

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND
SOUTHERN DIVISION**

ELECTRONIC PRIVACY INFORMATION
CENTER,

Plaintiff,

v.

U.S. CITIZENSHIP AND IMMIGRATION
SERVICES, *et al.*,

Defendants.

Case No. 8:26-cv-03457-PX

DECLARATION OF ALAN BUTLER

I, Alan Butler, declare as follows:

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 collecting, consolidating, misusing, and disclosing 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.

¹ See *EPIC Alert*, EPIC (last visited Sep. 3, 2026) <https://epic.org/alert/>.

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”) 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 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

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

³ See, e.g., *Big Data: Privacy Risks and Needed Reforms in the Public and Private Sectors*, Hearing Before the H. Comm. on H. Admin., 117th Cong. (2022) (Statement of Caitriona Fitzgerald, EPIC Deputy Director).

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

⁵ See, e.g., *Memorandum on The Pentagon Recruiting Database and the Privacy Act*, EPIC (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.

statements to the press and public,⁷ responses to requests for information from 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

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>.

⁸ See, e.g., *Comments to Rep. Lori Trahan on Efforts to Reform Privacy Act of 1974 and Protect Americans’ Data from Government Abuse*, EPIC (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*, EPIC (Mar. 27, 2012), <https://archive.epic.org/privacy/1974act/EPIC-on-S-1732-Privacy-Act-Modernization.pdf>.

⁹ See, e.g., *FOIA Request to Department of Homeland Security*, EPIC (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., *Assessing CBP’s Use of Facial Recognition Technology, Hearing Before the Subcomm. on Border Sec., Facilitation, & Operations of the H. Comm. on Homeland Security, 117th Cong. (2022) (Testimony of Jeramie Scott, EPIC Senior Counsel)*.

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 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 Security (DHS) and on the SAVE Program SORNs. In addition to these comments, EPIC has submitted dozens of comments on SORNs and related Privacy Act notices over the years.¹²

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

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->

12. SORNs are often the only records available to EPIC that describe 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 the entity will dispose of that information. 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

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](http://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).

¹³ *FOIA Request to U.S. Department of Agriculture's Food and Nutrition Service, EPIC* (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); *FOIA Request to U.S. Census Bureau, EPIC* (Mar. 8, 2019), <https://epic.org/wp-content/uploads/foia/dhs/ois/EPIC-19-03-08-DHS-OIS-FOIA-20190308-Request.pdf>; *FOIA Request to Department of Homeland Security's National Protection Programs Directorate, EPIC* (Apr. 12, 2018), <https://epic.org/wp-content/uploads/foia/dhs/media-monitoring-services/EPIC-v-DHS-18-1268-FOIA-request-041318.pdf>.

receive all of the information it seeks.

Informational Injuries to EPIC

14. Defendants have collected, consolidated, repurposed, and disclosed personal information, including by amassing citizenship data and constructing State Citizenship Lists, without going through the required SORN process.

15. When Defendants failed to timely publish these records with respect to their consolidation and disclosure of personal information, 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 not able to assess the identity of the system(s) which will be used to create and maintain the State Citizenship Lists and related records; the purported legal authority for the establishment and maintenance of the relevant system(s) and State Citizenship Lists; the categories of records implicated; the sources of those records; the full range of proffered routine uses for which the State Citizenship Lists and related records may be disclosed; the procedures for verifying the accuracy of State Citizenship Lists; the policies and practices for the access, retrieval, verification, contesting, retention, and disposal of the relevant records; the administrative, technical, and physical safeguards in place to protect the relevant systems and records; and whether any statutory exemptions assertedly apply to the relevant system(s).

16. 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 consolidated, matched, and disclosed across agencies and governments and the magnitude of the privacy risks to eligible naturalized, derived, and U.S.-born citizen registrants and voters.

17. 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 Defendants' collection, consolidation, repurposing, and disclosure of personal citizenship data and construction of State Citizenship Lists; from fully informing EPIC members, the public, the press, and other parties about the risks and protections associated with Defendants' actions; and from advising EPIC's members whether and how they should take additional steps to safeguard their privacy.

18. As a result, EPIC is also unable to properly educate the public, policymakers, or their members about these risks and how to mitigate them.

Procedural Injuries to EPIC

19. 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.

20. 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).

21. Defendants' failure to provide for timely, meaningful notice-and-comment opportunities on the systems implicated by their collection, consolidation, repurposing, and disclosure of personal citizenship data and their construction of State Citizenship Lists 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.

22. 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 offered 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.

Privacy and Reputational Injuries to Members of EPIC

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

24. 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.

25. 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 members whose personal information is implicated in SSA's disclosure and DHS's collection, consolidation, and redisclosure of SSA data.

26. 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.

27. These members did not consent to the interagency and intergovernmental collection, consolidation, disclosure, and matching of their personal information held by SSA, DHS, and the Department of State, including disclosure to third-party states. And they did not consent to this information being used for "voter verification" purposes.

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

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

30. EPIC members' personal data is being misused and repurposed in unauthorized ways and shared with unauthorized third parties with no lawful right to access it through unsecured means.

31. The disclosure of their personal 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.

32. EPIC has also identified a member whom DHS previously falsely identified to the Texas Secretary of State and other users of the Systematic Alien Verification for Entitlements (SAVE) system as a potential non-citizen registered voter, and thus a potential criminal.

33. EPIC is aware that the citizenship data Defendants are consolidating and the State

Citizenship Lists DHS is constructing are based on the same unreliable SSA data that led this member to be falsely identified as a non-citizen.

34. This EPIC member, and others similarly situated, have suffered reputational harm and will continue to suffer such harm based on the dissemination of false or misleading information about them to third parties.

I declare under penalty of perjury as prescribed in 28 U.S.C. § 1746 that the foregoing is true and correct.

Alan Butler

Executed on September __, 2026, in Washington, DC.

Citizenship Lists DHS is constructing are based on the same unreliable SSA data that led this member to be falsely identified as a non-citizen.

34. This EPIC member, and others similarly situated, have suffered reputational harm and will continue to suffer such harm based on the dissemination of false or misleading information about them to third parties.

I declare under penalty of perjury as prescribed in 28 U.S.C. § 1746 that the foregoing is true and correct.

A handwritten signature in blue ink, appearing to read 'Alan Butler', with a stylized, cursive script.

Alan Butler

Executed on September 3, 2026, in Washington, DC.