

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

LEAGUE OF WOMEN VOTERS *et al.*,

Plaintiffs,

v.

U.S. DEPARTMENT OF HOMELAND
SECURITY, *et. al.*,

Defendants.

Civil Case No. 25-cv-3501-SLS

DECLARATION OF ALAN BUTLER

I, Alan Butler, declare under penalty of perjury, under 28 U.S.C. § 1746, that the following is true and correct:

1. I am over eighteen years old, of sound mind, and fully competent to make this declaration. I also have personal knowledge of the factual statements contained herein.

2. I am the President and Executive Director of the Electronic Privacy Information Center (EPIC).

EPIC's Mission and Activities

3. EPIC is a 501(c)(3) public interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues. EPIC's mission is to secure the fundamental right to privacy in the digital age for all people through advocacy, research, and litigation. Central to EPIC's mission is oversight of government activities that impact individual privacy, free expression, and democratic values.

4. EPIC conducts numerous activities in furtherance of its mission to secure the fundamental right to privacy. EPIC routinely monitors, analyzes, and educates the public about the collection, use, retention, and transfer of personal information by federal agencies. For example, since 1994, EPIC has produced a monthly publication that covers issues related to

privacy and civil liberties in the Information Age. It currently has a readership of over 10,000, and it is among the longest-running electronic newsletters on the Internet.¹

5. As described in more detail below, EPIC also conducts oversight of government activities that impact individual privacy, free expression, and democratic values, and it has undertaken considerable research, advocacy, and public education concerning federal privacy abuses.

6. For over 30 years, EPIC has advocated for stronger data privacy and security protections for government information systems, including by calling for amendments to strengthen the Privacy Act.

7. Defendants' actions have directly hindered EPIC's mission of securing the fundamental right to privacy in the digital age for all people. By unlawfully breaching, disclosing, and accessing personal information, including Social Security numbers and other information contained in Social Security Administration systems, Defendants have directly violated Americans' privacy rights. By failing to disclose lawfully required information, Defendants have prevented EPIC from ensuring oversight of government activities that impact individual privacy, free expression, and democratic values. Their actions have caused EPIC informational, procedural, and organizational injuries.

EPIC's Use of SORNs and Computer Matching Agreements

8. In pursuit of its mission, EPIC has made extensive use of public notices and records concerning the collection, use, retention, and transfer of personal information by federal agencies. These include Systems of Records Notices ("SORNs") and Computer Matching Agreements mandated by the Privacy Act of 1974. The information published in the Federal Register through these notices is indispensable for EPIC to fulfill its organizational mission because they enable EPIC to identify, analyze, comment upon, shape advocacy around, focus

¹ See EPIC Alert, EPIC, <https://epic.org/alert/>.

public attention on, and in some cases undertake litigation to halt the collection, use, retention, and transfer of personal information by federal agencies.

9. EPIC has relied on these records, and other public notices, on hundreds of occasions to formulate comments,² testimony,³ reports,⁴ published analysis,⁵ educational materials,⁶ statements to the press and public,⁷ responses to requests for information from

² See, e.g., EPIC, Comments on Circular No. A-108, Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act (Oct. 28, 2016), <https://archive.epic.org/apa/comments/EPIC-OMB-Cir-A-108-Comments-10-28-2016.pdf>.

³ See, e.g., Testimony of Caitriona Fitzgerald, EPIC Deputy Director, on Big Data: Privacy Risks and Needed Reforms in the Public and Private Sectors (Feb. 2022), <https://epic.org/wp-content/uploads/2022/02/EPIC-HouseAdmin-Feb2022.pdf>.

⁴ See, e.g., EPIC, DHS's Data Reservoir (Aug. 2022) <https://epic.org/wp-content/uploads/2022/08/DHS-Data-Reservoir-Report-Aug2022.pdf>.

⁵ See, e.g., EPIC, Memorandum on The Pentagon Recruiting Database and the Privacy Act (July 15, 2005), https://archive.epic.org/privacy/student/epic_dod_71505.pdf.

⁶ See, e.g., EPIC Alert 28.01, EPIC (Feb. 2, 2021), https://archive.epic.org/alert/epic_alert_28.01.html; EPIC Alert 24.18, EPIC (Oct. 2, 2017), https://archive.epic.org/alert/epic_alert_24.18.html; EPIC Alert 22.22, EPIC (Nov. 25, 2015), https://archive.epic.org/alert/epic_alert_22.22.html; EPIC Alert 21.24, EPIC (Dec. 19, 2014), https://archive.epic.org/alert/epic_alert_21.24.html; EPIC Alert 21.23, EPIC (Dec. 10, 2014), https://archive.epic.org/alert/epic_alert_21.23.html; EPIC Alert 20.19, EPIC (Oct. 3, 2013), https://archive.epic.org/alert/epic_alert_20.19.html.

