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, U.S. Customs and Border Protection

Collection of Biometric Data From Aliens Upon Entry to and Departure From the United States

[Docket No. USCBP-2020-0062]

December 21, 2020

The Electronic Privacy Information Center (EPIC) submits these comments in response to the U.S. Customs and Border Protection (CBP) Notice of Proposed Rulemaking (NPRM) titled "Collection of Biometric Data From Aliens Upon Entry to and Departure From the United States" published November 19, 2020.[1] The Department of Homeland Security (DHS) and its subcomponent CBP propose to expand the scope of Biometric Entry/Exit by removing all references to pilot programs at specific locations and to mandate that all aliens be photographed upon entry to and departure from the United States.

EPIC urges CBP to refrain from using facial recognition technology for Entry/Exit as facial recognition is an inherently dangerous technology and CBP has not demonstrated competence to safeguard individuals' data. In the alternative, if CBP does continue to use facial recognition technology, EPIC urges the agency to implement only 1:1 facial recognition matching to authenticate travel documents and to use no form of facial recognition which requires a database of images of facial recognition profiles.

[1] 85 F.R. 74162.

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 Act safeguards enacted by Congress.[2] EPIC also has a sustained interest in DHS's biometrics policies and practices, particularly the development and implementation of Biometric Entry/Exit.[3]

Through the NPRM, DHS plans to initially "expand its facial recognition system to commercial air ports of entry" and to eventually "establish a biometric entry-exit system at all air, sea, and land ports of entry".[4] DHS's rule would require non-citizens to be photographed upon both entry and departure from the United States.[5] The rule would impose "voluntary" collection of facial recognition images from U.S. citizens and provide for faster deletion of images collected from

[2] *See, e.g.*, Comments of EPIC to the Department of Homeland Security, Correspondence Records Modified System of Records Notice, Docket No. DHS-2011-0094 (Dec. 23, 2011), http://epic.org/privacy/1974act/EPIC-SORN-Comments-FINAL.pdf; Comments of EPIC to the Department of Homeland Security, 001 National Infrastructure Coordinating Center Records System of Records Notice and Notice of Proposed Rulemaking, Docket Nos. DHS-2010-0086, DHS-2010-0085 (Dec. 15, 2010), http://epic.org/privacy/fusion/EPIC_re_DHS-2010-0086_0085.pdf; Comments of EPIC to the Department of Homeland Security, Terrorist Screening Database System of Records Notice and Notice of Proposed Rulemaking, Docket Nos. DHS-2016-0002, DHS-2016-0001 (Feb. 22, 2016), https://epic.org/apa/comments/EPIC-Comments-DHS-TSD-SORN-Exemptions-2016.pdf.

[3] *See e.g.*, Comments of EPIC to the Transportation Security Administration, Intent to Request Revision of Agency Information Collection Activity Under OMB Review: TSA PreCheck, Docket ID: TSA-2013-0001 (June 22, 2020), https://epic.org/apa/comments/EPIC-TSA-PreCheck-FRT-Comment-June2020.pdf; Comments of EPIC to the Department of Homeland Security, Agency Information Collection Activities: Biometric Identity, Docket No. 1651-0138 (Jul. 24, 2018), https://epic.org/apa/comments/EPIC-CBP-Vehicular-Biometric-Entry-Exit-Program.pdf; EPIC v. CBP (Biometric Entry/Exit Program), https://epic.org/foia/dhs/cbp/biometric-entry-exit/default.html (EPIC obtained a report which evaluated iris imaging and facial recognition scans for border control); EPIC Statement to U.S. House Committee on Homeland Security, "Border Security, Commerce and Travel: Commissioner McAleenan's Vision for the Future of CBP" (Apr. 24, 2018), https://epic.org/testimony/congress/EPIC-HHSC-CBP-Apr2018.pdf; Comments of EPIC to the Department of Homeland Security, Privacy Act of 1974: Implementation of Exemptions; Department of Homeland Security/U.S. Citizenship and Immigration Services—018 Immigration Biometric and Background Check (IBBC) System of Records, Docket Nos. DHS-2018-0002 and DHS-2018-0003 (Aug. 30, 2018), https://epic.org/apa/comments/EPIC-DHS-Immigration-Biometric-Database.pdf.

