From: [b(6); (b)(7)(C)]
Sent: [Thu, 5 Dec 2019 13:28:51 +0000]
To: [b(6); (b)(7)(C)]
Subject: RE: DHS proposes expanding facial-recognition scans to US citizens

Very interesting, than [b(6); (b)(7)(C)]

From: [ice.dhs.gov>
Sent: Wednesday, December 4, 2019 5:09 PM
To: [b(6); (b)(7)(C)]
Ce: [b(6); (b)(7)(C)]
Subject: DHS proposes expanding facial-recognition scans to US citizens

I don’t know if this came up in the facial recognition session at the Federal Privacy Summit, but this was in the news yesterday in case anyone hasn’t seen it yet,

[b(7)(E)]

RIN Data

DHS/USCBP | RIN: 1651-AB22 | Publication ID: Fall 2019

Title: Collection of Biometric Data From U.S. Citizens Upon Entry To and Departure From the United States

Abstract:

The Department of Homeland Security (DHS) is required by statute to develop and implement a biometric entry-exit data system. To facilitate the implementation of a seamless biometric entry-exit system that uses facial recognition and to help prevent persons attempting to fraudulently use U.S. travel documents and identify criminals and known or suspected terrorists, DHS is proposing to amend the regulations to provide that all travelers, including U.S. citizens, may be required to be photographed upon entry and/or departure.

Agency: Department of Homeland Security(DHS) | Priority: Other Significant
RIN Status: Previously published in the Unified Agenda | Agenda Stage of Rulemaking: Proposed Rule Stage
Major: No | Unfunded Mandates: Undetermined
EO 13771 Designation: Other
CFR Citation: 8 CFR 215.8, 8 CFR 235.1
Legal Authority: 8 U.S.C. 1357(b), 8 U.S.C. 1185(b), 6 U.S.C. 211(c)
Legal Deadline: None

Timetable:

<table>
<thead>
<tr>
<th>Action</th>
<th>Date</th>
<th>FR Cite</th>
</tr>
</thead>
<tbody>
<tr>
<td>NPRM</td>
<td>07/00/2020</td>
<td></td>
</tr>
</tbody>
</table>

Regulatory Flexibility Analysis Required: Undetermined

Government Levels Affected: Undetermined

Federalsm: Undetermined

Included in the Regulatory Plan: No

RIN Data Printed in the FR: No

Agency Contact:
Director, Entry/Exit Policy and Planning
Department of Homeland Security
1300 Pennsylvania Avenue NW, Office of Field Operations
Washington, DC 20229
Phone: 202-325-
Email: ctp.dhs.gov

From: Holz, Jordan
To: Holz, Jordan
Subject: RE: 2019 Federal Privacy Summit: Registration Confirmation

Thanks, sharing this with the team as I think it would be helpful for all of us to learn a little bit more about AI.

Jordan Holz
Privacy Officer
Office of Information Governance and Privacy
U.S. Immigration and Customs Enforcement
Desk: 202-732-
Mobile: 202-7
Main: 202-732-3300

From: Holz, Jordan
To: Holz, Jordan
Subject: FW: 2019 Federal Privacy Summit: Registration Confirmation
It was IA who had an interesting chart on AI Ethics Framework. It included 1) Stewardship & Accountability, 2) Periodic review, 3) Human judgement & Accountability, 4) Transparency & Explainability (do we understand how the black box works) & Interpretability (verify accuracy); 5) What bias might exist in the project; 6) What legal obligations govern AI and the data; 7) How do I account for iterations (e.g. perfecting your golf game), auditability; 8) Documentation of your purpose, parameters, limitations, and design outcome, Testing your AI.

Also brought up her concerns about AI, and Hiring. She asked if anyone knew of any government agencies that were using AI for hiring. The following article is relevant to her concerns raised about using AI to determine an applicant’s employability, https://www.washingtonpost.com/technology/2019/10/22/ai-hiring-face-scanning-algorithm-increasingly-decides-whether-you-deserve-job/. P. 9 of the attached comparative review of AI, dated January 2019 from the Library of Congress shows a map of countries that have an AI strategy in place (e.g. Canada, Mexico, Russia, China, France, Great Britain). The U.S. is listed as not having a national AI Strategy.

Building an Artificial Intelligence Ethics Framework for Your Agency

Moderator and Background Presenter: Benjamin Huebner (ODNI)
Panelists: 

From: On Behalf Of Privacy Council
Sent: Thursday, November 21, 2019 10:19 AM
Subject: 2019 Federal Privacy Summit: Registration Confirmation

Good morning,

This email is to confirm your registration for the 2019 Federal Privacy Summit on Monday, December 2 at the Natcher Conference Center (NIH Campus, 45 Center Dr, Bethesda, MD 20894).

