive Federal funding." *Id.* It further instructs agencies "to ensure Federal officials designated by the President or Agency Heads (or their designees) have full and prompt access to all unclassified agency records, data, software systems, and information technology systems" . . . including by "authorizing and facilitating both the intra- and inter-agency sharing and consolidation of unclassified agency records." *Id.*

75. In particular, the Trump-Vance Administration has focused on accessing state administrative data for public benefit programs partially funded by federal dollars for uses unrelated to the administration of those programs. *Federal Efforts to Expand Access to Data From State-Run Programs and Individual Privacy*, Protect Democracy (July 28, 2025),

<https://perma.cc/6THQ-KW79>. These efforts are part of a broader pattern of the federal government to “obtain more state data, allow access by more federal agencies, and use that information for immigration enforcement” as well as “potentially, to monitor protests and disenfranchise voters.” *See Ayoub, The Dangers of the Trump Administration’s Data Consolidation Efforts*.

76. Courts have repeatedly found such efforts to consolidate—and share—these types of data to be unlawful.

77. For example, in May 2025, the U.S. Department of Agriculture sought to obtain access to sensitive personal information collected by states of applicants to, or recipients, of Supplemental Nutrition Assistance Program (“SNAP”) benefits, including their names, dates of birth, personal addresses, and Social Security numbers. *See Jude Joffe-Block, At least 27 states turned over sensitive data about food stamp recipients to USDA*, NPR (Oct. 16, 2025), <https://perma.cc/69MM-9KZN>. A coalition of states filed suit challenging the planned disclosure of data, and the district court entered a temporary restraining order against the USDA, explaining that the USDA is “subject to strict restrictions placed on its use of the information so obtained” and enjoining the plaintiff states from “disclosing it where the recipient announces in advance an intent to use it for some other purpose.” *California v. USDA*, 800 F. Supp. 3d 1015, 1026 (N.D. Cal. 2025), *modified*, No. 25-cv-06310, 2025 WL 2772872 (N.D. Cal. Sept. 29, 2025).

78. Then, in July 2025, the Centers for Medicare & Medicaid Services (“CMS”), a component of Defendant HHS, turned over personal data of millions of enrollees in the Medicaid program to the Department of Homeland Security. This action is also being challenged in the courts. Amanda Seitz & Kimberly Kindy, *20 states sue after the Trump administration releases private Medicaid data to deportation officials*, Associated Press (July 1, 2025), <https://perma.cc/RCK3-XSGQ>. Here too, a district court granted a preliminary injunction that

prohibits CMS from turning over to DHS the personal data of millions of enrollees in the Medicaid program in part because the government did not give sufficient “indication that the agencies considered whether to limit the scope of the data to which ICE has access” and because the agency did not “consider[] the extent to which the states, providers, and patients relied on assurances that patient data would not be used for immigration enforcement purposes.”

California. v. HHS, No. 25-cv-05536-VC, 2025 WL 2356224, at *2 (N.D. Cal. Aug. 12, 2025).

79. And even though the court had temporarily paused the sharing of Medicaid data for immigration enforcement purposes in May 2026, the Centers for Medicare and Medicaid Services (“CMS”), a component of Defendant HHS, shared Medicaid data about millions of people with employees and contractors of the artificial intelligence firm Palantir. Jude Joffe-Block, *ICE shared Medicaid data it wasn't supposed to have with Palantir*, NPR (July 18, 2026), <https://perma.cc/2WXR-K9PP>; Pls’ Opp. to Defs’ Motion to Clarify/Modify Preliminary Injunction, 25-cv-05536, Dkt. No. 182 at 4.

80. The federal government has engaged in other efforts designed to circumvent the requirements of the Privacy Act. In March 2026, DHS attempted to disclose personal information found in various federal databases to state officials and the U.S. DOGE Service to “identify unqualified voters registered in States,” without ever first publishing a SORN notifying the public of the new “routine use” as required under the Privacy Act. *See League of United Latin Am. Citizens v. Exec. Off. of the President*, No. 25-cv-0946 (CKK), 2026 WL 880056 (D.D.C. Mar. 31, 2026), *aff’d sub nom.* No. 25-5476, 2026 WL 1991571 (D.C. Cir. July 2, 2026).

81. Also in March 2026, President Trump signed Executive Order 14395, which establishes a “Task Force to Eliminate Fraud.” The Executive Order directs the task force to “maximize enforcement of eligibility requirements,” “promote the facilitation of information and data sharing and coordination,” and “audit and ensure prospective compliance monitoring, including

for use in identifying fraud in Federal benefits programs.” *Establishing the Task Force To Eliminate Fraud*, Exec. Order. No. 14395, 91 Fed. Reg. 13485, 13487 (Mar. 19, 2026).

