epic.org

Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

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

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

TRANSPORTATION SECURITY ADMINSTRATION of the

DEPARTMENT OF HOMELAND SECURITY

Review of the 2018 Biennial National Strategy for Transportation Security (NSTS)

[Docket No. 2019-05693]

April 25, 2019

By notice published March 26, 2019, the Transportation Security Administration ("TSA") requested comments on the 2020 Biennial National Strategy for Transportation Security ("2020 Strategy").[1] TSA asked commenters to review the 2018 Strategy "base plan," "which describes the risk-based foundation of the strategy and sets forth the mission, vision, goals, priorities, and risk-based actions to reduce the vulnerabilities of nationally significant transportation assets against terrorist threats."[2] According to the agency, the 2020 Strategy is intended to "present[] a forward-looking, risk-based plan to provide for the security and freedom of movement of people and goods while preserving civil rights, civil liberties, and privacy. It identifies objectives to enhance the security of transportation infrastructure, conveyances, workers, travelers, cargo, and operations."[3]

EPIC submits these comments to TSA to 1) insist that the 2020 Strategy include a commitment to conduct a rulemaking on facial recognition; 2) urge TSA to halt further

[1] *Review of the 2018 Biennial National Strategy for Transportation Security (NSTS)*, 84 Fed. Reg. 11320, (Mar. 26, 2019), *available at* https://www.govinfo.gov/content/pkg/FR-2019-03-26/pdf/2019-05693.pdf.
[2] *Id.*
[3] 84 Fed. Reg. 11321.

deployment of facial recognition programs until meaningful consideration of public comments has taken place; and 3) call on TSA to adopt the principles contained in the Universal Guidelines for Artificial Intelligence.

As it stands, TSA plans broad expansion of facial recognition technology, despite well-documented problems with fairness and bias, and the potential for cybersecurity threats. Additionally, there is a lack of safeguards to prevent misuse of the technology. Further, TSA applies proprietary analytical tools to make secret risk determinations about travelers. The use of machine-learning algorithms, artificial intelligence, or rule-based decision tools that impact the rights of people requires the implementation of new protections. The adoption of the Universal Guidelines for Artificial Intelligence ("UGAI"), endorsed by over 300 organizations and experts, are a necessary step to provide the accountability and oversight needed for the use of advancing analytical tools.[4]

EPIC is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging privacy issues.[5] EPIC routinely comments on TSA and other Department of Homeland Security data collections and data systems.[6] EPIC successfully sued the agency for its deployment of body scanners without following the rulemaking procedures required by the Administrative Procedure Act.[7] EPIC argued that "the TSA has acted outside of its regulatory authority and with profound disregard for the statutory and constitutional rights of air travelers[,]"[8] and the D.C. Circuit agreed "TSA ha[d] not justified

[4] The Public Voice, *Universal Guidelines for Artificial Intelligence* (Oct. 23, 2018) *available at* https://thepublicvoice.org/ai-universal-guidelines/ [hereinafter UGAI].
[5] EPIC, *About EPIC* (2019), https://epic.org/epic/about.html.
[6] EPIC, Comments on Intent to Request Revision from OMB of One Current Public Collection of Information: TSA Pre-Check Application Program, Transp. Sec. Admin., U.S. Dep't of Homeland Sec., Docket No. TSA-2014-0001 (July 3, 2017), *available at* https://epic.org/apa/comments/EPIC-TSA-Pre-Check-Expansion-Comments.pdf; EPIC, Comments on TSA PreCheck Application Program System of Records and Secure Flight Records System of Records, U.S. Dep't of Homeland Sec., Docket Nos. DHS-2013-0040, DHS-2013-0041, DHS-2013-0020, (Oct. 10, 2013), *available at* https://epic.org/apa/comments/EPIC-TSAPreCheck-Comments.pdf;
[7] *Elec. Privacy Info. Ctr. v. U.S. Dep't of Homeland Sec.*, 653 F.3d 1 (D.C. Cir. 2011).
[8] Reply Brief for Petitioners at 10, *EPIC v. DHS*, 653 F.3d 1 (D.C. Cir. 2011).

its failure to issue notice and solicit comments."[9] Now, TSA makes a similar end-run in violation of the Administrative Procedure Act ("APA") to implement facial recognition technology[10] without following Congressionally mandated notice-and-comment procedures.[11]

I. TSA must halt deployment of facial recognition technology until a notice-and-comment rulemaking is complete, and the 2020 Strategy should reflect that.