[4] 85 F.R. 74163.

[5] 85 F.R. 74164.

citizens.[6] To implement Biometric Exit, CBP would allow airlines to administer CBP's facial recognition technology, or even use their own technology to provide CBP with facial recognition images.[7] CBP's planned system would compare images to travelers to "galleries" of facial recognition profiles compiled and updated by the agency.[8] This is known as 1:N matching, where instead of comparing two photos, a gallery is searched for a potential match. CBP would populate the galleries with images from its Advanced Passenger Information System (APIS) and other sources, including passport photos from the State Department, based on flight plans or frequent border crossers.[9]

CBP's current Biometric Entry program collects facial recognition images from travelers upon arrival to the U.S. and stores those images in CBP's Traveler Verification System (TVS).[10] CBP's system compares the images against biometric photo templates stored in the Automated Targeting System-Unified Passenger (ATS-UPAX) subsystem of TVS.[11] The proposed expansion of Biometric Exit would function in the same way, comparing live traveler photos against a profile image stored in CBP's databases.[12] According to CBP's Privacy Impact Assessment, U.S. citizen photos are to be deleted within 12 hours of confirming that the individual is a citizen.[13] Non-citizen images are retained for 14 days.[14]

[6] 85 F.R. 74177.
[7] 85 F.R. 74176.
[8] 85 F.R. 74163.
[9] 85 F.R. 74175.
[10] *Id*.
[11] DHS/CBP/PIA-056 Traveler Verification Service (Nov. 14, 2018), https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp056-tvs-january2020_0.pdf.
[12] *Id*. at 4.
[13] *Id*. at 10.
[14] *Id*.

I. CBP has failed to properly administer the existing Biometric Entry/Exit pilot programs.

CBP's implementation of the various Biometry Entry/Exit pilot programs has consistently fallen below baseline standards for privacy articulated in DHS's Fair Information Privacy Principles (FIPPs).[15] The FIPPs set benchmarks for data collection and use that DHS must meet to comply with the Privacy Act of 1974.[16] The FIPPs comprise eight mandates: Transparency, Individual Participation, Purpose Specification, Data Minimization, Use Limitation, Data Quality and Integrity, Security, and Accountability/Auditing.[17] By DHS policy, the FIPPs "must be considered whenever a DHS program or activity raises privacy concerns or involves the collection of personally identifiable information from individuals, regardless of their status."[18] If CBP cannot meet their own metrics for ensuring privacy when using facial recognition then the agency should not collect that data from even more individuals.

a. CBP does not meet the FIPPs of Transparency and Individual Participation by failing to provide adequate notice on facial recognition programs.

The Government Accountability Office (GAO) investigated CBP's Biometric Entry/Exit programs this year.[19] In a September 2020 report, the GAO found four major shortcomings in CBP's Biometric Entry/Exit program. Together, these failures demonstrate that CBP is either unable or unwilling to take basic steps to protect individuals' privacy, often falling short of DHS's Fair Information Practice Principles (FIPPs).

[15] Hugo Teufel III, The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security Memorandum Number 2008-01, Dep't. of Homeland Sec. (Dec. 29, 2008), https://www.dhs.gov/sites/default/files/publications/privacy-policy-guidance-memorandum-2008-01.pdf.
[16] Privacy Act of 1974, 5 U.S.C. § 552a, as amended.
[17] DHS FIPPs Memorandum, supra note 15, at 4.
[18] Hugo Teufel III, Memorandum Number 2008-01, Privacy Policy Guidance Memorandum (Dec. 29, 2008), https://www.dhs.gov/sites/default/files/publications/privacy-policy-guidance-memorandum-2008-01.pdf.
[19] U.S. Gov't Accountability Off., GAO-20-568 Facial Recognition: CBP and TSA are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues (Sept. 2020) (hereinafter GAO Facial Recognition Report), https://www.gao.gov/products/GAO-20-568.

First, the GAO found that CBP routinely failed to provide adequate notice and opt out procedures. At the time of the GAO's investigation, CBP's online resources on facial recognition programs had incomplete information and did not list all of the locations where CBP had deployed facial recognition.[20] Similarly, CBP did not provide enough information for call center employees to answer questions about facial recognition.[21] The call center was often offline, and when GAO could get through, operators did not know which air and land ports were using facial recognition.[22] As a result, CBP has not met the FIPP of Transparency.