82. The Trump-Vance administration has since turned its attention to the TANF program.

Defendants Publish a Modified TANF SORN Announcing Plans to Amass and Widely Share Personal Information of TANF Recipients and Families

83. On June 23, 2026, the Defendant OFA published the TANF Notice.

84. The TANF Notice pertains to a system of records, herein the “TANF System of Records,” that “contains data about TANF clients received from TANF grantee agencies in the states, territories, and Tribal organizations, as well as verification information obtained from those agencies, other HHS records, or other government agencies or entities engaged to assist ACF with program integrity reviews or projects.” 91 Fed. Reg. at 37406.

85. The TANF Notice contains personal information about not just current and former TANF recipients, but also other members of their households. This information includes Social Security numbers, immigration status, marital status, parentage, employment information, and income, among other pieces of data. *See* TANF Data Reporting Instructions, *supra* ¶ 41. Although some states submit a statistical sample of such data, *see* 42 U.S.C. § 611(a)(1)(B)(i), other states submit this data for all TANF recipients in the State.⁵

86. The TANF Notice contains information for “[m]embers of families (as defined at 45 CFR § 265.2) who received assistance under the TANF program in any month” as well as “[m]embers of families no longer receiving assistance under the TANF program.” 91. Fed. Reg. at 37408. The TANF Notice broadly defines families to be “all individuals receiving assistance as part of a family under the grantee’s TANF or separate state program (including noncustodial

⁵ *See* ACF, Temporary Assistance for Needy Families 13th Report to Congress Fiscal Years 2016 through 2021 at 46 n.21, <https://perma.cc/928D-PZYJ> (identifying which states reported a sample of data collected in the relevant time period).

parents, where required under 45 CFR § 265.3(f)),” as well as “parent(s) or caretaker relative(s) of any minor child receiving assistance,” “minor siblings of any child receiving assistance,” and “any person whose income or resources would be counted in determining the family’s eligibility for or amount of assistance” who lives with the household. *Id.*

87. ACF uses information in the TANF System of Records for the following purposes, each of which is specifically authorized by statute: (1) to determine whether grantees are meeting specific and narrow requirements prescribed by PRWORA, such as the statute’s “work participation and time-limit requirements”; (2) to “compile information used in the report to Congress,” and (3) to “perform research on the caseload dynamics and employment trajectories of TANF recipients.” 89 Fed. Reg. at 25881; *see* 42 U.S.C. § 609(a)(9), (14)–(15); § 611(b); § 613(A).

88. The TANF Notice outlines several sweeping modifications to the System of Records Notice. 91 Fed. Reg. at 37406-10.

89. The TANF Notice adopts a **new purpose** for the system of records: “to ensure and confirm grantee compliance with TANF program requirements through HHS agency oversight activities including but not limited to program integrity reviews (*e.g.* comprehensive assessments of how grantees administer TANF programs and follow statutory requirements), additional audits (*e.g.* financial audits, programmatic audits, and fraud investigations), and monitoring (*e.g.* regular review of data reports, on-site or virtual visits to TANF agencies, periodic review of policies and procedures).” *Id.* The TANF Notice goes on to state that the system of records shall be used to “ensure compliance with all TANF program requirements including but not limited to the work participation rate and time-limits, the requirement to provide complete and accurate data, and the requirement to verify TANF recipients’ citizenship or immigration status in records

maintained by [DHS].” *Id.* (citing 45 U.S.C. § 265.7(b); 42 U.S.C. § 1320b-7(d); 6 U.S.C. § 552 (d)).

90. The TANF Notice expands the **scope and sources** of data in the system of records to include “verification information” obtained from grantee agencies, “other HHS records,” and “other government agencies or entities (e.g.,] DHS or the Social Security Administration (SSA)) engaged to assist ACF with program integrity reviews or projects.” 91 Fed. Reg. at 37407.

91. But by describing the scope and sources in such broad and vague terms, Defendants fail to provide any notice of what they are actually collecting. For example, “other HHS records,” *id.*, could mean records from literally *any* part of HHS, from medical records submitted for Medicare claims to HHS’s own employee personnel files. And records from “other government agencies or entities . . . engaged to assist ACF with program integrity reviews or projects” is even more vague. The TANF Notice provides the public and the individuals whose information HHS is amassing no information whatsoever about what type of information HHS is amassing into the TANF System of Records or where this data is coming from.

92. The TANF Notice includes a new **category of records** to be contained in the system: verification information that “may include SSN, date of birth, county of residence, name, address, and detailed immigration status information (e.g., whether an individual is a refugee, non-immigrant, has no status, has temporary protected status, requires additional verification).” *Id.* at 37408.