⁷ See, e.g., EPIC, Coalition Object to Selective Service System's Expanding Data Disclosure, EPIC (Jan. 27, 2026), <https://epic.org/epic-coalition-object-to-selective-service-systems-expanding-data-disclosures/>; EPIC Comments Call on USDA to Abandon Plan for Nationwide SNAP Database, EPIC (July 17, 2026), <https://epic.org/epic-comments-call-on-usda-to-abandon-plan-for-nationwide-snap-database/>; EPIC Urges DHS to Suspend New Counterintelligence Records System, EPIC (Jan. 13, 2021), <https://archive.epic.org/2021/01/epic-urges-dhs-to-suspend-new-.html>; In Comments to Defense Dept. EPIC Urges Adherence to Privacy Act, Algorithmic Fairness, EPIC (Apr. 22, 2019), <https://archive.epic.org/2019/04/in-comments-to-defense-dept-ep.html>; EPIC Urges Department of Defense to Limit Disclosure of Personnel Records, EPIC (Nov. 16, 2018), <https://archive.epic.org/2018/11/epic-urges-department-of-defen-1.html>.

policymakers,⁸ litigation materials, and requests under the Freedom of Information Act (“FOIA”).⁹

10. For example, EPIC has relied on SORNs to understand and respond to Immigration and Customs Enforcement (ICE) and Customs and Border Protection (CBP)’s use of location surveillance technologies and methods of obtaining location information. On July 27, 2022, EPIC provided testimony to the U.S. House Committee on Homeland Security’s Subcommittee on Border Security, Facilitation, & Operations, in which EPIC described CBP’s use of facial recognition as part of its Biometric Entry-Exit program and warned of the issues with the program and the threat CBP’s use of facial recognition poses to individuals and our society.¹⁰ In August 2022, EPIC released a report describing the ICE and CBP databases and record systems that store location information and providing policy recommendations to protect the right to privacy.¹¹

11. EPIC also routinely relies on this information to submit comments on SORNs, Computer Matching Agreements, and other proposed agency actions related to information databases and to mobilize its members and partners to do the same. On December 1, 2025, EPIC led a coalition of organizations in submitting written comments addressing computer matching agreements to the Social Security Administration (SSA) and to the Department of Homeland

⁸ See, e.g., EPIC, Comments to Rep. Lori Trahan on Efforts to Reform Privacy Act of 1974 and Protect Americans’ Data from Government Abuse (Mar. 18, 2025), <https://epic.org/wp-content/uploads/2025/05/Trahan-RFI-EPIC-Comments-Final.pdf>; Letter from EPIC to Sen. Daniel Akaka Concerning Privacy Act Modernization Act of 2011 (Mar. 27, 2012), <https://archive.epic.org/privacy/1974act/EPIC-on-S-1732-Privacy-Act-Modernization.pdf>.

⁹ See, e.g., EPIC, FOIA Request to Department of Homeland Security (Apr. 12, 2011), <https://epic.org/wp-content/uploads/privacy/socialnet/EPIC-FOIA-DHS-Social-Media-Monitoring-04-12-11.pdf>.

¹⁰ See, e.g., Testimony of Jeramie Scott, EPIC Senior Counsel, on Assessing CBP’s Use of Facial Recognition Technology (July 2022), <https://epic.org/wp-content/uploads/2022/07/Testimony-Scott-CBP-FRT-Use-2022.07.27.pdf>.

¹¹ See, e.g., EPIC, DHS’s Data Reservoir (Aug. 2022) <https://epic.org/wp-content/uploads/2022/08/DHS-Data-Reservoir-Report-Aug2022.pdf>.

Security (DHS) and on the SAVE Program SORNs. In addition to these comments, EPIC has submitted dozens of SORN and Computer Matching Agreement comments over the years.¹²