TSA's 2018 Biennial Strategy referenced facial recognition to combat insider threats and identified such technology as a Research and Development priority.[12] TSA has already partnered with another Department of Homeland Security ("DHS") component, U.S. Customs and Border Protection ("CBP"), and private airlines to introduce facial recognition at airports without following notice-and-comment procedures.[13] Legislators have concerns. In September 2018, Senator Tom Udall stated, "TSA claims this technology will streamline the security process, but it is unclear how these technologies would impact efficiency and whether the software treats all travelers and Americans equally in practice."[14] And Senator Edward J. Markey stated, "I'm very disappointed that [TSA] will not commit to ensuring these fundamental protections are in place through a formal rulemaking before [the agency] move[s] forward. The American people deserve to have a set of guidelines which are put in place in order to protect their privacy."[15]

Instead of responding to this oversight hearing by suspending the practice and conducting a rulemaking, TSA immediately released a "Biometrics Roadmap," summarizing plans for

[9] *EPIC v. DHS*, 653 F.3d 1, 3.
[10] Kathryn Steele, *Delta unveils first biometric terminal in U.S. in Atlanta; next stop: Detroit*, Delta (Nov. 29, 2018), *available at* https://news.delta.com/delta-unveils-first-biometric-terminal-us-atlanta-next-stop-detroit.
[11] 5 U.S.C. § 553.
[12] Transp. Sec. Admin., 2018 Biennial National Strategy for Transportation Security, 12, 18 (Apr. 4, 2018), *available at* https://www.tsa.gov/sites/default/files/foia-readingroom/final_2018_nsts_signed.pdf.
[13] Kathryn Steele, *Delta unveils first biometric terminal in U.S. in Atlanta; next stop: Detroit*, Delta (Nov. 29, 2018), *available at* https://news.delta.com/delta-unveils-first-biometric-terminal-us-atlanta-next-stop-detroit.
[14] *TSA Oversight*, S. Comm. on Commerce, Science and Trans., 115 Cong. (2018) (statement of Sen. Tom Udall), *available at* https://www.c-span.org/video/?c4747316/facial-recognition-tsa&start=2166.
[15] *TSA Oversight*, S. Comm. on Commerce, Science and Trans., 115 Cong. (2018) (statement of Sen. Edward J. Markey), *available at* https://www.c-span.org/video/?c4747316/facial-recognition-tsa&start=2166.

further deployment.[16] Despite publishing lofty goals to rapidly expand the program, TSA has yet to issue a notice of proposed rulemaking in the federal register and request public comment.

a. TSA plans broad expansion of the program.

TSA intends to join with CBP on biometric programs for international travelers.[17] TSA and CBP plan to continue to test programs and work with one another and airline companies to develop their biometric technology.[18] TSA and CBP plan to integrate biometric information with the Homeland Advanced Recognition Technology ("HART").[19] Further, the agencies intend to work with the Office of Biometrics and Identity Management ("OBIM"), which is a component of DHS that enables "biometric matching, storing, sharing, and analysis."[20] TSA plans to join with CBP to expand the use of facial recognition despite CBP's failure to conduct a notice-and-comment rulemaking on its deployment of facial recognition.

TSA plans to use biometric technology for TSA Pre-check travelers and collect fingerprints from applicants to perform background checks.[21] TSA also plans to require facial images for Pre-check applications, and to supplement data of already-enrolled members, it will "leverag[e] similar systems" from other agencies and components, such as the State Department and CBP.[22] TSA intends to "integrate" this biometric data with IDENT and HART.[23]

TSA plans to use biometrics for "additional domestic travelers" beyond those travelers who sign up for Pre-check and expand the agency's the use of facial recognition to domestic travelers for whom they do not have access to biometric data currently.[24] TSA intends to use data

[16] Transp. Sec. Admin., *TSA Biometrics Roadmap*, (Sept. 2018), *available at* https://www.tsa.gov/sites/default/files/tsa_biometrics_roadmap.pdf [hereinafter TSA Roadmap].
[17] *Id.* at 10.
[18] *Id.* at 11.
[19] *Id.*
[20] *Id.*
[21] *Id.* at 12.
[22] *Id.* at 13.
[23] *Id.*
[24] *Id.* at 15.