93. Here too the TANF Notice provides no clear demarcation of what information Defendants are collecting. Although they provide examples, they do not identify the full range of data collected.

94. Finally, the TANF Notice includes a new additional **routine use**, “Routine Use 10.” The TANF Notice authorizes Defendants to share records from this system of records “to another

federal or grantee agency or entity engaged by ACF (*e.g.*, DHS or TANF program administrators), to assist ACF with program integrity reviews or projects, to verify whether TANF grantee agencies are complying with TANF program requirements, including verifying citizenship or immigration status.” *Id.* at 37409.

95. The TANF Notice does not cite a valid legal basis for HHS’s planned expansion of the TANF System of Records, nor for Routine Use 10. As sources of authority for the SORN, Defendants list the TANF Statute at 42 U.S.C. §§ 601–619; 42 U.S.C. § 1320b-7; and 8 U.S.C. § 1373. None authorize the breadth of the collection or dissemination of data in the TANF Notice. 42 U.S.C. §§ 601–619 permit only the limited collection of information that predated the TANF Notice. 42 U.S.C. § 1320b-7 requires each “*State*”—not the federal government—to establish a system for checking recipients’ eligibility. And 8 U.S.C. § 1373 is not an affirmative grant of authority, but instead a *prohibition*, stating that federal, state, and local agencies “may not” restrict the sharing of information solely “regarding the citizenship or immigration status, lawful or unlawful, of any individual.” 8 U.S.C. § 1373(a). The sources of authority Defendants cite in the TANF SORN do not permit them to amass or share a vast amount of sensitive personal information about millions of TANF recipients and non-recipient family members across the government and to any agency ACF engages to “assist ... with program integrity reviews.” 91 Fed. Reg. at 37407-09.

Defendants’ TANF Notice and Routine Use 10 Were Issued without Observance of Procedure Required by Law

96. The TANF Notice and Routine Use 10 were issued without observance of procedure required by the Privacy Act, 5 U.S.C. § 552a.

97. The Privacy Act requires agencies publish notice of any new routine use in the Federal Register “and provide an opportunity for interested persons to submit written data, views, or arguments to the agency.” 5 U.S.C. § 552a(e)(11).

98. Inherent in the requirement to solicit comments from the public is the requirement to actually consider those comments.

99. Nevertheless, Defendants made the TANF Notice effective immediately upon publication and made Routine Use 10 effective at the start of the day on August 11, 2026, even though the comment period does not close until midnight that same day. 91 Fed. Reg. at 37406; 91 Fed. Reg. at 45278.

100. Because Routine Use 10 becomes effective before *all* comments can be submitted, Defendants necessarily cannot consider all comments submitted.

101. Additionally, the TANF Notice itself (including Routine Use 10) is so devoid of detail as to preclude any meaningful opportunity to comment. The Notice identifies new sources of information amassed about individuals so broadly—to now include information from *any* “other HHS record” or record from *any* “other federal or state agencies engaged to assist ACF with program integrity reviews or projects”—as to preclude any meaningful notice of what information the records will now contain and where that data may originate. 91 Fed. Reg. at 37407–08. Similarly, Routine Use 10 now “authorize[s] disclosure” to *any* other “federal or grantee agency or entity engaged by ACF . . . to assist ACF with program integrity reviews or projects, to verify whether TANF grantee agencies are complying with TANF program requirements, including verifying citizenship or immigration status.” *Id.* Thus, the Notice now discloses that it can obtain virtually any information from anywhere about an individual and disclose it to virtually anyone.

102. Such broad categories of sources and recipients of information are too vague to allow a meaningful opportunity to comment on the TANF Notice and Routine Use 10.

Defendants' TANF Notice and Routine Use 10 are Contrary to Law

103. The TANF Notice and Routine Use 10 are contrary to law and exceed Defendants' statutory authority in myriad ways.

104. *First*, Defendants lack authority to amass and share this information in this fashion. 42 U.S.C. § 1306 likewise prohibits the sharing of this information. Although Defendants reference the TANF Statute (42 U.S.C. §§ 601–619), 42 U.S.C. § 1320b-7, and 8 U.S.C. § 1373, as their source of statutory authority to enlarge and share the TANF system of records pursuant to Routine Use 10, none of these statutes authorize the extensive dissemination of personal information that can be disclosed under this new “routine use.”