¹² EPIC et al., Comment Letter on Selective Service System SORN (Jan. 16, 2026), <https://epic.org/wp-content/uploads/2026/01/Comments-SSS-SORN-16JAN2026.pdf>; EPIC, Comment Letter to the U.S. Department of Agriculture on the National Supplemental Nutrition Assistance Program (SNAP) Information Database SORN (July 16, 2025), <https://epic.org/documents/comments-of-epic-to-the-usda-on-system-of-records-notice-for-the-snap-information-database/> (responding to 90 Fed. Reg. 26521, 26521); EPIC, Comment Letter to the U.S. Customs and Border Protection on the Electronic Visa Update System (EVUS) SORN (July 27, 2023), <https://epic.org/wp-content/uploads/2023/07/EPIC-Comments-DHS-EVUS-Social-Media-Jul-2023.pdf>; EPIC et al., Comment Letter to the U.S. Department of Health and Human Services on HIV Prevention Medication Distribution Records SORN (Feb. 22, 2023), <https://epic.org/documents/comments-of-epic-chlp-prep4all-and-patient-privacy-rights-to-hhs-on-hiv-prep-database-sorn/>; EPIC, Comment Letter to the General Services Administration on Login.gov SORN (Dec. 21, 2022), <https://epic.org/wp-content/uploads/2022/12/EPIC-comments-GSA-LoginDotGov-SORN-Dec-2022.pdf>; EPIC, Comment Letter to the Department of Homeland Security on Counterintelligence Program System of Records SORN (Jan. 13, 2020), <https://archive.epic.org/apa/comments/EPIC-Comments-DHS-Counterintelligence-SORN-January-2021.pdf>; EPIC, Comment Letter to the Department of Homeland Security on DHS Insider Threat Program SORN (Apr. 9, 2020), <https://archive.epic.org/apa/comments/EPIC-DHS-Insider-Threat-Apr2020.pdf>; EPIC, Comment Letter the Department of Defense on DOD Insider Threat Management and Analysis Center (DITMAC) & DOD Component Insider Threat Records System SORN (June 20, 2016), <https://archive.epic.org/apa/comments/EPIC-Comments-DoD-Insider-Threat-Database.pdf>; EPIC, Comment Letter to the Department of Homeland Security on Insider Threat Program SORN (Mar. 28, 2016), <https://archive.epic.org/apa/comments/EPIC-DHS-Inisder-Threat-Comments.pdf>; EPIC, Comment Letter to the Department of Justice on Insider Threat Program Records SORN (June 30, 2017), <https://archive.epic.org/apa/comments/EPIC-DOJ-Insider-Threat-Database.pdf>; EPIC, Comment Letter on U.S. Customs and Border Protection on Automated Targeting System SORN (June 21, 2012), <ht://archive.epic.org/privacy/travel/ats/EPIC-ATS-Comments-2012.pdf>; EPIC, Comment Letter to the Department of Homeland Security on DHS National Infrastructure Coordinating Center Records SORN (Dec. 15, 2010) https://epic.org/wp-content/uploads/privacy/fusion/EPIC_re_DHS-2010-0086_0085.pdf; EPIC, Comment Letter to the Department of Health and Human Services on the National Disaster Medical System (NDMS) Patient Treatment and Tracking Records System SORN (July 26, 2007), <https://archive.epic.org/apa/comments/EPIC-HHS-Med-Patient-Tracking.pdf>; EPIC et al., Comment Letter on Computer Matching Between the Selective Service System and the Department of Education, (Dec. 21, 2004), <https://archive.epic.org/privacy/student/sssdatabmatch.html> (responding to a computer matching agreement between SSS and DoE, 69 Fed. Reg. 64353, 64353 (Nov. 4, 2004).

12. SORNs and Computer Matching Agreements are often the only records available to EPIC of how and why a federal entity is collecting personal information, what information is being collected, what burdens collection will impose, how the information may be used, with whom it may be shared, how it will be stored and secured, and whether and when it will be disposed of. A public accounting of these details is both required by law and vital to the protection of the vast quantities of personal data that the federal government collects and uses or intends to collect and use.

13. When agencies do not post SORNs or other notices required to be published in the Federal Register, EPIC must resort to seeking this information through FOIA requests.¹³ However, FOIA requests are imperfect. They assume EPIC is aware of the record collection at all, and thus require a substantial amount of vigilance and effort on the part of EPIC. Responses to FOIA requests also take a substantial amount of time to receive and do not guarantee that EPIC will receive all of the information it seeks.

Informational Injuries to EPIC

14. Defendants moved ahead with overhauling SAVE (and beginning to use the system to allow states to purge voter rolls) before going through the required SORN and computer matching agreements processes.