stored in other DHS systems, like IDENT and HART, as well as State Department passport photos, and "solutions that may broker verification touchpoints between federal and state systems."[25] They will work with "industry and interagency partners" as well as airlines and airports, and "other stakeholders."[26]

TSA plans to develop infrastructure for biometrics and expand the use of facial recognition broadly, stating in the Roadmap:

> TSA will identify pathways to appropriately leverage existing capabilities and services across TSA, DHS, other Federal agencies, and third parties to accommodate a variety of front-end concepts and solutions. Likewise, TSA will pursue a system architecture that promotes data sharing to maximize biometric adoption throughout the passenger base and across the aviation security touchpoints of the passenger experience.[27]

b. TSA's expansion of facial recognition use ignores major problems with the technology.

TSA exposes travelers' immutable biometric information to cybersecurity threats. To understand the risks of hacking, consider the largest biometric ID system in the world: India's Aadhaar system.[28] This database has been hacked multiple times.[29] In January 2018, the hacked personal data of more than 1 billion individuals was for sale on WhatsApp for less than ten dollars.[30] Before that, "as many as 600,000 children had their data leaked" by an Indian government website.[31]

TSA's program also creates facial morphing risks, where multiple face images are combined to create one image. The National Institute of Standards and Technology tests vendors of face recognition software, and said, "Facial morphing (and the ability to detect it) is an area of high interest to a number of photo-credential issuance agencies and those employing face

---

[25] *Id.*
[26] *Id.*
[27] *Id.*
[28] Ashish Malhotra, *The World's Largest Biometric ID System Keeps Getting Hacked*, Motherboard, Jan. 8, 2018, https://motherboard.vice.com/en_us/article/43q4jp/aadhaar-hack-insecure-biometric-id-system.
[29] *Id.*
[30] *Id.*
[31] *Id.*

recognition for identity verification."[32] And, "security vendors warn, this practice of face-swapping could morph into a monster with chilling implications for the cybersecurity world."[33]

Beyond cybersecurity risks, there is the problem of bias. Face recognition algorithms fail often and in unfair ways. In September 2018, the DHS Office of Inspector General raised the concern that "CBP could not consistently match individuals of certain age groups or nationalities" and the 2017 match rate was a "low 85-percent[.]"[34] Recent research shows "substantial disparities" in facial analysis algorithm accuracy along gender and racial lines.[35] Discrimination through automation should not be tolerated, and when it is undertaken by a federal agency it simply cannot be tolerated.

c. The use of facial recognition completely lacks the safeguards necessary to even consider its implementation.

DHS has ignored the existing federal regulation and legislation preventing DHS from using facial recognition technology it develops, the photos it has captured, and the databases it creates as part of this program for other purposes.[36] In fact, the TSA Biometrics Roadmap, specifically states that it will transfer biometric information to other DHS entities and the State Department.[37] CBP already pulls photos from the State Department's Consular Consolidated

[32] U.S. Dep't of Commerce, Nat. Inst. of Standards and Technology, Performance of Automated Facial Morph Detection and Morph Resistant Face Recognition Algorithms Concept, Evaluation Plan and API, VERSION 1.1, 4 (Sept. 6, 2018), https://www.nist.gov/sites/default/files/documents/2018/09/07/frvt_morph_api_v1.1.pdf.
[33] Fergus Halliday, *Deepfakes are just the beginning for cybersecurity's Faceswap nightmare*, PC World, Apr. 4, 2018, https://www.pcworld.idg.com.au/article/634156/deepfakes-just-beginning-cybersecurity-faceswap-nightmare.
[34] OIG Report, *supra* note 2, DHS OIG HIGHLIGHTS.
[35] Joy Buolamwini and Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, Proceedings of Machine Learning Research 81:1–15, 2018, 2 http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.
[36] Letter from Sens. Edward J. Markey and Mike Lee to Sec'y Kirstjen Nielsen, Dep't of Homeland Sec., 1-2 (Dec. 21, 2017) *available at* https://www.markey.senate.gov/imo/media/doc/DHS%20Biometrics%20Markey%20Lee%20.pdf.
[37] TSA Roadmap, *supra* note 16, 15.