Second, signs at airports are consistently outdated and contradictory. The GAO found that signs within a single airport contained contradictory information on data retention policies.[23] CBP claimed their failure to update signage was justified by the prohibitive cost of printing signs.[24] CBP has not prioritized updating posed notices to reflect current procedures and data retention protocols. CBP appears unconcerned with providing accurate and meaningful notice to travelers. CBP has not done enough to fulfill the Transparency FIPP.

Third, the GAO faulted CBP for providing inadequate information on how travelers could opt-out of facial recognition identity verification.[25] CBP's signs mentioned an opt-out but did not describe what "alternative procedures" travelers would have to go through in lieu of facial recognition.[26] Throughout its implementation of Biometric Entry/Exit CBP has provided vague and inconsistent descriptions of alternative screening procedures. In 2018, EPIC obtained documents through a FOIA lawsuit revealing that CBP had developed a detailed opt-out and alternative

[20] *Id*. at 39.
[21] *Id*. At 39-40.
[22] *Id*.
[23] *Id*. at 40.
[24] *Id*.
[25] *Id*. at 41.
[26] *Id*.

screening procedure.[27] But the agency did not describe that procedure to the public.[28] This critique echoes the Data Privacy and Integrity Advisory Committee's report from a year earlier which recommended basic improvements to CBP's written notices to improve readability, ensure adequate time for consideration, and explain opt-out procedures.[29] CBP has for years been on notice that the agency needs to provide and publicize a clear opt-out procedure. As of May 2020 it has not done so.

Fourth, CBP and its corporate partners routinely fail to post signs or obscure notices on facial recognition. The GAO observed that "facial recognition signs were not consistently posted or were posted in such a way that they were not easily seen by travelers."[30] Where CBP delegates responsibility for posting signs to commercial airlines, the GAO found that the agency does not enforce or monitor this requirement.[31] As a result, required signs are often missing. The GAO also observed signs that were difficult to read because they were posted far away from travelers and written in small print.[32] Facial recognition notices are also often blocked by other signs so that they could not be read.[33] CBP claims that their Biometric Entry/Exit staff is small, and cannot ensure signs are posted so they rely on local airport agents.[34] Yet CBP's airport agents told the GAO that they did not check signs, and were not required to do so.[35] CBP is currently unable to ensure that

[27] U.S. Customs and Border Prot., Traveler Verification Service: Standard Operating Procedure at 9 (June, 2017), https://epic.org/foia/dhs/cbp/biometric-entry-exit-alt-screening-procedures/Traveler-Verification-Service-SOP-June2017.pdf; U.S. Customs and Border Prot., Biometric Air Exit: Standard Operating Procedure (Mar. 2019), https://epic.org/foia/dhs/cbp/biometric-entry-exit-alt-screening-procedures/Biometric-Air-Exit-SOP-Mar2019.pdf.

[28] *See*: EPIC v. CBP (Biometric Entry-Exit Alternative Screening Procedures), EPIC.org (last accessed Dec. 18, 2020 at 2:15pm), https://epic.org/foia/dhs/cbp/alt-screening-procedures/.

[29] DHS Data Privacy and Integrity Advisory Committee, Report 2019-01 of the DHS Data Privacy and Integrity Advisory Committee (DPIAC): Privacy Recommendations in Connection with the Use of Facial Recognition Technology at 4-5 (Feb. 26, 2019) (hereinafter DPIAC Facial Recognition Recommendations), https://www.dhs.gov/sites/default/files/publications/Report%202019-01_Use%20of%20Facial%20Recognition%20Technology_02%2026%202019.pdf.

[30] GAO Facial Recognition Report at 42.

[31] *Id.*

[32] *Id.* at 44.

[33] *Id.*

[34] *Id.* at 43.

[35] *Id.*

travelers receive adequate, or often any, notice that they can opt out of one of the most invasive technologies in use today.

