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

February 5, 2020

The Honorable Bennie Thompson, Chairman
The Honorable Mike Rogers, Ranking Member
Committee on Homeland Security
U.S. House of Representatives
H2-176 Ford House Office Building
Washington, D.C. 20515

Dear Chairman Thompson and Ranking Member Rogers:

We write to you in advance of the hearing on "About Face: Examining the Department of Homeland Security's Use of Facial Recognition and Other Biometric Technologies, Part II."[1] EPIC supports a moratorium on facial recognition technology for mass surveillance. This Committee should halt DHS's use of face surveillance technology.

The Electronic Privacy Information Center ("EPIC") is a public interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues.[2] EPIC is focused on protecting individual privacy rights, and we are particularly interested in the privacy problems associated with surveillance.[3] Last year, EPIC filed a lawsuit against the Customs and Border Protection ("CBP") agency for failure to establish necessary privacy safeguards for the collection of facial images at US borders.[4]

A Call to Ban Face Surveillance

EPIC and the Public Voice Coalition are leading a global campaign to establish a moratorium on "face surveillance," the use of facial recognition for mass surveillance.[5] In October 2019 more than 100 NGO's and hundreds of experts endorsed our petition.[6] The signatories stated:

- We urge countries to suspend the further deployment of facial recognition technology for mass surveillance;

[1] *About Face: Examining the Department of Homeland Security's Use of Facial Recognition and Other Biometric Technologies, Part II*, House Comm. on Homeland Security, 116th Cong. (Feb. 6, 2020), https://homeland.house.gov/activities/hearings/about-face-examining-the-department-of-homeland-securitys-use-of-facial-recognition-and-other-biometric-technologies-part-ii.
[2] *See About EPIC*, EPIC.org, https://epic.org/epic/about.html.
[3] EPIC, *EPIC Domestic Surveillance Project,* https://epic.org/privacy/surveillance/.
[4] *EPIC v. U.S. Customs and Border Protection*, No. 19-cv-689 (D.D.C. filed Mar. 12, 2019); *See* https://epic.org/foia/dhs/cbp/alt-screening-procedures/
[5] EPIC, *Ban Face Surveillance,* https://epic.org/banfacesurveillance/.
[6] The Public Voice, *Declaration: A Moratorium on Facial Recognition Technology for Mass Surveillance Endorsements*, https://thepublicvoice.org/ban-facial-recognition/endorsement/.

- We urge countries to review all facial recognition systems to determine whether personal data was obtained lawfully and to destroy data that was obtained unlawfully;

- We urge countries to undertake research to assess bias, privacy and data protection, risk, and cyber vulnerability, as well as the ethical, legal, and social implications associated with the deployment of facial recognition technologies; and

- We urge countries to establish the legal rules, technical standards, and ethical guidelines necessary to safeguard fundamental rights and comply with legal obligations before further deployment of this technology occurs.

Courts and regulators are also listening. There is growing awareness of the need to bring this technology to a halt. The state of California prohibited the use facial recognition on police-worn body cameras. Several cities in the U.S. have banned the use of facial recognition systems, and there is a growing protest around the world. For example, In 2019 the Swedish Data Protection Authority prohibited the use of facial recognition in schools. EPIC has published a resource of laws, regulations, legal decisions and reports on face surveillance worldwide at https://epic.org/banfacesurveillance/.

Threats to Privacy and Civil Liberties

Facial recognition poses serious threats to privacy and civil liberties and can be deployed covertly, remotely, and on a mass scale. There is a lack of well-defined regulations controlling the collection, use, dissemination, and retention of biometric identifiers. Ubiquitous identification by commercial or government entities eliminates the individual's ability to control the disclosure of their identities, creates new opportunities for tracking and monitoring, increases the security risks from data breaches. An individual's ability to control disclosure of his or her identity is an essential aspect of personal freedom and autonomy. The use of facial recognition erodes these freedoms.

There is little a person in the United States could do to prevent the capture of their image by the government or a private company if face surveillance is deployed. Participation in society necessarily requires participation in public spaces. But ubiquitous and near effortless identification eliminates the individual's ability to control the disclosure of their identities to others. Strangers will know our identities as readily as our friends and family members.