105. *Second*, Routine Use 10 is so vague and broad that it fails to adequately apprise interested and affected individuals as to what it encompasses. It lacks any clear indication as to which agencies and what entities exactly may receive the highly sensitive personal information amassed into the now-expanded TANF System of Records. It does not in any way define or explain what may constitute “program integrity reviews” or “projects,” opening up the possibilities for what this data can be used for. Under this purportedly routine use, Defendants could share information from this system of records with any “federal or grantee agency or entity engaged by ACF (e.g., DHS or TANF program administrators) to assist ACF with program integrity reviews or projects” 91 Fed. Reg. at 37407. Because of the extraordinary breadth of potential recipients, it is not possible to know from the TANF Notice with whom this information will be shared. It therefore runs afoul of the Privacy Act's publication requirements.

106. *Third*, Routine Use 10 is not “compatible with the purposes for which [information] was collected.” 5 U.S.C. § 552a(a)(7). Routine Use 10 authorizes disclosure “to another federal or grantee agency or entity engaged by ACF (e.g., DHS or TANF program administrators) to assist ACF with program integrity reviews or projects” and “to verify whether TANF grantee

agencies are complying with TANF program requirements, including verifying citizenship or immigration status.” 91 Fed. Reg. at 37407. But TANF recipients and their family members provided sensitive personal information to enroll in benefits—a purpose that is untethered to the expansive purpose now articulated in Routine Use 10. And the breadth of the disclosures that Defendants propose to make—which include, for example, sharing the immigration status of household members who have not themselves ever received TANF benefits—is incompatible even with the new “program integrity” purpose articulated in the TANF Notice.

107. *Fourth*, on information and belief, Defendants have not provided the individuals whose information is in the TANF System of Records with actual notice of this new routine use. It was not disclosed on the forms they completed to obtain benefits and Defendants do not appear to have done anything to apprise them of this retroactive use of their data in contravention of 5 U.S.C. § 552a(e)(3).

108. *Fifth*, while the TANF Notice indicates HHS’s intention to share the personal information of millions of TANF recipients and household members with the U.S. Department of Homeland Security, HHS has provided no indication that it has entered into such a computer matching agreement or any other written agreement, as required under the CMPPA.

109. *Sixth*, Defendants have not complied with the applicable notice-and-comment requirements of the Privacy Act. Defendants originally published the TANF Notice in the Federal Register on June 23, 2026; it instructed that comments “may be submitted to the Federal eRulemaking Portal electronically at <http://www.regulations.gov>” until July 23. This portal was created by the federal government as a requirement of Section 206 of the eGovernment Act, and it is now the standard (and, for rulemaking subject to 5 U.S.C. § 553, statutorily required) vehicle for public comments in response to any federal agency notice. ACF did not post the TANF SORN on www.regulations.gov and did not make the TANF SORN available for

comments on that website until being notified of its error by Plaintiff EPIC. Defendants opened the notice for comment on www.regulations.gov on July 20, 2026, and extended the deadline for both comments and for the effective date of the new routine use would be August 11, 2026.

Privacy Act, System of Records, 91 Fed. Reg. 45278 (July 20, 2026).

110. Nevertheless, Defendants have set Routine Use 10 to take effect before the close of the comment period and before Defendants could possibly review the comments submitted, much less consider them.

111. And as noted above, the TANF Notice and Routine Use 10 are so vague as to not provide meaningful opportunities for interested or impacted parties to comment.

Defendants' TANF Notice and Routine 10 are Also Arbitrary and Capricious

112. The TANF Notice and Routine Use 10 are arbitrary and capricious for numerous reasons.

113. *First*, by setting Routine Use 10 to take effect before the close of the comment period, Defendants have evinced their intention not to consider the full scope of “written data, views, or arguments” submitted by Plaintiffs or other members of the public and refusal to consider the critical the aspects of the problem identified in those comments. 5 U.S.C. § 552a(e)(11).

114. *Second*, Defendants have not articulated a reasonable, or even a rational, explanation for their change of policy to enlarge the existing system of records with a vast amount of information pertaining to current and former TANF recipients—and for people who may never have received TANF—and to then share this data so widely.

115. *Third*, by making the TANF Notice effective immediately upon publication, except for Routine Use 10, Defendants have arbitrarily refused to consider important aspects of the new policy, specifically those raised in comments by the public.

116. *Fourth*, Defendants have not considered numerous aspects of the problem. For example, they have failed to consider the relevant reliance interests, including of the children or families receiving TANF, or particularly vulnerable people with heightened privacy interests, like survivors of domestic abuse, to whom Congress has given particular attention in the TANF Statute. 42 U.S.C. §§ 602(a)(7)–(8). Nor have Defendants considered the chilling effect that this policy will have on TANF eligible households who will be deterred from applying for benefits and concomitant impacts on needy children and their families.

117. *Fourth*, Defendants did not consider any less personally intrusive or risky alternatives to achieve their stated purpose in the TANF Notice and Routine Use 10, namely for “program integrity reviews” or to “ensure and confirm grantee compliance with all TANF program requirements.” 91 Fed. Reg. at 37407.