By not providing travelers meaningful notice and the time to consider their options, the GAO found that CBP has not met its requirements under the FIPPs of Transparency and Individual Participation.[36] While providing notice may not be the strongest step CBP can take to protect individuals' personally identifiable information, it is the easiest. If CBP cannot or will not take the basic steps necessary to provide travelers with adequate notice of facial recognition, then the agency's ability to provide more substantive protection is dubious at best.

CBP's failure to provide notice of its facial recognition policies has caused real privacy harms. An ACLU attorney crossing the southern border was forced to submit to facial recognition when a CBP border agent refused to provide an opt-out.[37] The GAO received reports of similar incidents, including individuals "being told by CBP officers and airline agents that opting out would lead to additional security scrutiny, increased wait times, and could be grounds to deny boarding."[38] Although CBP claims to provide opt-out procedures which do not inconvenience or prejudice travelers, the agency is clearly failing to adequately inform either its employees or the general public of these procedures.

b. *CBP has not performed necessary audits to ensure facial recognition images are secure.*

In its review earlier this year, the GAO found that CBP "has not audited most of its partners and has not developed a plan for future audits".[39] CBP's agreements prohibit corporate partners from

[36] *Id*. at 46.
[37] Shaw Drake, A Border Officer Told Me I Couldn't Opt Out of the Face Recognition Scan. They Were Wrong., ACLU (Dec. 5, 2019), https://www.aclu.org/news/immigrants-rights/a-border-officer-told-me-i-couldnt-opt-out-of-the-face-recognition-scan-they-were-wrong/.
[38] GAO Facial Recognition Report at 42.
[39] *Id*. at 46.

retaining images for their own purposes and require partners to expediently delete images.[40] CBP has allowed its partners to use facial recognition technology for identification, since 2017 for airlines and since 2018 for cruise ships.[41] It took three years for the agency to perform its first audit of an airline, in March 2020.[42] The agency still has not audited a cruise line. In that time, over 7 million passengers have submitted to facial recognition by more than 20 airlines and cruise lines.[43] More than 95% of CBP's corporate partners have never received an audit. The agency has no idea if its partners are taking individuals' images for their own purposes or complying with data retention requirements.

The GAO's findings echo DPIAC's findings from a year earlier, in which the Committee stressed that "it is important to ensure transparency in the process, strong contractual guidelines, auditing, and rigor in the process of ensuring the FIPPs are adhered to."[44] The DPIAC called for thorough audits as a necessary step to protect particularly sensitive facial recognition images.[45] Yet despite the DPIAC's urgings, CBP has performed only one audit of its commercial partners and has no plan in place for further audits of either its commercial partners or its contractors. This amounts to willful blindness on the part of the agency. CBP's failure to perform necessary audits for years displays a callous disregard for individuals' privacy, even after the agency suffered a serious data breach of its facial recognition systems.

c. CBP cannot safeguard facial recognition images.

Recent data breaches and hacks within CBP and across the federal government demonstrate that CBP is incapable of safeguarding sensitive personal information, including facial recognition

[40] *Id*.
[41] *Id*.
[42] *Id*.
[43] *Id*.
[44] DPIAC Facial Recognition Report at 10.
[45] *Id*. at 10-12.

images. In 2016 the U.S. Government Accountability Office warned that "[c]yber-based intrusions and attacks on federal systems have become not only more numerous and diverse but also more damaging and disruptive."[46] The GAO called on DHS to enhance cybersecurity protection in key areas including intrusion detection and prevention. At the time DHS had not even put in place an adequate process for sharing information on intrusions and potential malicious activity.[47] Since that time DHS and its subcomponents have not shown that they are capable of safeguarding personally identifiable information, particularly biometric data.

In 2019 a data breach at CBP subcontractor Perceptics, LLC exposed approximately 184,000 images of travelers from CBP's Biometric Entry/Exit pilot.[48] Perceptics staff were able to violate several DHS security and privacy protocols to download the images used for facial recognition without CBP's IT security controls preventing the unauthorized action or sounding an alarm.[49] When Perceptics, LLC was subsequently hacked outside agents had access to those 184,000 images and an additional 105,000 license plate images.[50] At least 19 facial recognition images were released on the dark web.[51] DHS's Office of the Inspector General found that, "Perceptics was able to make unauthorized use of CBP's biometric data, in part because CBP did not implement all available IT security controls, including an acknowledged best practice."[52] OIG concluded that CBP "Did not adequately fulfill its responsibilities for IT security".[53]