Use of Face Surveillance in China

Face surveillance capabilities have been on full display in China. China is not only the leading government for face surveillance technology, it is also the leading exporter of the technology.[7] The Chinese government has implemented a massive facial recognition surveillance system.[8] China has leveraged its surveillance network to implement an "advanced facial recognition

[7] Steven Feldstein, *The Global Expansion of AI Surveillance* 13-15 (Sept. 2019), https://carnegieendowment.org/files/WP-Feldstein-AISurveillance_final1.pdf.
[8] 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/.

technology to track and control the Uighurs, a largely Muslim minority."[9] And China continues to expand the use of facial recognition technology. A university in China is testing the use of facial recognition to monitor whether students attend classes and to track their attention during lectures.[10] To register a new mobile phone number in China now requires one to submit to a facial scan.[11] Trials have also begun to use facial recognition at security checkpoints in the subway system.[12]

In Hong Kong, where protests have been ongoing since March, face scans have become a weapon. Protesters fear that facial recognition technology is being used to identify and track them.[13] In response to this fear, protesters have resorted to covering their faces and have taken down facial recognition cameras. Hong Kong reacted by banning masks and face paint.[14] Many of the demonstrators worry that the mass surveillance implemented on the mainland of China will be implemented in Hong Kong.

Face Surveillance in the United States

The implementation of facial recognition technology by government and commercial actors in the United States is pushing the U.S. towards a similar mass surveillance infrastructure. Already some schools are implementing the use of facial recognition technology.[15] Customs and Border Protection (CBP) is using facial recognition on travelers entering and exiting the U.S.[16] And airlines are using CBP's facial recognition system to conduct flight check-ins, check bags, and board flights.[17] The Rochester airport has implemented the surveillance infrastructure to perform facial recognition on every person that enters the airport.[18] Amazon drafted plans to use their Ring

[9] Paul Mozur, *One Month, 500,000 Face Scans: How China is Using A.I. to Profile a Minority*, N.Y. Times (Apr. 14, 2019), https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html.
[10] Brendan Cole, *Chinese University Tests Facial Recognition System to Monitor Attendance and Students' Attention to Lectures*, Newsweek (Sept. 2, 2019), https://www.newsweek.com/nanjing-china-facial-recognition-1457193.
[11] Kyle Wiggers, *AI Weekly: In China, You Can No Longer Buy a Smartphone without a Face Scan*, VentureBeat (Oct. 11, 2019), https://venturebeat.com/2019/10/11/ai-weekly-in-china-you-can-no-longer-buy-a-smartphone-without-a-face-scan/.
[12] Wan Lin, *Beijing Subway Station Trials Facial Recognition*, Global Times (Dec. 1, 2019), http://www.globaltimes.cn/content/1171888.shtml.
[13] Paul Mozur, *In Hong Kong Protests, Faces Become Weapons*, N.Y. Times (July 26, 2019), https://www.nytimes.com/2019/07/26/technology/hong-kong-protests-facial-recognition-surveillance.html.
[14] Matt Novak, *Hong Kong Announces Ban on Masks and Face Paint That Helps Protesters Evade Facial Recognition*, Gizmodo (Oct. 4, 2019), https://gizmodo.com/hong-kong-announces-ban-on-masks-and-face-paint-that-he-1838765030.
[15] Tom Simonite and Gregory Barber, *The Delicate Ethics of Using Facial Recognition in Schools*, Wired (Oct. 17, 2019), https://www.wired.com/story/delicate-ethics-facial-recognition-schools/.
[16] Davey Alba, *The US Government Will Be Scanning Your Face At 20 Top Airports, Documents Show*, BuzzFeed (Mar. 11, 2019), https://www.buzzfeednews.com/article/daveyalba/these-documents-reveal-the-governments-detailed-plan-for?ref=bfnsplash.
[17] *See, e.g.*, Kathryn Steele, *Delta Unveils First Biometric Terminal in U.S. in Atlanta; next stop: Detroit*, Delta News Hub, https://news.delta.com/delta-unveils-first-biometric-terminal-us-atlanta-next-stop-detroit.
[18] James Gilbert, *Facial Recognition Heading to Rochester Airport Despite Concerns*, Rochester First (June 26, 2019), https://www.rochesterfirst.com/news/local-news/facial-recognition-heading-to-airport-despite-concerns/.