118. *Finally*, Defendants’ stated goals—to verify program compliance—is pretext for Defendants’ aim to support their unrelated immigration agenda.

Injuries to Plaintiffs

119. Plaintiffs Common Cause and Make the Road and their members will suffer immediate and irreparable injuries caused by Defendants’ actions to collect and share their members’ personal data, as indicated through the TANF Notice and Routine Use 10, unless those actions are enjoined. *See generally* Common Cause Comment, *supra* ¶ 15.

120. As a consequence of the TANF Notice and Routine Use 10, Defendants are poised to disclose the personal and sensitive data in the TANF System of Records, which Defendants indicated they are enlarging to include a vast amount of additional sensitive information pursuant to the TANF Notice since June 23. This disclosure could begin as soon as Routine Use 10 goes into effect in just eight days—on August 11.

121. If it is not enjoined, Routine Use 10 will enable Defendants to disclose all the information in the enlarged TANF system of records broadly to *any other federal or state agency* or undefined *entity* engaged by ACF to assist it with vaguely defined and seemingly boundless “program integrity reviews” or “projects.” 91 Fed. Reg. at 37407.

122. Once that information is disseminated, it may be dramatically harder or impossible to claw back the sensitive information of millions of current and former TANF recipients and members of their households.

Injuries Resulting from Enlarging of Records in System of Records

123. Members of Plaintiffs Common Cause and Make the Road States will first suffer from Defendants’ vast expansion of the sources and types of information amassed about them into a single database—the exact harm the Privacy Act sought to prevent by requiring careful siloing of information.

124. By amassing TANF recipients’ and their household members’ personal data from any number of federal, state, and private data sources—with no disclosure as to what those data sources are or what information may be pulled from them—Defendants greatly increase the risk that false or erroneous information about TANF recipients will be perpetually replicated and become impossible to correct. This is particularly the case because the information collected includes information regarding *former* recipients and their household members, which are more likely to be out of date. *See* Common Cause Comment, *supra* ¶ 15 (“The proposed routine use number 10 does not” describe “how the data will be protected against misuse, and how any errors relating to the reliance on outdated data will be avoided and corrected”).

125. Moreover, by failing to disclose *what* data Defendants are collecting from *what* sources—beyond the opaque description of information from “other HHS records” and “other federal or state agencies or entities engaged to assist ACF with program integrity reviews or

projects”—Defendants ensure TANF recipients and their households would not even know what *possible* information could be in those records that might need to be corrected. 91 Fed. Reg. at 37407. Indeed, “other HHS records” could include anything from sensitive medical records collected from HHS subagencies Indian Health Services or Center for Medicaid and Medicare Services to information regarding individuals’ disabilities from HHS subagency Administration for Community Living – or to any number of other types of data amassed by “other HHS” agencies.

126. Additionally, Defendants have not identified any additional security measures to protect this new super-database of all TANF recipients’ and their household members’ most personal information, making Plaintiffs’ members more vulnerable to more dangerous breaches of security. *See* Common Cause Comment, *supra* ¶ 15 (the TANF Notice contains “no description of the security protocols that would be used to safeguard that data”). This newly expanded system of records will house not only Social Security numbers, addresses, phone numbers, family relationships (*i.e.*, mothers’ maiden names), and incomes, but also potentially any documentation “verifying” that information like birth certificates, passports, and bank statements—in short, anything a would-be hacker would need to usurp the identity of this highly vulnerable population for any number of nefarious purposes.

127. Moreover, because the data collection portion of the TANF Notice became effective immediately upon publication of the TANF Notice on June 23, 2026, these harms may already be occurring. And the more time Defendants have to collect more data from more sources related to TANF recipients and their household members, the more difficult it will be to disentangle data sources, and the more TANF recipients and their household members are harmed.

Injuries Resulting from Routine Use 10

128. Members of Plaintiffs Common Cause and Make the Road States will also be irreparably injured by Defendants' imminent sharing of their highly personal information, set to begin on August 11, unless that sharing is enjoined. *See generally* Common Cause Notice.

129. As noted *supra* ¶¶ 83–95, Defendants have greatly expanded the types and sources of highly sensitive information that can be housed in the TANF system of records. And, beginning August 11, Defendants will have a virtually unfettered ability to share Plaintiffs' members' personal information with *any* federal or state agency or other “entity” with which ACF “engages.”

130. Such a deprivation of individuals' statutory right of privacy is analogous to the common-law torts of intrusion upon seclusion and breach of confidence. *See Am. Fed'n of Gov't Emps., AFL-CIO v. U.S. Off. of Pers. Mgmt.*, 786 F. Supp. 3d 647, 694 (S.D.N.Y. 2025) (“an improper disclosure within the Government is a serious and cognizable harm.”).