[46] U.S. Gov't Accountability Office, DHS Needs to Enhance Capabilities, Improve Planning, and Support Greater Adoption of Its National Cybersecurity Protection System (Jan. 2016), https://www.gao.gov/assets/680/674829.pdf.
[47] *Id*. at 27.
[48] Joseph Cuffari, Review of CBP's Major Cybersecurity Incident During a 2019 Biometric Pilot, Dep't of Homeland Sec. Off. of Inspector Gen. (Sept. 21, 2020), https://www.oig.dhs.gov/sites/default/files/assets/2020-09/OIG-20-71-Sep20.pdf .
[49] *Id*. at 6.
[50] *Id*. at 8.
[51] *Id*. at 13.
[52] *Id*. at 12.
[53] *Id*.

The 2019 breach is far from the only example of DHS and its' subcomponents failing to safeguard sensitive information. DHS and agencies across the federal government were recently exposed in the SolarWind hack.[54] The extent of the hack remains unknown, but emails at several federal agencies were compromised.[55] The Federal Emergency Management Agency (FEMA) unnecessarily disclosed sensitive information of victims of the 2017 California wildfires, exposing up to 2.3 million people.[56] FEMA shared details of victims financial institutions and personal lives including EFT and bank transit numbers and complete addresses.[57] The unidentified subcontractor then failed to notify FEMA of receiving extra information.[58] A 2017 data breach by an agency employee exposed the personal information, including Social Security numbers, of 247,167 DHS employees.[59] DHS's recent track record demonstrates that the agency has failed to implement adequate safeguards for personal data.

Data breaches are common across the federal government as well, exposing the PII of millions to exploitation and abuse. On August 24, 2020 a cyber-attack compromised a federal

[54] Megan Roos, Suspected Russian SolarWinds Hack Compromised Homeland Security Department, Newsweek (Dec. 14, 2020), https://www.newsweek.com/suspected-russian-solarwinds-hack-compromised-homeland-security-department-1554656.

[55] David E. Sanger, Nicole Perlroth and Eric Schmitt, Scope of Russian Hack Becomes Clear: Multiple U.S. Agencies Were Hit, NY Times (Dec. 14, 2020), https://www.nytimes.com/2020/12/14/us/politics/russia-hack-nsa-homeland-security-pentagon.html.

[56] Christopher Mele, Personal Data of 2.3 Million Disaster Victims Was Released by FEMA, Report Says, N.Y. Times (Mar. 22, 2019), https://www.nytimes.com/2019/03/22/us/fema-data-breach.html; John V. Kelly, Management Alert – FEMA Did Not Safeguard Disaster Survivors' Sensitive Personally Identifiable Information, OIG-19-32 Dep't of Homeland Sec. Off. of Inspector Gen. (Mar. 15, 2019), https://www.oig.dhs.gov/sites/default/files/assets/2019-03/OIG-19-32-Mar19.pdf.

[57] OIG FEMA Memorandum, *supra* note 56, at 4.

[58] *Id*.

[59] Steven Musil, Homeland Security breach exposes data on 240,000 employees, CNET (Jan. 3, 2018), https://www.cnet.com/news/homeland-security-breach-exposes-data-on-240000-employees/; Dep't. of Homeland Sec., Privacy Incident Involving DHS Office of Inspector General Case Management System (Update) (Jan. 18, 2018), https://www.dhs.gov/news/2018/01/18/privacy-incident-involving-dhs-oig-case-management-system-update.

agency and documents were stolen.[60] As an example of the trend across the federal government, a 2015 data breach at the Office of Personnel Management (OPM) exposed social security numbers and other personal data from 21.5 million individuals.[61] Around the same time OPM reported another major data breach exposing records on about 4 million federal employees.[62] Again in 2015, approximately 390,000 tax accounts with the Internal Revenue Service were compromised, revealing SSNs, dates of birth and street addresses among other PII.[63] In September 2014, a breach at the United States Postal Service led to the loss of PII from more than 800,000 employees.[64] In sum, data breaches at federal agencies have grown exponentially more common in the last decade, from a reported 5,503 data security incidents in 2006 to 35,277 discovered in 2019.[65] In 2018 the GAO found that over 700 of its cybersecurity recommendations since 2010 had not been implemented by federal agencies.[66] Both DHS and the federal government have broad track records of failing to secure personally identifiable information, resulting in the disclosure of sensitive information on millions of individuals. CBP should not unnecessarily seek to collect sensitive personally identifiable information on exponentially more individuals when the agency cannot even protect the data it currently holds.