surveillance cameras to create neighborhood watch lists that leverage facial recognition.[19] Retailers have implemented the use facial recognition at their stores.[20] A landlord in Brooklyn wanted to use facial recognition as the means to gain entry into a rent-stabilized apartment building.[21] Facial recognition is being used at major sporting events[22] and concerts.[23] And the companies that are creating the facial recognition algorithms are often using—without consent—millions of photos scraped from social media sites and other webpages in order train the algorithms.[24]

It is important to note that not all uses of facial recognition are equally problematic. For instance, where the user has control and there is no government mandate, such as using Face ID for iPhone authentication, the same privacy issues do not arise. Facial recognition can also be used for verification or authentication using 1:1 matching – that is, where the system does not check every record in a database for a match, but matches the individual's face to their claimed identity.[25] This 1:1 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 do not need to be connected to the cloud. Such an implementation virtually eliminates data breach risks and the chance of mission creep.

Face Surveillance in Airports

Recently, new privacy risks have arisen with the deployment of facial recognition technology at U.S. airports following a 2017 Executive Order to "expedite the completion and implementation of biometric entry exit tracking system."[26] Customs and Border Protection ("CBP") has now implemented the Biometric Entry-Exit program for international travelers at 17 airports.[27] TSA is

[19] Sam Biddle, *Amazon's Ring Planned Neighborhood "Watch Lists" Built on Facial Recognition*, The Intercept (Nov. 26, 2019), https://theintercept.com/2019/11/26/amazon-ring-home-security-facial-recognition/.
[20] Nick Tabor, *Smile! The Secretive Business of Facial-Recognition Software in Retails\ Stores*, New York Intelligencer (Oct. 20, 2018), http://nymag.com/intelligencer/2018/10/retailers-are-using-facial-recognition-technology-too.html.
[21] Gina Bellafante, *The Landlord Wants Facial Recognition in Its Rent-Stabilized Buildings. Why?*, N.Y. Times (Mar. 28, 2019), https://www.nytimes.com/2019/03/28/nyregion/rent-stabilized-buildings-facial-recognition.html.
[22] Ryan Rodenberg, *Sports Betting and Big Brother: Rise of Facial Recognition Cameras*, ESPN (Oct. 3, 2018), https://www.espn.com/chalk/story/_/id/24884024/why-use-facial-recognition-cameras-sporting-events-the-rise.
[23] Steve Knopper, *Why Taylor Swift Is Using Facial Recognition at Concerts*, Rolling Stone (Dec. 13, 2018), https://www.rollingstone.com/music/music-news/taylor-swift-facial-recognition-concerts-768741/.
[24] Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, N.Y. Times (Jan. 18, 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.
[25] Lucas D. Introna and Helen Nissenbaum, *Facial Recognition Technology: A Survey of Policy and Implementation Issues*, Ctr. for Catastrophe Preparedness & Response, N.Y. Univ., 11 (2009), *available at* https://nissenbaum.tech.cornell.edu/papers/facial_recognition_report.pdf.
[26] Exec. Order No. 13,780 § 8.
[27] Davey Alba, *The US Government Will Be Scanning Your Face At 20 Top Airports, Documents Show* (Mar. 11, 2019), https://www.buzzfeednews.com/article/daveyalba/these-documents-reveal-the-governments-detailed-plan-for.

quickly moving to leverage CBP's Biometric Entry-Exit program to expand the use of facial recognition at airports.[28]

TSA has already deployed facial recognition technology at two TSA Checkpoints.[29] In September 2018, TSA released a "TSA Biometrics Roadmap," detailing its plans to use facial recognition, including on domestic travelers.[30] The Roadmap makes clears TSA's intention to leverage CBP's facial recognition capabilities implemented as part of the Biometric Entry-Exit Program. But corresponding privacy safeguards have not yet been established.

In response to EPIC's Freedom of Information Act request, CBP recently released 346 pages of documents detailing the agency's scramble to implement the flawed Biometric Entry-Exit system, a system that employs facial recognition technology on travelers entering and exiting the country. The documents obtained by EPIC describe the administration's plan to extend the faulty pilot program to major U.S. airports. The documents obtained by EPIC were covered in-depth by Buzzfeed.[31]

Based on the documents obtained, EPIC determined that there are few limits on how airlines will use the facial recognition data collected at airports.[32] Only recently has CBP changed course and indicated that the agency will require airlines to delete the photos they take for the Biometric Entry-Exit program.[33] No such commitment has been made by TSA. Indeed, TSA's Roadmap indicates that the agency wants to expand the dissemination of biometric data as much as possible, stating:

> 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.[34]

TSA seeks to broadly implement facial recognition through "public-private partnerships" in an effort to create a "biometrically-enabled curb-to-gate passenger experience."[35] Currently, TSA plans to implement an opt-in model of facial recognition use for domestic travelers but there are no

---

[28] TSA, *TSA Biometrics Roadmap* (Sept. 2018), https://www.tsa.gov/sites/default/files/tsa_biometrics_roadmap.pdf.
[29] Trans. Security Admin., *Travel Document Checker Automation Using Facial Recognition,* (Aug. 2019), https://www.dhs.gov/publication/dhstsapia-046-travel-document-checker-automation-using-facial-recognition; U.S. Customs and Border Protection, *CBP Deploys Facial Recognition Biometric Technology at 1 TSA Checkpoint at JFK Airport* (Oct. 11, 2017), https://www.cbp.gov/newsroom/national-media-release/cbp-deploys-facial-recognition-biometric-technology-1-tsa-checkpoint.
[30] TSA, *TSA Biometrics Roadmap* (Sept. 2018), https://www.tsa.gov/sites/default/files/tsa_biometrics_roadmap.pdf.
[31] Davey Alba, *The US Government Will Be Scanning Your Face At 20 Top Airports, Documents Show* (Mar. 11, 2019), https://www.buzzfeednews.com/article/daveyalba/these-documents-reveal-the-governments-detailed-plan-for.
[32] *See* CBP Memorandum of Understanding Regarding Biometric Pilot Project, https://epic.org/foia/dhs/cbp/biometric-entry-exit/MOU-Biometric-Pilot-Project.pdf.
[33] Ashley Ortiz, CBP Program and Management Analyst, Presentation before the Data Privacy & Integrity Advisory Committee, slide 23 (Dec. 2018), https://www.dhs.gov/sites/default/files/publications/SLIDES-DPIAC-Public%20Meeting%2012%2010-2018.pdf.
[34] TSA, *TSA Biometrics Roadmap*, 17 (Sept. 2018).
[35] *Id.* at 19.

guarantees that in the future TSA will not require passengers to participate in facial recognition or make the alternative so cumbersome as to essentially require passengers to opt-in.

Preserving the ability of U.S. citizens to forgo facial recognition for alternative processes is one of the privacy issues with CBP's Biometric Entry-Exit program. Senator Markey (D-MA) and Senator Lee (R-UT) called for the CBP to suspend facial recognition at the border to ensure that travelers are able to opt-out of facial recognition if they wish.[36]

In fact, EPIC recently sued CBP for all records related to the creation and modification of alternative screening procedures for the Biometric Entry-Exit program.[37] The alternative screening procedure for U.S. travelers that opt-out of facial recognition should be a manual check of the traveler's identification documents. CBP, however, has provided vague and inconsistent descriptions of alternative screening procedures in both its "Biometric Exit Frequently Asked Questions (FAQ)" webpage[38] and the agency's privacy impact assessments.[39] The creation and modification of CBP's alternative screening procedures underscores CBP's unchecked ability to modify alternative screening procedures while travelers remain in the dark about how to protect their biometric data.

Face Surveillance and AI

It is also becoming increasingly clear that AI tools are being deployed with facial recognition to accelerate the deployment of technology not only for identification but also for scoring. As we explained recently in the New York Times, "The United States must work with other democratic countries to establish red lines for certain AI applications and ensure fairness, accountability, and transparency as AI systems are deployed."[40] In a subsequent letter to the New York Times, we

---

[36] Press Release, Sens. Edward Markey and Mike Lee, *Senators Markey and Lee Call for Transparency on DHS Use of Facial Recognition Technology* (Mar. 12, 2019), https://www.markey.senate.gov/news/press-releases/senators-markey-and-lee-call-for-transparency-on-dhs-use-of-facial-recognition-technology.

[37] *EPIC v. CBP*, 19-cv-00689, *Complaint*, https://epic.org/foia/cbp/alternative-screening-procedures/1-Complaint.pdf.

[38] CBP, *Biometric Exit Frequently Asked Questions (FAQs)*, https://www.cbp.gov/travel/biometrics/biometric-exit-faqs.