- If you were on the waitlist, this means you have been moved off and officially registered. Due to system limitations, MAX will not show this information.
- If you no longer plan to attend the Summit, please visit OMB MAX to unregister yourself or email privacy.council@gsa.gov in consideration for those on the waitlist.

Attached is the program which includes the agenda and session descriptions. Please also refer to the program for detailed directions about transportation, security, lunch, and a post-summit happy hour.

- Registration will open at 8:00 am and the first breakout sessions will begin at 9:00 am.
- All visitors must enter through the NIH Gateway Center and clear security. Visitors are required to show one form of government-issued identification.
- Take the Metro Redline to Medical Center Station. Or, limited parking is available at Gateway Parking Garage (MP-11) at the cost of $2/hour or $12/day.
• The deadline to pre-order and purchase a boxed lunch is COB Tuesday, November 26. Ordering instructions can be found on page 2 of the attached program. Attendees also have the option of bringing their own lunch.

For questions, please email privacy.council@gsa.gov.

--

Federal Privacy Council
FPC.gov
Come at me ACLU, I’m ready.

Best,

Privacy Compliance Specialist, CIPP/G
Information Governance and Privacy (IGP)
U.S. Immigration & Customs Enforcement
Direct: (202) 732-(b)(6)
Main: (202) 732-(b)(7)(C)

https://www.congress.gov/bill/116th-congress/senate-bill/3284?q=%7B%22search%22%3A%5B%22%5C%22facial-recognition%5C%22%22%5D%7D&s=2&r=1
From: [b](b)(6); (b)(7)(C) @ice.dhs.gov

Sent: Tuesday, February 18, 2020 12:06 PM

To: [b](b)(6); (b)(7)(C) ke.dhs.gov>

Subject: RE: facial recognition

Thanks! Let me know if/when there are updates

Best,
[b](b)(6); (b)(7)(C)

Mobile: 202-8 [b](b)(7)(C)

From: [b](b)(6); (b)(7)(C) @ice.dhs.gov

Sent: Tuesday, February 18, 2020 12:05 PM

To: [b](b)(6); (b)(7)(C) ke.dhs.gov>

Subject: facial recognition

“Two Democratic senators on Wednesday introduced a bill that would place a moratorium on federal government use of facial recognition technology until Congress passes legislation regulating it.”


https://www.congress.gov/bill/116th-congress/senate-bill/3284/text?q=%7B%22search%22%3A%5B%22%5C%22%5D%7D&r=4&s=2
Hi Jordan,

I have attached a draft summary of issues discussed in the CBP, USCIS, and FEMA Social Media PIAs (attached).

From: Holz, Jordan
Sent: Wednesday, September 25, 2019 10:15 AM
To: @ice.dhs.gov>
Subject: Social Media Project

Hi

Jordan Holz
Acting Privacy Officer
Office of Information Governance and Privacy
U.S. Immigration and Customs Enforcement
Desk: 202-732-4
Mobile: 202-701
Main: 202-732-
DHS Component Social Media Privacy Impact Assessments (PIAs) – Summary of Issues and Uses


Summary of issues discussed:

(b)(5)

Principal of Data Quality and Integrity

(b)(5)

Principal of Security

(b)(5)
First Amendment Protections

(b)(5)

Principal of Use Limitation

(b)(5)

**Operational Uses:**
B. Fraud Detection and National Security Directorate, DHS/USCIS/PIA-013-01(a),

Summary of issues discussed:

Principal of Purpose Specification

(b)(5)
Principal of Data Quality and Integrity

(b)(5)

Principal of Security

(b)(5)
Accountability:

Operational Uses:

C. FEMA Operational Use of Publicly Available Social Media for Situational Awareness, DHS/FEMA/PIA-041 (March 10, 2016)

Summary of issues discussed:

Principal of Purpose Specification
Data Quality and Integrity

Principal of Use Limitation
Operational Uses:

(b)(5)
Hi Jordan,

I have attached a copy of FY2020 training efforts metrics. The only person that did not complete is [redacted] because she just has training planned in the future for FY20.

I also sent you my review for the CBP, USCIS, and FEMA Social Media PIAs on September 25, 2019.

From: Holz, Jordan
Sent: Tuesday, January 21, 2020 9:43 AM
To: Holz, Jordan
Subject: RE: Pending Assignments with me

Thanks, just flagged it.

Jordan Holz
Privacy Officer
Office of Information Governance and Privacy
U.S. Immigration and Customs Enforcement
Desk: 202-732-0077
Mobile: 202-705-2230
Main: 202-732-3300

From: Holz, Jordan
Sent: Tuesday, January 21, 2020 9:36 AM
To: Holz, Jordan
Subject: RE: Pending Assignments with me

Good morning,

I sent you my comments for the PTA SOP on 1/13/2020.
Good morning,

I have a slight backlog in reviewing some of the work in my inbox, so I wanted to make sure I have a complete list of what you’re all waiting for. If there’s something I’m missing from the list below, please let me know.

