epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

Department of Homeland Security

Deferred Action for Childhood Arrivals

DHS Docket No. USCIS-2021-0006

November 29, 2021

---

The Electronic Privacy Information Center ("EPIC") submits these comments in response to the Department of Homeland Security (DHS)'s proposed rule to preserve and revise the DACA program, titled Deferred Action for Childhood Arrivals[1] ("the proposed rule"). The proposed rule maintains most of the central elements of the DACA program—a "temporary forbearance from removal" for certain undocumented people who arrived in the United States as children.[2]

EPIC supports the reissuance of the DACA program and associated privacy protections but urges several changes to further limit collection and disclosure of biographical and biometric information: (1) DHS should limit its collection of biometric data and refrain from expanding upon the data collected or its use; (2) DHS should enact further protections to safeguard from enforcement agencies data on DACA requestors who were denied deferred action and on DACA

[1] Deferred Action for Childhood Arrivals, 86 Fed. Reg. 53736 (proposed Sept. 28, 2021) (to be codified at 8 C.F.R. pt. 106, 8 C.F.R. pt. 236, 8 C.F.R. pt. 274).
[2] *Id*. at 53739. The proposed rule departs from the original DACA program by separating the employment authorization process from the DACA determination. *Id*. at 53739-40. The new proposed rule also explicitly defines deferred action as "temporary forbearance from removal that does not confer any right or entitlement to remain in or re-enter the United States, and that does not prevent DHS from initiating any criminal or other enforcement action against the DACA recipient at any time." *Id*. at 53739.

requestors' family members; (3) DHS should eliminate or amend the broad exceptions to its information use protections; and (4) DHS should eliminate or amend the broad disclaimer in Form I-812D.

EPIC is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging privacy and related human rights issues, and to protect privacy, the First Amendment, and constitutional values. EPIC has a particular interest in preserving the privacy rights of immigrants and travelers at the border, including limiting the collection of biometric data and safeguarding the data that is collected.[3]

## I. Background on Data Protection under DACA and EPIC Advocacy

In 2012, DHS established the DACA program and began collecting the personal data of at least 800,000 individuals. The personal data included biometric and biographical data. DHS's 2012 Privacy Impact Assessment stated that collected data would be entered into "mixed databases," including the Alien Files (A-Files), a database managed by USCIS, CBP, and ICE.

[3] *See, e.g.*, *Traveler Screening and Border Surveillance*, EPIC, https://epic.org/issues/surveillance-oversight/border-surveillance; *EPIC, Coalition Urge DHS to End Broad, Unwarranted Surveillance Programs*, EPIC (Sept. 16, 2021), https://epic.org/epic-coalition-urge-dhs-to-end-broad-unwarranted-surveillance-programs (letter to DHS Secretary); *EPIC, Coalition Call on Biden Administration to Abandon "Virtual Border Wall," Invest in Migrant Communities*, EPIC (Feb. 25, 2021), https://epic.org/epic-coalition-call-on-biden-administration-to-abandon-virtual-border-wall-invest-in-migrant-communities (letter to Biden Administration concerning U.S. Citizenship Act of 2021); *EPIC v. ICE (Facial Recognition Services)*, EPIC (2020), https://epic.org/documents/epic-v-ice-facial-recognition-services (background on EPIC FOIA litigation concerning ICE's use of facial recognition services); *EPIC Urges Advisory Council to Address Privacy Risks of DHS's Use of Biometrics*, EPIC (Dec. 11, 2020), https://epic.org/epic-urges-advisory-council-to-address-privacy-risks-of-dhss-use-of-biometrics (Comment to the Homeland Security Advisory Council); *Collection and Use of Biometrics by U.S. Citizenship and Immigration Services*, EPIC (Oct. 2020), https://epic.org/documents/collection-and-use-of-biometrics-by-u-s-citizenship-and-immigration-services (APA Comment); *EPIC Opposes DHS's Plans to Broadly Expand Biometric Collection*, EPIC (Oct. 14, 2020), https://epic.org/epic-opposes-dhss-plans-to-broadly-expand-biometric-collection (APA Comment); *EPIC Settles ICE Lawsuit About Technology Used for Warrantless Searches of Mobile Devices*, EPIC (June 24, 2020), https://epic.org/epic-settles-ice-lawsuit-about-technology-used-for-warrantless-searches-of-mobile-devices; *Deferred Action for Childhood Arrivals ("DACA")*, EPIC, https://epic.org/deferred-action-for-childhood-arrivals-daca; *EPIC Urges Congress to Press ICE on Surveillance Practices*, EPIC (Apr. 9, 2019), https://epic.org/epic-urges-congress-to-press-ice-on-surveillance-practices; *DNA-Sample Collection From Immigration Detainees*, EPIC (Nov. 12, 2019), https://epic.org/documents/dna-sample-collection-from-immigration-detainees (APA Comment).