[60] Cybersecurity and Infrastructure Security Agency, Federal Agency Compromised by Malicious Cyber Actor, AR20-268A, Dep't. of Homeland Sec. (Sept. 24, 2020), https://us-cert.cisa.gov/ncas/analysis-reports/ar20-268a; Duncan Riley, DHS discloses data breach of US agency but doesn't name which was hacked, SiliconAngle (Sept. 24, 2020), https://siliconangle.com/2020/09/24/dhs-discloses-data-breach-us-agency-doesnt-name-hacked/.
[61] 2016 GAO Report, *supra* note 46, at 8.
[62] *Id*.
[63] *Id*. at 7-8.
[64] *Id*. at 8.
[65] U.S. Gov't Accountability Office, GAO-20-629 Cybersecurity: Clarity of Leadership Urgently Needed to Fully Implement the National Strategy (Aug. 18, 2020), https://www.gao.gov/assets/710/709555.pdf; U.S. Gov't Accountability Office, GAO-19-105 Information Security: Agencies Need to Improve Implementation of Federal Approach to Securing Systems and Protecting against Intrusions (Dec. 18, 2018), https://www.gao.gov/assets/700/696105.pdf, U.S. Gov't Accountability Office, Federal Agencies Need to Better Protect Sensitive Data 4 (Nov. 17, 2015), http://www.gao.gov/assets/680/673678.pdf.
[66] *Id*. at 2.

II. Facial recognition technology is inherently dangerous.

EPIC urges CBP to halt the use of facial recognition because this technology enables comprehensive surveillance from currently available technology. Facial recognition turns virtually every camera into a potential means of surveillance. The technology is now powerful enough to pick an individual out of a crowd, even if the individual is masked.[67] Facial recognition has already been used against protesters across the country.[68] When cell phones, door-bells, and innumerable other devices contain cameras facial recognition enables virtually unlimited surveillance. The technology upends the basic assumption that monitoring a person requires action before and during the time to be monitored. But facial recognition enables passive surveillance through video recording which can be easily searched at a later date.

Because facial recognition technology is so dangerous, individuals cannot give meaningful consent to its use, particularly in the travel and border-crossing context. As prominent privacy scholars Evan Selinger and Woodrow Hartzog argue, "consent is a broken regulatory mechanism for facial surveillance. The individual risks of facial surveillance are impossibly opaque, and our collective autonomy and obscurity interests aren't captured or served by individual decisions."[69] Facial surveillance destroys basic and timeless privacy interests including the ability to be anonymous in a crowd and the right to privacy in one's everyday movements.

[67] Chris Udemans, Facial recognition firm can ID masked faces in a crowd, Technode (Mar. 10, 2020), https://technode.com/2020/03/10/facial-recognition-firm-can-id-masked-faces-in-a-crowd/.

[68] *See e.g.* Justin Jouvenal and Spencer S. Hsu, Facial recognition used to identify Lafayette Square protester accused of assault, Washington Post (Nov. 2, 2020), https://www.washingtonpost.com/local/legal-issues/facial-recognition-protests-lafayette-square/2020/11/02/64b03286-ec86-11ea-b4bc-3a2098fc73d4_story.html; and Evan Selinger and Albert Fox Cahn, Did you protest recently? Your face might be in a database, The Guardian (Jul. 17, 2020), https://www.theguardian.com/commentisfree/2020/jul/17/protest-black-lives-matter-database.

[69] Evan Selinger and Woodrow Hartzog, The Inconsentability of Facial Surveillance, 66 Loyola L. Rev. 102 (2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3557508.