[39] U.S. Dep't of Homeland Sec., DHS/CBP/PIA-030(b), *Privacy Impact Assessment Update for the Traveler Verification Service (TVS): Partner Process* 8 (2017), https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp030-tvs-may2017.pdf; *see also* U.S. Dep't of Homeland Sec., DHS/CBP/PIA-030(c), *Privacy Impact Assessment Update for the Traveler Verification Service (TVS): Partner Process* 5–6 (2017), https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp030-tvs-appendixb-july2018.pdf; U.S. Dep't of Homeland Sec., DHS/CBP/PIA-056, *Privacy Impact Assessment for the Traveler Verification Service* 2 (2018), https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp030- tvs-november2018_2.pdf.

[40] Marc Rotenberg, *The Battle Over Artificial Intelligence*, N.Y. Times, Apr. 18, 2019, https://www.nytimes.com/2019/04/18/opinion/letters/artificial-intelligence.html. (In the introduction to the *EPIC AI Policy Sourceboook* and in a subsequent letter to the New York Times, we warned of the growing risk of the Chinese AI model. Marc Rotenberg and Len Kennedy, *Surveillance in China: Implications for Americans,* N.Y. Times, Dec. 19, 2019, https://www.nytimes.com/2019/12/19/opinion/letters/surveillance-china.html.

warned of the growing risk of the Chinese AI model, and specifically explained, "China also dominates the standards-setting process for techniques like facial recognition."[41]

Society is simply not in a place right now for the wide-scale deployment of facial recognition technology. It would be a mistake to deploy facial recognition at this time. We urge the Committee to support a ban of DHS's further deployment of face surveillance technology.

We ask that this statement be entered in the hearing record. EPIC looks forward to working with the Committee on these issues of vital importance to the American public.

Sincerely,

/s/ *Marc Rotenberg*
Marc Rotenberg
EPIC President

/s/ *Caitriona Fitzgerald*
Caitriona Fitzgerald
EPIC Policy Director

/s/ *Jeramie Scott*
Jeramie Scott
EPIC Senior Counsel

Attachment

Declaration: A Moratorium on Facial Recognition Technology for Mass Surveillance
The Public Voice, Tirana Albania (October 2019)

[41] Marc Rotenberg and Len Kennedy, *Surveillance in China: Implications for Americans,* N.Y. Times, Dec. 19, 2019, https://www.nytimes.com/2019/12/19/opinion/letters/surveillance-china.html.

Declaration: A Moratorium on Facial Recognition Technology for Mass Surveillance

October 2019
Tirana, Albania

We the undersigned call for a moratorium on the use of facial recognition technology that enables mass surveillance.

We recognize the increasing use of this technology for commercial services, government administration, and policing functions. But the technology has evolved from a collection of niche systems to a powerful integrated network capable of mass surveillance and political control.

Facial recognition is now deployed for human identification, behavioral assessment, and predictive analysis.

Unlike other forms of biometric technology, facial recognition is capable of scrutinizing entire urban areas, capturing the identities of tens or hundreds of thousands of people at any one time.

Facial recognition can amplify identification asymmetry as it tends to be invisible or at best, opaque.

Facial recognition can be deployed in almost every dimension of life, from banking and commerce to transportation and communications.

We acknowledge that some facial recognition techniques enable authentication for the benefit of the user. However facial recognition also enables the development of semi-autonomous processes that minimize the roles of humans in decision making.

We note with alarm recent reports about bias, coercion, and fraud in the collection of facial images and the use of facial recognition techniques. Images are collected and used with forced consent or without consent at all.

We recall that in the 2009 Madrid Declaration, civil society called for a moratorium on the development or implementation of facial recognition, subject to a full and transparent evaluation by independent authorities and through democratic debate.

There is growing awareness of the need for a moratorium. In 2019 the Swedish Data Protection Authority prohibited the use of facial recognition in schools. The state of California prohibited the use facial recognition on police-worn body cameras. Several cities in the United States have banned the use of facial recognition systems, and there is growing protest around the world.

Therefore

1. We urge countries to suspend the further deployment of facial recognition technology for mass surveillance;
2. We urge countries to review all facial recognition systems to determine whether personal data was obtained lawfully and to destroy data that was obtained unlawfully;
3. We urge countries to undertake research to assess bias, privacy and data protection, risk, and cyber vulnerability, as well as the ethical, legal, and social implications associated with the deployment of facial recognition technologies; and
4. We urge countries to establish the legal rules, technical standards, and ethical guidelines necessary to safeguard fundamental rights and comply with legal obligations before further deployment of this technology occurs.