131. This deprivation of Plaintiffs' members' statutory right of privacy will cause them substantial distress and fear. It will also deter these vulnerable families from seeking essential support, jeopardizing the well-being of children who rely on this aid for food and clothing. See Common Cause Notice (the proposed changes “will also discourage them from even attempting to access the health and support services they need in the first place” and “threatens to leave these vulnerable families without healthy food, safe housing, and other necessities”).

132. The potential harms from the sharing of this information are expansive given that Defendants have imposed no limitations on what the undisclosed recipients may do with TANF recipients and their household members' sensitive data.

133. At the outset, each of Plaintiffs' harms are multiplied with each additional agency or entity Defendants share TANF recipients and their household members' sensitive data. Because

Defendants have not identified which agencies might receive the data, they have compounded the likelihood that individuals will never be able to correct any errors throughout all agencies and entities housing their data. And because the information to be shared is retroactive, and includes former recipients and their families, the likelihood of out-of-date or inaccurate information is enhanced.

134. The potential ramifications of these errors become even more grave with the sharing of this information to entities like DHS, which the TANF Notice specifically references. Sharing data with DHS of not just current and former TANF recipients (who must be U.S. citizens, permanent residents, or in a qualifying status pursuant to 8 U.S.C. § 1641), but *also* their household members (who may be in any immigration status) that was *not* collected for immigration enforcement purposes and may be erroneous, out of date, or misconstrued, dramatically increases the risk these individuals will be erroneously targeted for DHS action.

135. Additionally, by expanding the agencies and “entities” that can receive these individuals’ highly sensitive information, with no attendant requirements regarding how those recipients must store and protect that information, Defendants greatly increase the likelihood of data breaches and identity theft. Every time another agency or entity receives this information, another opportunity for inadvertent data disclosure or data breach arises.

136. The risks of data breach are particularly acute for TANF recipients and their household members who are victims of domestic violence or stalking. Congress was so concerned about this particularly vulnerable set of people that it placed extra safeguards on how the state agencies administering TANF must protect this information. 42 U.S.C. § 602(a)(7)(A)(i) (giving states the option to certify that they “screen and identify individuals receiving assistance under this part with a history of domestic violence while maintaining the confidentiality of such individuals”).

The TANF Notice gives no indication that Defendants or any entity they share the data with will abide by these same protective limitations.

Injuries from the Lack of Disclosure in the TANF Notice

137. All three Plaintiffs are injured by the dearth of information disclosed in the TANF Notice in violation of the Privacy Act. *See generally* Common Cause Comment, *supra* ¶ 15.

138. The Privacy Act entitles Plaintiffs to know what information federal agencies are collecting about individuals, what sources are supplying that information, how that information will be used, and to whom it will be shared.

139. The TANF Notice is a model of opacity, defining types of information, sources of information, potential recipients of information, and potential uses of information in the broadest and vaguest terms possible.

140. The lack of clarity as to even the most basic information regarding the expansion of Defendants' data collection and sharing harms Plaintiffs' ability to carry out their missions of educating their members and the public about how the government is collecting and using information.

141. Plaintiff EPIC's mission is to educate its members and the public about privacy concerns in the digital age. For decades, EPIC has made extensive use of public notices and records concerning the collection, use, retention, and transfer of personal information by federal agencies to educate its members and the public about the government's uses of their information, to inform policy debates, and to submit their own comments and organize other organizations and individuals to submit comments on notices, including SORNs mandated by the Privacy Act.

142. Plaintiffs Make the Road States' and Common Cause's missions are focused on educating their members and the public about infringements on their civil rights, including privacy rights.

143. Common Cause has relied on its knowledge of longstanding government practices and information disclosed under open government laws to educate and inform the public so that they can make their voices heard in the political process and to push for a more open, honest, and accountable government that serves the public interest.

144. By depriving Plaintiffs of sufficient information to know what data is being collected from whom, shared with whom, and why, Defendants have directly impeded Plaintiffs' abilities to carry out these critical missions.

CLAIMS FOR RELIEF

COUNT I

Violation of the Administrative Procedure Act/Privacy Act: Failure to Observe Procedure Required by Law

145. Plaintiffs restate and reallege paragraphs ¶¶ 1–144 as if fully set forth here.

146. The TANF Notice is a final agency action subject to the APA, 5 U.S.C. § 706.

147. Under the APA, agency action must be held “unlawful and set aside” if found to be “without observance of procedure required by law.” 5 U.S.C. § 706(2)(D).