15. When Defendants failed to timely publish these records with respect to the SAVE system and SSA's NUMIDENT system, EPIC was denied information essential to its operations, and EPIC's mission of focusing public attention on emerging privacy and civil liberties issues, and securing the fundamental right to privacy was materially impaired. Specifically, EPIC was

¹³ EPIC, FOIA Request to U.S. Department of Agriculture's Food and Nutrition Service (May 27, 2025), <https://epic.org/wp-content/uploads/2025/05/25-05-27-USDA-FOIA-Request-SNAP-data-demand.pdf> (requesting all proposed and final SORNs for the system or records that USDA/FNS has used or planned to use to store and retrieve SNAP data); EPIC, FOIA Request to U.S. Census Bureau (Mar. 8, 2019), <https://epic.org/wp-content/uploads/foia/dhs/ois/EPIC-19-03-08-DHS-OIS-FOIA-20190308-Request.pdf>; EPIC, FOIA Request to Department of Homeland Security's National Protection Programs Directorate (Apr. 12, 2018), <https://epic.org/wp-content/uploads/foia/dhs/media-monitoring-services/EPIC-v-DHS-18-1268-FOIA-request-041318.pdf>.

not able to assess how complete and accurate SAVE's search results are, and whether there are enough safeguards to protect people's privacy and voting rights.

16. Even after DHS and SSA published belated SORNs in the Federal Register, EPIC still lacks critical information, including matching-agreement information between the relevant agencies that would authorize DHS and SSA to carry out the data matching activities.

17. In particular, EPIC lacks matching-agreement information on the anticipated results of the various types of data matching, including a specific estimate of any savings; specific information on the data elements to be used in matching and the approximate number of records to be matched; the procedures for verifying information produced via matching; the procedures for ensuring the administrative, technical, and physical security of the records matched and the results of such programs; and information on assessments that have been made on the accuracy of the records that will be used in matching.

18. Without this vital information, EPIC is kept in the dark about exactly how its members' information and the information of millions of Americans is being matched across agencies and the magnitude of the privacy risks to eligible naturalized, derived, and U.S.-born citizen registrants and voters.

19. As a result, EPIC cannot properly educate the public, policymakers, or their members about these risks and how to mitigate them.

Procedural Injuries to EPIC

20. The opportunities to submit comments are also crucial for EPIC to fulfill its organizational mission because they enable EPIC to provide its expertise to inform and shape agency action to protect the public and its members with respect to issues affecting privacy rights.

21. EPIC is one of the few organizations in the country that 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 the Federal Register. 5 U.S.C. § 4 552(e)(11).

22. Defendants' failure to provide for timely, meaningful notice-and-comment opportunities on the DHS and SSA SAVE SORNs, and failure to provide any notice of the computer matching agreement between the agencies or opportunity to comment on them, denies EPIC its rightful opportunity to be heard and frustrates EPIC's mission. As a result, EPIC must divert its limited resources to more burdensome methods of advocacy for its members and the public, including litigation, the development of public resources and analysis, and the provision of expertise to lawmakers and members of the press.

23. Had EPIC been provided such an opportunity, it would have raised the privacy and security risks attendant to the federal government matching large volumes of personal information across sources, and to offer potential solutions to safeguard sensitive personal information in a manner that could be constructive to Defendants' policy goals while protecting privacy rights. This feedback could have protected EPIC's members and the public from the reputational and privacy injuries those individuals now face. This feedback could also have saved the resources and time that EPIC has expended, and continues to expend, in response to the lack of opportunity to comment.

Organizational Injuries to EPIC

24. Defendants' failure to disclose the information required has hindered EPIC's mission by preventing EPIC from ensuring oversight of government activities that impact individual privacy, free expression, and democratic values. EPIC has been prevented from fully evaluating the protections in place for the personal records implicated in the overhaul of SAVE; fully informing EPIC members, the public, the press, and other parties about the risks and protections associated with the overhaul of SAVE and its dramatically expanded use by states in voter roll maintenance; and advising EPIC's members whether they should take additional steps to safeguard their privacy.

25. EPIC as an organization understood and expected that the federal government would keep personal information collected by the SSA private and confidential and would adhere to all applicable laws, regulations, and policies protecting the privacy, confidentiality, and

security of personal information, including and especially the Privacy Act and the Social Security Act.

26. Defendants' actions have therefore forced EPIC to expend significant organizational resources to minimize the impacts on EPIC's mission. To ensure that EPIC, its members, and the public are adequately informed about Defendants' creation of a landmark new citizenship database, EPIC has investigated the overhaul and expanded use of the SAVE system. But Defendants' failure to publish legally-required information about the SAVE overhaul has forced EPIC to divert staff time to alternate, more labor-intensive, and less comprehensive methods of gathering information about the system transformation.

27. EPIC has also been forced to draft and file extensive comments on Defendants' unlawful overhaul of the SAVE system and failure to disclose information concerning their computer matching activities; and disseminate research and expertise to other organizations and individuals affected by the overhaul of SAVE to inform their own educational and advocacy missions.