As Hartzog and Neil Richards have described for consent to be meaningful there are three basic requirements, "(1) such a request should be infrequent, (2) the harms to be weighed must be vivid, and (3) there should be incentives to take each request for consent seriously."[70] In addition, consent requires viable alternatives. Applying this model of consent to travel and border crossings reveals several fatal flaws in claiming that citizens can meaningfully consent to facial recognition.[71] The harms of facial recognition are often unclear and are not squarely presented to travelers. Inclusion in a facial recognition database could lead to surveillance by the government or to a data breach and private sector surveillance or identity theft. Even if CBP can clearly describe the harms of facial recognition and present them to travelers, the pressures of travel reduce incentives to seriously consider one's alternatives. Many individuals crossing the border have time constraints which demand their attention above privacy harms. And air travel commonly imposes time-pressure and other stressors on travelers. Individuals have every incentive not to take privacy concerns seriously when they are lined up to board a plane or have a stack of cars waiting on them to cross the border. In addition, CBP's failure to provide a clear alternatives process, one which is reliably available and takes the same time as facial recognition, renders consent to CBP's facial recognition meaningless.

III. 1:1 Facial recognition is substantially safer and more privacy protective than 1:N matching.

Not all uses of facial recognition are equally problematic. Facial recognition can be used authentication using 1:1 matching – where the system does not check every record in a database for a match, but matches the individual's face to an identifying image like a passport photo. This 1:1

[70] Neil Richards and Woodrow Hartzog, The Pathologies of Digital Consent, 96 WASH. U. L. REV. 1461, 1466 (2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3370433.

[71] Of course, non-citizens are not given even a putative choice under the proposed rule. Under CBP's regime they must submit to face surveillance or be denied entry to the country.

matching is a much more privacy protective implementation of facial recognition. 1:1 matching does not require a massive biometric database, there is no need to retain the image, and the machines conducting the 1:1 match need not be connected to the cloud. Such an implementation virtually eliminates data breach risks and the chance of mission creep.

Implementing only 1:1 facial recognition would resolve a number but not all of the concerns with CBP's Biometric Entry/Exit program. A proper 1:1 system never stores the images it compares, drastically reducing the risk of data theft or an inadvertent breach. This would go a long way to protecting privacy where CBP delegates collection of biometrics to its commercial partners. While uniformly implementing a 1:1 system would not resolve all concerns with CBP's failure to provide notice or audit, the stakes would be considerably lower.

Furthermore, a 1:1 system would eliminate the need for CBP to store facial recognition templates in the TVS system, reducing the risk to individuals if CBP or DHS are again victims of a hack. As an added benefit, 1:1 matching would greatly reduce the potential for mission creep – when an agency seeks to leverage existing tools and data for new purposes beyond the agency's original ambit or the original reason for collection. Because CBP would not have access to traveler images, the agency cannot be tempted to use those images for non-identity verification purposes. A 1:1 system would also be much easier for CBP to implement and administer as it would not require connecting CBP's TVS database to various facial recognition camera systems.

a. CBP Has Successfully Pilot Tested a 1:1 Facial Recognition System

CBP has tested 1:1 facial recognition since 2015 and currently employs the technology at the San Luis and Nogales entry points in Arizona.[72] In a final report obtained by EPIC through a FOIA

[72] 85 F.R. 74176.

request, CBP concluded that its 2015 1:1 facial recognition pilot was a “overwhelming success”.[73] However, CBP’s implementation of 1:1 facial recognition matters. If the agency retains the photos after comparison, then many of the same risks about data breach apply.

Conclusion

EPIC urges CBP to halt the collection of facial recognition images and rescind the Biometric Entry/Exit NPRM. 1:N facial recognition is inherently dangerous and cannot be the subject of meaningful consent. In the alternative, if CBP insists on using facial recognition, the agency should implement the use of 1:1 facial recognition comparison to travelers’ documents.

Respectfully Submitted,

Jeramie Scott
Jeramie Scott
EPIC Senior Counsel

Jake Wiener
Jake Wiener
EPIC Law Fellow

[73] U.S. Customs and Border Protection, 1:1 Face ePassport Air Entry Experiment Washington Dulles International Airport – Main Terminal at 21 (Oct. 2015) https://www2.epic.org/foia/dhs/cbp/biometric-entry-exit/Face-Recognition-Air-Entry-Final-Report.pdf (“In conclusion, the evaluation demonstrates that the experiment at Dulles was a success and further operational deployments are warranted.”).