DHS also assured recipients' data would be "protected from disclosure to ICE and CBP for the purpose of immigration enforcement proceedings."[4]

In 2017, the Trump Administration attempted to rescind the DACA program by Executive Order.[5] In response, EPIC issued a FOIA request calling for records demonstrating DHS and USCIS's handling of personal data obtained under the DACA program.[6] EPIC also called on the U.S. Senate Committee on the Judiciary to inquire into how DHS would mitigate the privacy risks associated with the program's rescission.[7] In October 2017, a DHS official told Congress it would be adhering to the guidelines for safeguarding DACA recipients' data located in the 2012 Privacy Impact Assessment.[8]

## II. EPIC's Recommendations to the Proposed Rule

EPIC recognizes the value that the DACA program confers on its recipients, who otherwise might live under constant threat of removal despite growing up and living most of their lives in the United States. As such, EPIC commends the DHS's effort to maintain and fortify most elements of the original DACA program. EPIC also appreciates the preservation of the privacy protections from the 2012 Privacy Impact Assessment,[9] and DHS's refrain from expanding its collection of and dissemination of recipients' personal information. Nevertheless, EPIC identifies several concerning privacy risks present in both the preexisting features of the DACA program and new privacy risks under this Notice of Proposed Rulemaking.

---

[4] *Privacy Impact Assessment for the Deferred Action for Childhood Arrivals (DACA)*, DHS (Aug. 15, 2012), at 13, https://www.dhs.gov/sites/default/files/publications/privacy_pia_uscis_daca_0.pdf (DHS/USCIS/PIA-045).
[5] Enhancing Public Safety in the Interior of the United States, 82 Fed. Reg. 8799 (Jan. 25, 2017) (codified as E.O. 13768) (revoked by E.O. 13993 (Jan. 20, 2021)).
[6] *See Deferred Action for Childhood Arrivals ("DACA")*, DHS, https://epic.org/deferred-action-for-childhood-arrivals-daca/#FOIA (linking EPIC's October 18, 2017 FOIA request to USCIS, *available at* https://epic.org/wp-content/uploads/foia/uscis/daca/EPIC-17-10-18-USCIS-FOIA-20171018-Request.pdf).
[7] *Id*. (describing EPIC's October 2017 request to the Senate Judiciary Committee to protect Dreamers' privacy, *available at* https://epic.org/wp-content/uploads/testimony/congress/SJC-DACA-Oct2017.pdf).
[8] *Id*. (describing DHS official's statement to the Senate in 2017 assuring that the agency won't target Dreamers).
[9] *Supra* note 4.

*a. DHS Should Limit Collection of and Safeguard Biometric Data*

First, EPIC once again urges DHS to limit its collection of biometric and biographical data.[10] Data requested on applicants, their families, and associates should be limited only to the information that is absolutely necessary to verify the applicant's eligibility for temporary forbearance under the DACA program. Moreover, DHS must provide the public the opportunity to comment on any future proposals to expand either the biometric data collected or its use.

*b. DHS Should Institute Heightened Protections for Non-DACA recipients*

EPIC also urges DHS to establish stronger safeguards for data from applicants denied DACA status. The proposed rule explains that noncitizens' A-Files are used by ICE and CBP "to verify whether [noncitizens] are permitted to remain in or enter the United States and to ensure that the officers do not erroneously remove or take other enforcement action . . . against a person, such as a DACA recipient."[11] While this ability to view DACA requestors immigration statuses certainly would protect a DACA *recipient*, as written, it does not necessarily protect a *denied* DACA requestor. The DACA requestor who has been denied deferred action, whose information and immigration status is otherwise listed on the A-File, could therefore be vulnerable to identification and removal by enforcement officers even if their case is not affirmatively referred to ICE. This data collection makes applying to the DACA program risky for applicants who must