28. EPIC has reassigned a senior staff member from their previous position supervising EPIC's consumer privacy work to a role principally focused on the federal government's ongoing misuse of systems of records. The unlawful overhaul of SAVE was a substantial contributor to this staffing change, and has consumed a significant portion of this staffer's time and resources.

29. To continue to carry out its mission of educating the public and makeup for the lack of access to statutorily mandated disclosures of information, EPIC has had to expend resources to develop and publish original material for EPIC's website and monthly newsletter about the overhaul of the SAVE system and its implications for voter privacy,¹⁴ the security of

¹⁴ See Voter Privacy, EPIC, <https://epic.org/issues/democracy-free-speech/voter-privacy/>.

government databases,¹⁵ and the confidentiality of government records.¹⁶ It has also had to conduct interviews and share expertise with members of the press who themselves have been deprived by Defendants of important information concerning the overhaul of the SAVE system.¹⁷

30. Altogether, four members of EPIC's staff have collectively devoted at least 75 working hours to these activities (excluding the instant litigation), time which could have been dedicated to EPIC's other programmatic priorities. Based on a very conservative estimate of these staffers' respective contributions of time and the applicable staff costs, I estimate the value of the resources diverted by EPIC so far to be at least \$5,772.

Privacy and Reputational Injuries to Members of EPIC

31. Beyond the injuries to EPIC as an organization, Defendants' actions have also inflicted privacy and reputational injuries on EPIC's members.

32. EPIC is a membership organization with members in at least 24 states and the District of Columbia. Under EPIC's bylaws, a person is a member of EPIC if they contribute to the advancement of the mission of EPIC, act in accordance with the core values and policies of EPIC, and are recognized and registered as a member by EPIC by virtue of providing financial support to EPIC.

33. Like most Americans, EPIC members have obtained Social Security numbers (SSNs) and cards in order to access work authorization and SSA benefits. EPIC has identified

¹⁵ See Government Databases, EPIC, <https://epic.org/issues/open-government/government-databases/>.

¹⁶ See Government Records & Privacy, EPIC, <https://epic.org/issues/data-protection/government-records-privacy/>.

¹⁷ See, e.g., Derek B. Johnson & Colin Wood, *The SAVE Database Was Already a Headache for States. Now It's Fueling Trump's Voter Fraud Allegations.*, Cyberscoop (June 23, 2025, 7:22 p.m.), <https://cyberscoop.com/voter-citizenship-verification-trump-save-database/>; Jude Joffe-Block & Miles Parks, *The Trump Administration is Building a National Citizenship Data System*, NPR: All Things Considered (June 29, 2025, 5:00 a.m.), <https://www.npr.org/2025/06/29/nx-s1-5409608/citizenship-trump-privacy-voting-database>.

members whose personal information was incorporated from SSA into DHS's SAVE system, and whose information from SSA has been further passed along by DHS to state officials conducting voter verification.

34. These members trusted the SSA to safeguard their private information, as provided for by the explicit guarantees of the Privacy Act, the Social Security Act, and SSA's longstanding commitment to safeguard SSN records. They did not consent to the inter-governmental collection, consolidation, disclosure, and matching of their personal information held by SSA and DHS, including disclosure to third-party states. And they did not consent to this information being used for "voter verification" purposes.

35. EPIC's members include registered voters in states like Texas and Indiana that have bulk uploaded or will imminently bulk upload sensitive voter roll data into the overhauled SAVE system to run searches on records from SSA's NUMIDENT database and other agency systems to identify potential non-citizens on their voter rolls.

36. This aggregation and publication of EPIC members' personal information in SAVE has caused, and will continue to cause, EPIC members significant harm.

37. EPIC members have been denied their statutory privacy rights.

38. EPIC members' private data was misused and repurposed in unauthorized ways, and it was shared with unauthorized third parties with no lawful right to access it through unsecured means.

39. The disclosure of their private data has also caused EPIC members, and continues to cause them, significant unease, fear, and emotional distress about the misuse of their information by those who have accessed it and will access it; the increased vulnerability of their data to theft and security breaches; and the increased risk that their data will be used to subject them to unwarranted investigations or impediments to their fundamental right to vote.

40. EPIC has also identified a member whom DHS falsely identified to the Texas Secretary of State and other SAVE users as a potential non-citizen registered voter, and thus a

potential criminal. And EPIC is aware of reporting that DHS has said that it is automatically referring these individuals for criminal investigation.

41. These EPIC members have suffered reputational harm based on the dissemination of false or misleading information about them to third parties.

I declare under penalty of perjury that, to the best of my knowledge, the foregoing is true and correct.

Executed this 11th of March, 2026 in Washington, DC.

/s/ Alan Butler

Alan Butler