- FIP SharePoint Site PTA
- Comments on Privacy Incident SOP
- SEVP Procurement, SEVP LOI
- Clearview PTA
- N/A
- HSI training module, OAFM workplace procurement
- Deloitte – PATRIOT PIA, Privacy Act Statement SOP, Privacy Incident SOP, LPR use case memo, PACS PTA renewal

Thanks!

Jordan Holz
Privacy Officer
Office of Information Governance and Privacy
U.S. Immigration and Customs Enforcement
Desk: 202-732-1
Mobile: 202-70
Main: 202-732-1
From: Holz, Jordan

Sent: Wednesday, September 25, 2019 10:15 AM

To: ice.dhs.gov>

Subject: Social Media Project

Hi,

I have attached a draft summary of issues discussed in the CBP, USCIS, and FEMA Social Media PIAs (attached).

Privacy Compliance Specialist, CIPP/G
Information Governance and Privacy (IGP)
U.S. Immigration & Customs Enforcement

Direct: (202) 732-2021
Main: (202) 732-2022
Good afternoon,

Please find attached the latest ICE Monthly Report and Crystal Report. Please let me know of any inaccuracies you may find in the reports.

Respectfully,

[Redacted]
Privacy Analyst
Contractor supporting the DHS Privacy Office
Phone: (202) 343-
Email: associates.hq.dhs.gov
From:
Sent: Wed, 4 Mar 2020 13:44:12 +0000
To: Holz, Jordan
Subject: ICE wants to use facial recognition to track people threatening its agents online

This was in today’s ICE Briefing on Insight.

Privacy Compliance Specialist, CIPP/G
Information Governance and Privacy (IGP)
U.S. Immigration & Customs Enforcement
Direct: (202) 732
Main: (202) 732
Learning Hour: Artificial Intelligence, Machine Learning and Data Ethics
12/7/2018, IAPP
From: [redacted]  
Sent: Thu, 5 Mar 2020 14:30:35 +0000  
To: [redacted]  
Subject: [MD] HSI special agent talks about DMV access

[MD] HSI special agent talks about DMV access
WAMU [3/4/2020 12:57 PM, Staff, DC] reports that special agent John Isaac in Baltimore, who is in charge of Homeland Security Investigations, says that HSI doesn’t search the Maryland driver database for civil immigration purposes very often. He says that facial recognition is used in criminal investigations, including in cases of child exploitation and human trafficking. [Editorial note: consult source link for audio]

Privacy Compliance Specialist, CIPP/G
Information Governance and Privacy (IGP)
U.S. Immigration & Customs Enforcement
Direct: (202) 7[redacted]; Main: (202) 7[redacted]

Disclaimer: The views expressed in this shared material-article(s) do not necessarily reflect the views of the sender (in official or unofficial capacity). The sender does not necessarily agree with the views expressed by the shared material article(s). The material-article is merely being shared through the privacy professional community (as privacy or data privacy news, noteworthy item(s)) or being shared by a fellow Federal Privacy Council member-leader throughout the privacy professional community. If you wish to no longer receive these “privacy in the news” emails, please notify the sender soonest.
116TH CONGRESS
1ST SESSION

S. 2878

To limit the use of facial recognition technology by Federal agencies, and for other purposes.

IN THE SENATE OF THE UNITED STATES

NOVEMBER 14, 2019

Mr. COONS (for himself and Mr. LEE) introduced the following bill; which was read twice and referred to the Committee on the Judiciary

A BILL

To limit the use of facial recognition technology by Federal agencies, and for other purposes.

Be it enacted by the Senate and House of Representa-
tives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the “Facial Recognition Technology Warrant Act of 2019”.

SEC. 2. DEFINITIONS.

In this Act:

(1) AGENCY.—The term “agency” has the meaning given the term in section 551 of title 5, United States Code.
(2) COVERED COURT ORDER.—The term “covered court order” means a court order obtained in accordance with rule 41 of the Federal Rules of Criminal Procedure and in connection with the investigation of an offense for which an order could be sought under section 2516 of title 18, United States Code.

(3) FACIAL RECOGNITION TECHNOLOGY.—The term “facial recognition technology” means technology that analyzes facial features and is used for the unique personal identification of individuals in still or video images.