Database to use for purposes unrelated to those specified at collection,[38] without legal authority and in violation of the Privacy Act.[39]

Facial recognition is the biometric identifier most easily used for mass surveillance; indeed, as the DHS Data Privacy and Integrity Advisory Committee's 2019 report notes, "facial recognition systems can be used to identify people in photos, videos, or in real-time."[40] Facial recognition software paired with cameras aimed toward public spaces in China is used to monitor and shame individuals as part of a campaign for social control through mass surveillance.[41] The U.S. government's slide toward these techniques runs directly against American values.

The Secret Service has already begun use of facial recognition technology to monitor parts of the White House and surrounding area, including "an open setting, where individuals are free to approach from any angle."[42] The PIA for this program states, "individuals who do not wish to be captured by White House Complex CCTV and cameras involved in this pilot may choose to avoid the area."[43] That is, of course, absurd as few people will even be aware they are subject to facial recognition. The use of facial recognition technology at a site where hundreds of demonstrations, vigils, protests, and marches occur annually[44] also raised particular alarm for the protection of the First Amendment. As we warned the DC City Council in 2008:

---

[38] U.S. Dep't of Homeland Sec., Office of Inspector Gen., OIG-18-80, Progress Made, but CBP Faces Challenges Implementing a Biometric Capability to Track Air Passenger Departures Nationwide, 7 (Sept. 21, 2018), https://www.oig.dhs.gov/sites/default/files/assets/2018-09/OIG-18-80-Sep18.pdf.
[39] 5 U.S.C. § 552a(b).
[40] Data Privacy and Integrity Advisory Comm., U.S. Dep't of Homeland Sec., Report 2019-01 of the DHS Data Privacy and Integrity Advisory Committee: Privacy Recommendations in Connection with the Use of Facial Recognition Technology, 2 (Feb. 26, 2019), *available at* https://www.dhs.gov/sites/default/files/publications/Report%202019-01_Use%20of%20Facial%20Recognition%20Technology_02%2026%202019.pdf.
[41] Simon Denyer, *China's Watchful Eye*, Wash. Post, Jan. 7, 2018, https://www.washingtonpost.com/news/world/wp/2018/01/07/feature/in-china-facial-recognition-is-sharp-end-of-a-drive-for-total-surveillance/; Paul Mozur, *Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras*, N.Y. Times, July 8, 2018, https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html.
[42] DHS, Privacy Impact Assessment for the Facial Recognition Pilot, DHS/USSS/PIA-024, 2 (Nov. 26, 2018) https://www.dhs.gov/sites/default/files/publications/privacy-pia-usss-frp-november2018.pdf.
[43] *Id.* at 4.
[44] White House Historical Association, President's Park: A History of Protest at the White House, https://www.whitehousehistory.org/presidents-park-a-history-of-protest-at-the-white-house

> There is also a rapid evolution underway that makes surveillance far more intrusive than most people understand. Already you are seeing the use of facial recognition that will make it possible to identify people in public places. People enjoy privacy in public spaces because of anonymity. These new techniques are intended precisely to destroy that very real form of privacy.[45]

TSA must immediately suspend implementation of this program until Congressional legislation sets out clear limitations. Once federal safeguards are established, any implementation of facial recognition by DHS that impacts many people, including TSA's facial recognition program, should require a notice-and-comment rulemaking.

II. TSA use of secret algorithms to make screening decisions necessitates the need for guidelines

TSA's 2020 Strategy should include a commitment to the principles, rights, and obligations contained in the Universal Guidelines for Artificial Intelligence. TSA uses machine learning and algorithms to make decisions that impact individuals and should be governed by clear policy rules set out in agency regulations. There are several guidelines in the UGAI that are particularly applicable to TSA's Secure Flight and its components. Secure Flight checks against watch lists of known or suspected terrorists[46] and also uses CBP's Automated Targeting System "to identify individuals for enhanced screening during air travel through use of rules based on current intelligence as part of its Secure Flight vetting process."[47] The Quiet Skies program, a subset of Secure Flight, uses "rules to identify passengers for enhanced screening on some subsequent domestic and outbound international flights."[48]

TSA describes two subsets of Secure Flight:

> Silent Partner rules are based on a specific potential threat to aviation security or the United States, as assessed by TSA, with respect to international travel to the