[10] EPIC has long advocated for restricting biometric data collection and instituting strong privacy protections to safeguard collected data. *See, e.g.*, EPIC, Coalition Urge DHS to Rescind CBP's Proposed Biometrics Rulemaking, EPIC (Mar. 10, 2021), https://epic.org/epic-coalition-urge-dhs-to-rescind-cbps-proposed-biometrics-rulemaking; *EPIC Urges CBP to Halt Use of Facial Recognition for Biometric Entry/Exit*, EPIC (Dec. 21, 2020), https://epic.org/epic-urges-cbp-to-halt-use-of-facial-recognition-for-biometric-entry-exit; *EPIC Opposes DHS's Plans to Broadly Expand Biometric Collection*, EPIC (Oct. 14, 2020), https://epic.org/epic-opposes-dhss-plans-to-broadly-expand-biometric-collection; *Comments of the Electronic Privacy Information Center to the National Protection and Programs Directorate of the Department of Homeland Security*, EPIC, (June 14, 2013), https://epic.org/wp-content/uploads/privacy/biometrics/EPIC-OBIM-Cmts.pdf (EPIC's APA Comment regarding the Office of Biometric Identity Management's biometric data collection at ports of entry).

[11] Deferred Action for Childhood Arrivals, 86 Fed. Reg at 53771.

decide whether applying is worth the possibility of being denied and becoming more vulnerable to deportation.

To eliminate this risk and avoid deterring DACA applicants, EPIC urges DHS not to enter biographical information, biometric information, and immigration status information from denied applicants into the A-File. If there is information about denied applicants entered into the A-File—and EPIC strongly urges that that information is not entered—EPIC urges DHS to hide the immigration statuses of those applicants from enforcement agencies accessing the A-File.

EPIC also requests that family information from DACA applicants be hidden in the A-File from enforcement agencies. When applying, information about families and guardians of applicants are entered into A-File.[12] These family members are not independently electing to subject themselves to consideration for the DACA program. Often, these family members may themselves be undocumented. As third parties to the applicant's consideration under DACA, family members' information should be afforded heightened privacy protections. In particular, their biographical, biometric, and immigration status information should be hidden from view of any enforcement agencies accessing the A-File. One way to accomplish this is by inputting family information only within the file of the applicant and not creating new files for non-applicant family members. Family member information can then become a part of the portion of the applicant's A-File that is not immediately accessible by simple searches.

*c. DHS Should Limit the Exceptions to Information Use Protections*

Second, while EPIC appreciates the partial privacy protection afforded to DACA recipients, exceptions to those privacy protections must be narrow and limited. The proposed rule provides for broad and ambiguous exceptions to DHS's promise to safeguard DACA

[12] *See id.*

recipient's information from use by federal, state, or local law enforcement. EPIC urges DHS to amend and eliminate these exceptions.

The proposed rule states that "information about the DACA requestor and their family members and guardians is protected from disclosure to ICE and CBP for the purpose of immigration enforcement proceedings unless the requester meets the criteria set forth in the 2011 USCIS NTA policy memorandum."[13] The proposed rule also notes that the information may be shared with national security and law enforcement agencies, including ICE and CBP, for purposes other than removal, including for assistance in the consideration of DACA, to identify or prevent fraudulent claims, for national security purposes, or for the investigation or prosecution of a criminal offense."[14]

EPIC objects to the breadth of these exceptions. Concerning the criminal offense exception, EPIC urges DHS to safeguard information provided by applicants from use for investigation or prosecution of criminal offenses. The criminal offense exception is overbroad and may deter otherwise eligible applicants from submitting requests. The "investigation of a criminal offense" can include the investigation of misdemeanor criminal offenses against property or other nonviolent crimes. Moreover, permitting information use for a criminal investigation in general means law enforcement can access personal data of suspects or the family members or acquaintances of criminal suspects. The criminal offense exception also may deter otherwise eligible applicants from submitting requests. The act of applying for the DACA program should not be an act of subjecting oneself to heightened scrutiny by criminal law enforcement. Or worse, it should not mean subjecting one's family members to police scrutiny. DACA applicants should not have to trade the threat of ICE knocking on their door in exchange

[13] *Id.*
[14] *Id.*

for the threat of their local police knocking on their door—or the doors of their loved ones. The proposed rule as written permits such a scenario and must be amended to avoid deterring otherwise eligible applicants from applying.

Second, EPIC objects to the vague and broad "national security" exception to DHS's promise to safeguard collected information. The federal government, and in particular DHS, has a history of broadly using "national security" to justify policies that erode civil liberties protections.[15] The justification is also disproportionately used to target or burden racial and religious minorities, particularly people who are Black, Middle Eastern, South Asian, African, and/or Muslim. As such, EPIC opposes DHS's proposal to create this broad, opaque, and potentially discriminatory exception to the information use restrictions it otherwise has proposed to integrate into the DACA Program.