148. The Privacy Act requires that “at least 30 days prior to publication of information under [a new routine use]” an agency must “publish in the Federal Register notice of any new use or intended use of the information in the system, and provide an opportunity for interested persons to submit written data, views, or arguments to the agency.” 5 U.S.C. § 552a(e)(11).

149. Inherent in the requirement to solicit comments is the requirement to actually consider those comments.

150. On June 23, 2026, Defendants published the TANF Notice in the Federal Register, disclosing and soliciting comments on new Routine Use 10. 91 Fed. Reg. at 37406.

151. Routine Use 10 lacks sufficient detail to afford the public a meaningful opportunity to comment. Specifically, Routine Use 10 does not disclose all agencies and entities to whom information may be disseminated or for what purpose information may be disseminated.

152. Additionally, Routine Use 10 will become effective at the start of August 11, 2026, before the comment period closes at midnight that same day. 91 Fed. Reg. at 45278.

153. By failing to disclose sufficient detail regarding Routine Use 10 to allow interested persons to comment and by refusing to fully consider comments on Routine Use 10 before the effective date, Defendants have promulgated Routine Use 10 “without observance of procedure required by law.” 5 U.S.C. § 706(2)(D).

154. Routine Use 10 thus must be held “unlawful and set aside.” *Id.* § 706(2).

COUNT II

Violation of the Administrative Procedure Act: Action Not in Accordance with Law or in Excess of Statutory Authority

155. Plaintiffs restate and reallege paragraphs ¶¶ 1–144 as if fully set forth here.

156. The TANF Notice is a final agency action subject to the APA, 5 U.S.C. § 706.

157. Under the APA, agency action must be held “unlawful and set aside” if it is “not in accordance with law[,] . . . in excess of statutory . . . authority, or limitations, or short of statutory right.” 5 U.S.C. § 706(2)(A), (C).

158. Defendants’ actions are contrary to law and exceed their statutory authority and are short of statutory right in several independent ways.

159. *First*, Defendants lack statutory authority to amass and share data in the manner set forth in the TANF Notice. Under 42 U.S.C. § 1306(a)(1), (2)(B), HHS is barred from disclosing “any [] file, record, report, or other paper, or any information[] obtained” under Chapter 7 of the U.S. Code (which includes the codification of the TANF Statute) “except as . . . regulations prescribe and except as otherwise provided by Federal law.” The TANF information that

Defendants collect from the states thus may not be disclosed, as there is no statute or regulation authorizing the broad disclosure of TANF records pursuant to Routine Use 10.

160. *Second*, the Social Security Act forbids Defendants from sharing Social Security numbers and related records (which encompass the data amassed here). 42 U.S.C. § 405(c)(2)(B)(viii)(I).

161. *Third*, the Privacy Act requires agencies to publish notice of a system of records in the Federal Register that includes “the categories of records maintained in the system” and “the categories of sources of records in the system.” 5 U.S.C. § 552a(e)(4)(C), (I). By broadening the sources of information included in the system of records to now include *any* “other HHS record” and records from *any* “other federal or state agencies,” 91 Fed. Reg. at 37407–08, Defendants have removed any cognizable limitation on what may be in the system of records, precluding any meaningful notice of *what* information about individuals from *what* sources can now be contained in the system. In so doing, Defendants have deprived Plaintiffs of information to which they are entitled by law.

162. *Fourth*, the Privacy Act requires that (a) notice of a new routine use be published with sufficient information to adequately inform interested parties of the recipients and uses of the data, 5 U.S.C. § 552a(e)(11); (b) that any routine use be compatible with the purpose for which information was collected, *id.* § 552a(a)(7), and (c) actual notice of the new routine use to individuals whose information is in the TANF system of records; *id.* § 552a(e)(3)(C). The TANF Notice and its Routine Use 10 fail on each of these grounds.

163. *Fifth*, Defendants have failed to comply with the notice and publication requirements of the CMPPA. 5 U.S.C. § 552a(a)(8), (e)(12), (o)(1). The CMPPA applies because “data reported to ACF by TANF grantee agencies” will be, on information and belief, matched against “verification information obtained from those agencies, other HHS records, or other government

agencies or entities (*e.g.* DHS or the Social Security Administration (SSA)).” 91 Fed. Reg. at 37408.

164. Routine Use 10 thus is “not in accordance with” the 42 U.S.C. § 1306, the Social Security Act, the Privacy Act, and/or the CMPPA and is “in excess of statutory . . . authority, or limitations, or short of statutory right. 5 U.S.C. § 706(2)(A), (C).

165. The TANF Notice and Routine Use 10 thus should be held “unlawful and set aside.” *Id.* § 706(2).

COUNT III
Violation of Administrative Procedure Act:
Arbitrary and Capricious Action

166. Plaintiffs restate and reallege paragraphs ¶¶ 1–144 as if fully set forth here.

167. Under the APA, the agency action must be held “unlawful and set aside” if it is “arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law.” 5 U.S.C. § 706(2)(A).