[45] Marc Rotenberg, Testimony to Comm. On Public Safety and the Judiciary of the D.C. Council on "Video Interoperability for Public Safety," 2 (June 2, 2008) *https://epic.org/privacy/surveillance/dccouncil_cctv060208.pdf*]
[46] Transp. Sec. Admin, U.S. Dep't of Homeland Sec., DHS/TSA/PIA-018(h), *Privacy Impact Assessment Update for Secure Flight*, 1 (July 12, 2017).
[47] Transp. Sec. Admin, U.S. Dep't of Homeland Sec., DHS/TSA/PIA-018(i), *Privacy Impact Assessment Update for Secure Flight Silent Partner and Quiet Skies*, 1 (Apr. 19, 2019).
[48] *Id.*

> United States. Once identified by the rule, those passengers are placed on a Silent Partner List that is retained for the period of the international in-bound flight.
>
> Quiet Skies rules are a subset of the Silent Partner rules that are aligned to potential aviation security threats within the United States. TSA uses Quiet Skies rules to create a temporary Quiet Skies List to designate passengers who fall within the Quiet Skies subset of rules for enhanced screening on some subsequent domestic and outbound international travel. Individuals will remain on the Quiet Skies List for a period of time.[49]

These lists are updated daily as individuals are added and deleted, and individuals flagged by the system may be "identified for enhanced screening and may result in other operational response including observation by the TSA Federal Air Marshal Service (FAMS) while the individual is onboard the flight or in the airport."[50]

TSA uses artificial intelligence techniques to determine which individuals should be flagged for additional surveillance: "The rules are based on aggregated travel data, intelligence, and trend analysis of the intelligence and suspicious activity."[51]

Since the Secure Flight program "leverages" CBP's Automated Targeting System, it amplifies the impact of that system on individuals. CBP's Automated Targeting System ("ATS") "compares traveler, cargo, and conveyance information against law enforcement, intelligence, and other enforcement data using risk-based scenarios and assessments."[52] ATS creates rules by comparing information about "cargo entering and exiting the country with patterns identified as requiring additional scrutiny. The patterns are based on CBP Officer experience, trend analysis of suspicious activity, law enforcement cases, and raw intelligence."[53] ATS may flag a person, shipment, or conveyance even without any association with a previous law enforcement action or

---

[49] *Id.* at 2.
[50] *Id.* at 3.
[51] *Id.*
[52] U.S. Customs and Border Prot., U.S. Dep't of Homeland Sec., DHS/CBP/PIA-006(e), Privacy Impact Assessment Update for the Automated Targeting System, 1 (Jan. 13, 2017), available at https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp006-ats-december2018.pdf [hereinafter ATS PIA].
[53] *Id.* at 1.

other note of law enforcement concern, using "predictive analytics".[54] "ATS uses data from many different source systems. In some instances ATS is the official record for the information, while in other instances ATS ingests and maintains the information as a copy or provides a pointer to the information in the underlying system."[55] ATS pulls information from at least 25 government databases, as well as from commercial data aggregators and other manually processed data.[56] Many of these databases contain personally identifiable information.[57]

ATS makes determinations about individuals and cargo by:

> standardiz[ing] names, addresses, conveyance names, and similar data so these data elements can be more easily associated with other business data and personal information to form a more complete picture of a traveler, import, or export in context with previous behavior of the parties involved. Traveler, conveyance, and shipment data are processed through ATS and are subject to a real-time, rules-based evaluation.[58]

The system uses "data mining, machine learning, and other analytic techniques to enhance [its cargo screening modules]."[59]

Because PII is used by ATS and Secure Flight to make decisions that impact individuals, it is imperative that the methods—now mostly secret—and factors used in making targeting assessments are made public, and that the system is governed by ethics and accountability. The 2020 Strategy should reflect these obligations.

a. Right to Transparency and the Assessment and Accountability Obligation

The principle of transparency is found in various modern privacy laws including the US Privacy Act, the EU Data Protection Directive, the GDPR, and the Council of Europe Convention 108. The aim of transparency is to "enable independent accountability for automated

[54] ATS PIA, *supra* note 49, 4; U.S. Dep't of Homeland Sec., *2017 DHS Data Mining Report to Congress*, 10 (Oct. 2018), available at https://www.dhs.gov/sites/default/files/publications/2017-dataminingreport_0.pdf [hereinafter Data Mining Report].
[55] ATS PIA, *supra* note 49, 2.
[56] *Id.* at 82-83.
[57] *Id.*
[58] Data Mining Report, *supra* note 51, 13.
[59] *Id.* at 16.

decisions."[60] This principle translates into an affirmative right of individuals, "to know the basis of an AI decision that concerns them[,]" including "access to the factors, the logic, and techniques that produced the outcome."[61] Individuals should not be left in the dark about analytical systems making decisions that affect them.