Thirdly, EPIC urges that the exception for the purpose of "identify[ing] or prevent[ing] fraudulent claims" be limited only to identifying or preventing fraudulent *DACA applications*. EPIC understands the necessity of verifying the validity of information provided by DACA applicants when considering whether to grant deferred action. However, as explained above, EPIC strongly believes that submitting a DACA application should not catalyze a criminal investigation or prosecution of a DACA applicant or their family members.

[15] *See, e.g.*, UNCONSTITUTIONAL AND UNJUST: DISMANTLING 20 YEARS OF DISCRIMINATORY 'NATIONAL SECURITY' POLICY, ASIAN L. CAUCUS, AM.-ARAB ANTI-DISCRIMINATION COMM., P'SHIP FOR THE ADVANCEMENT OF NEW AMS., CLEAR, & CCR (Sept. 20, 2021), https://www.advancingjustice-alc.org/wp-content/uploads/2021/09/Final_9.11Memo-1.pdf; Hugh Handeyside, *The Watchlisting System Exemplifies the Government's Post-9/11 Embrace of Biased Profiling*, ACLU (Sept. 9, 2021), https://www.aclu.org/news/civil-liberties/the-watchlisting-system-exemplifies-the-governments-post-9-11-embrace-of-biased-profiling; Faiza Patel, *Ending the 'National Security' Excuse for Racial and Religious Profiling*, BRENNAN CTR. (July 22, 2021), https://www.brennancenter.org/our-work/analysis-opinion/ending-national-security-excuse-racial-and-religious-profiling.

d. *DHS Should Reconsider the Form I-821D Disclaimer and Limit Third-Party Data Sharing*

Finally, EPIC urges DHS to reconsider the disclaimer in the privacy notice in Form I-821D that advises that information will be shared with federal, state, local and foreign agencies under routines described in system of records notices ("SORNs").[16] "Routine use" under the SORN means third parties may access the information during law enforcement investigations.[17] These third parties would be able to access information of people suspected of violating immigration-related criminal or civil provisions.[18] It also allows access to the same information from applicants' relatives and associates who are subject to the INA.[19]

EPIC objects to the data sharing alluded to in this disclaimer because the combined risk and complexity it poses could potentially deter eligible DACA recipients from applying. First, as emphasized in the proposed rule's justification for the program, DACA recipients and their loved ones rely on deferred action.[20] DACA recipients have known no other home than the United States and have built their families and livelihoods here. Deportation would be catastrophic for these recipients and their families. Under these conditions, DACA applicants submitting Forms I-821D are not meaningfully consenting to the broad information disclosures listed in the Form I-821D disclaimer. Second, as a practical matter, the disclaimer does not actually provide the information applicants need to decide whether to consent to such a disclosure. Referring to SORNS without providing the information contained in them makes it challenging for lay

[16] *See* 86 Fed. Reg. at 53771; *Instructions for Consideration of Deferred Action for Childhood Arrivals*, DHS, at 13, https://www.uscis.gov/sites/default/files/document/forms/i-821dinstr.pdf (Form I-821D).
[17] 78 Fed. Reg. 69864, 69865 (Nov. 21, 2013) (No. DHS-2013-0069), *available at* https://www.govinfo.gov/content/pkg/FR-2013-11-21/html/2013-27895.htm.
[18] *Id*. at 69866.
[19] *Id*.
[20] *See, e.g.*, Deferred Action for Childhood Arrivals, 86 Fed. Reg at 53738.

audiences to determine how their information will be shared. Applicants would have to learn what a SORN is, access the SORN, read through complicated regulatory provisions and acronyms of various agencies, and comprehend the privacy and legal implications of such a disclosure. Few laypeople can be expected to adequately digest this information and meaningfully consent to a disclosure of their private information. The disclaimer should thus be narrowed to preserve applicants' privacy and the disclaimer's scope should be specified in greater detail directly on Form I-821D.

## III. Conclusion

While EPIC generally supports the protections granted by the DACA program, EPIC urges DHS to implement the aforementioned measures to better safeguard the privacy rights of DACA requestors, their families, and their communities.

Respectfully Submitted,

*Jeramie Scott*
Jeramie Scott
EPIC Senior Counsel

*Jake Wiener*
Jake Wiener
EPIC Law Fellow

*Dana Khabbaz*
Dana Khabbaz
EPIC Law Fellow