168. The TANF Notice is a final agency action subject to the APA, 5 U.S.C. § 706.

169. The TANF Notice and Routine Use 10 are arbitrary and capricious for several reasons. *Id.* § 552a(e)(11).

170. For one, the effective date of Routine Use 10 – before the close of the comment period – reflects a refusal to consider the full scope of “written data, views, or arguments” that the agency is required to review, 5 U.S.C. § 552a(e)(11), and prejudgment that is impermissible under the APA.

171. Additionally, by making the TANF Notice, aside from Routine Use 10 effective immediately upon publication with no solicitation, much less consideration of public feedback and comments, Defendants have arbitrarily refused to consider critical aspects of the Notice,

including reasonable concerns about the legality and propriety of the expanded scope of categories of information amassed about individuals.

172. Nor have Defendants offered a reasonable explanation for their change in policy, much less a rational one. For example, Defendants have failed to identify why, given the copious amount of data grantees already give HHS, Defendants lack the information they need or why a vast data set of former TANF recipients will enable Defendants to meet their lawful goals. Nor do Defendants identify a history of grantee compliance issues to justify their boundless dissemination of that information.

173. Defendants have failed to take into account the serious reliance interests of current and former TANF recipients and members of their households, including individuals with heightened and statutorily highlighted privacy interests, like survivors of domestic abuse. 42 U.S.C. § 602(a)(8).

174. Nor did Defendants consider obvious alternatives, like limiting the scope of data to be amassed or shared, identifying with specificity the agencies or entities with whom they plan to share and the reasons for that sharing, or limiting the sharing of information to future (rather than current and former) recipients and their households.

175. Indeed, stated reasons given for the TANF Notice and Routine Use—for “program integrity reviews” or to “ensure and confirm grantee compliance with all TANF program requirements” —are a pretext for Defendants’ real aim, namely, to support unrelated immigration policies. 91 Fed. Reg. at 37407.

176. The TANF Notice and Routine Use 10 thus must be held “unlawful and set aside.” 5 U.S.C. § 706(2).

PRAYER FOR RELIEF

Plaintiffs respectfully request that this Court:

- a. Declare that the TANF Notice and Routine Use 10 are in excess of statutory authority, contrary to law, short of statutory right, arbitrary and capricious, and without observance of procedure required by law in violation of the Administrative Procedure Act.
- b. Stay the TANF Notice and Routine Use 10 pursuant to 5 U.S.C. § 705.
- c. Hold unlawful, vacate, and set aside the TANF Notice and Routine Use 10 pursuant to 5 U.S.C. § 706.
- d. Enter a preliminary and permanent injunction enjoining Defendants from sharing information pursuant to Routine Use 10 and implementing the TANF Notice.
- e. Enter a preliminary and permanent injunction enjoining Defendants from collecting data into the TANF system of records from “other HHS records, or other government agencies or entities,” as described in the TANF Notice. 91 Fed. Reg. at 37407.
- f. Award Plaintiffs their costs, reasonable attorneys’ fees, and other disbursements deemed appropriate; and
- g. Grant such other relief as the Court deems necessary, just, and proper.

Date: August 3, 2026

Respectfully submitted,

Saima A. Akhtar (NY Bar No. 4661237)
NATIONAL CENTER FOR LAW AND
ECONOMIC JUSTICE
50 Broadway, Suite 1500
New York, NY 10004
(212) 633-6967 (telephone)
(212) 633-6371 (fax)
Email: akhtar@nclej.org

/s/ Rachel L. Fried Nguemaha
Rachel L. Fried Nguemaha (NY Bar. 5314208)
Shiva Kooragayala (Ill. Bar No. 6336195) +*
Kimere Kimball (CA. Bar No. 260660)+*
Emily Newton (VA Bar No. 80745)*+
Paul R.Q. Wolfson (D.C. Bar No. 414759) +
Elena Goldstein (D.C. Bar No. 90034087) +
Democracy Forward Foundation
P.O. Box 34553
Washington, DC 20043
Phone: (202) 448-9090
Fax: (202) 796-4426
rnguemaha@democracyforward.org

skooragayala@democracyforward.org
kkimball@democracyforward.org
enewton@c.democracyforward.org
pwolfson@democracyforward.org
egoldstein@democracyforward.org
Counsel for Plaintiffs

** Not admitted to practice law in the District of Columbia; practicing under the supervision of Democracy Forward lawyers who are members of the DC Bar.*

+ Motion to appear pro hac vice pending

- Of Counsel, only admitted in Virginia