Further, TSA should implement an assessment and accountability mechanism. The UGAI states that "An AI system should be deployed only after an adequate evaluation of its purpose and objectives, its benefits, as well as its risks. Institutions must be responsible for decisions made by an AI system."[62] There is no indication that a full assessment and proper accountability mechanisms are in place for the various systems that will make up the passenger screening process, particularly for Secure Flight.

EPIC urges TSA to create and publish "Algorithmic Assessments" similar to the Privacy Impact Assessments conducted by federal agencies pursuant to Section 208 of the E-Government Act of 2002. These assessments would force the agency to determine the risks of an AI system prior to deployment. The assessments would also allow individuals to understand the methods and factors used in decisions that have an impact on their lives.

b. Fairness Obligation and Right to Human Determination

As the Universal Guidelines state, "Institutions must ensure that AI systems do not reflect unfair bias or make impermissible discriminatory decisions." This fairness obligation is particularly important to ensure that TSA systems are not used to make decisions that will adversely affect particular groups for illegitimate reasons. It is important to remember that

[60] The Public Voice, *Universal Guidelines for Artificial Intelligence Explanatory Memorandum and References* (Oct. 2018), available at https://thepublicvoice.org/ai-universal-guidelines/memo/ [hereinafter UGAI Explanatory Memo].
[61] UGAI, *supra* note 4,1.
[62] *Id.* at 5.

seemingly neutral factors and rules could lead to impermissible discriminatory results.[63] As such, even in the customs context, it is important to ensure that proper care is taken to ensure fairness.

This is particularly true for TSA, since it uses CBP's Automated Targeting System, which contains "information that could directly indicate the racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health or sex life" of individuals.[64] It is unclear how this data relates to screening for terrorist threats, and even if it did, the potential for abuse and unfair results is strong. The utility of big data is alluring, but it is important to avoid perpetuating unfair bias or discrimination by way of automation.

The right to meaningful human intervention is helpful to ensure algorithmic discrimination does not take place. Human decisionmaking "reaffirms that individuals and not machines are responsible for automated decision-making."[65] With better accountability for the results of such systems, there is less of a chance of unfair results.

c. Accuracy, Reliability, and Validity Obligations and Data Quality Obligation

The obligations of accuracy, reliability, validity, and data quality are important principles in any system, especially in one that subjects individuals to invasive screening and surveillance. Therefore, TSA must verify the information used in the agency's systems and should frequently audit such systems.

III. Conclusion

The 2020 Strategy should reflect the legal obligation TSA has to conduct a notice-and-comment rulemaking *before* deploying facial recognition technology, and the program should be

[63] Joi Ito, *Supposedly 'Fair' Algorithms Can Perpetuate Discrimination*, Wired (Feb. 5, 2019), https://www.wired.com/story/ideas-joi-ito-insurance-algorithms/.
[64] EPIC, Comments on the Automated Targeting System Notice of Privacy Act System of Records and Proposed Rule: Privacy Act of 1974 Exemptions, U.S Customs and Border Protection, U.S. Dep't of Homeland Sec., Docket Nos. 2012-0019; 2012-0020, 1 (June 21, 2012), available at https://epic.org/privacy/travel/ats/EPIC-ATS-Comments-2012.pdf.
[65] UGAI Explanatory Memo, *supra* note 57.

suspended until such procedures take place. This is imperative, given the potential for hacking, discriminatory impact, and broader government misuse. TSA should also adopt Universal Guidelines for Artificial Intelligence. In particular, the agency should produce and publish "Algorithmic Assessments" to ensure transparency and accountability, ensure that the systems are not impermissibly discriminatory, and vigilantly audit data quality.

Respectfully submitted,

/s/ Marc Rotenberg
Marc Rotenberg
EPIC President and Executive Director

/s/ Jeramie D. Scott
Jeramie D. Scott
EPIC Senior Counsel

/s/ Ellen Coogan
Ellen Coogan
EPIC Domestic Surveillance Fellow