(4) ONGOING SURVEILLANCE.—The term “ongoing surveillance”—

(A) means the utilization of facial recognition technology to engage in a sustained effort to track the physical movements of an identified individual through 1 or more public places where such movements occur over a period of time greater than 72 hours, whether in real time or through application of such technology to historical records; and

(B) does not include instances where facial recognition technology is utilized for a single identification or attempted identification of an
individual, if no subsequent attempt is made to
track that individual’s movement in real time or
through the use of historical records after the
individual has been identified.

SEC. 3. LIMITATION ON USE OF FACIAL RECOGNITION
TECHNOLOGY.

(a) IN GENERAL.—Subject to subsection (b), an offi-
cer or employee of an agency may not use facial recogni-
tion technology to engage in ongoing surveillance of an
individual or group of individuals in a public space, un-
less—

(1) the use of the facial recognition technology
is in support of a law enforcement activity; and

(2)(A) a covered court order has been obtained
to allow the use of facial recognition technology for
ongoing surveillance of the individual or group of in-
dividuals; or

(B) an investigative or law enforcement offi-
cer—

(i) reasonably determines that exigent cir-
cumstances and compelling law enforcement
needs make it impractical to obtain a covered
court order;
(ii) reasonably determines that there are grounds for which a covered court order could be obtained under subparagraph (A); and

(iii) causes an application for a covered court order to be made in accordance with subparagraph (A) not later than 48 hours after the use of facial recognition technology to engage in ongoing surveillance.

(b) REQUIREMENT.—If an application for a covered court order made under subsection (a)(2)(B) is denied, the use of facial recognition technology shall terminate at the time of the denial.

(c) DURATION OF ORDERS.—

(1) IN GENERAL.—Subject to paragraph (2), a covered court order may only authorize ongoing surveillance until the date on which the objective of the order is satisfied, except that such order may not authorize ongoing surveillance for a period of longer than 30 days.

(2) REQUIREMENT.—The 30-day period described in paragraph (1) shall begin on the earlier of—

(A) the date on which the agency begins to use facial recognition technology; or
(B) the date that is 10 days after the court order is issued.

(3) EXTENSION.—A court may grant an extension of the 30-day period described in paragraph (1) if the extension satisfies the requirements of subsection (a)(2)(A) and such extension may last not longer than 30 days.

(d) MINIMIZATION REQUIREMENT.—Any use of facial recognition technology pursuant to a covered court order shall be conducted in such a way as to minimize the acquisition, retention, and dissemination of information about the individuals other than those for whom there was probable cause to seek the covered court order obtained under subsection (a)(2)(A).

(e) MOTION TO SUPPRESS.—

(1) IN GENERAL.—Except as provided in paragraph (2), any aggrieved individual who has been the subject of ongoing surveillance using facial recognition technology, in any trial, hearing, or proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, may move to suppress information directly obtained through the use of facial recognition tech-
nology, or evidence derived therefrom, in violation of this section, on the grounds that—

(A) the information was unlawfully obtained;

(B) the order of authorization or approval under which the information was obtained is insufficient on its face; or

(C) the use of facial recognition technology was not used in conformity with the order of authorization or approval.

(2) EXCEPTION.—Evidence obtained through the use of facial recognition technology in violation of this section shall not be suppressed under paragraph (1) if the evidence was acquired by an officer or an employee of an agency with an objectively reasonable belief that the use of facial recognition technology was in compliance with this section.

(3) REQUIREMENT.—A motion described in paragraph (1) shall be made before the trial, hearing, or proceeding unless there was no opportunity to make such motion or the individual was not aware of the grounds of the motion. If the motion is granted, the information directly obtained through the use of facial recognition technology, or evidence derived
therefrom, shall be treated as having been obtained in violation of this section.

(4) INSPECTION OF INFORMATION.—The judge, upon the filing of a motion under this subsection by the aggrieved individual, may in his or her discretion make available to the aggrieved individual or counsel of the aggrieved individual for inspection such portions of the information or evidence derived therefrom as the judge determines to be in the interests of justice.

(5) APPEAL.—In addition to any other right to appeal, the United States shall have the right to appeal from an order granting a motion to suppress made under this subsection, or the denial of an application for an order of approval, if the United States attorney shall certify to the judge or other official granting such motion or denying such application that the appeal is not taken for purposes of delay. Such appeal shall be taken within 30 days after the date the order was entered and shall be diligently prosecuted.

(6) LIMITATION.—The remedies and sanctions described in this subsection with respect to the use of facial recognition technology are the only judicial
remedies and sanctions for nonconstitutional violations of this section involving such technology.

(f) **FOREIGN INTELLIGENCE INFORMATION.**—Nothing in this section shall be construed to affect the use of facial recognition technology to engage in ongoing surveillance connected with the acquisition of foreign intelligence information, as defined in section 101(e) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801(e)).

**SEC. 4. REPORTS ON GOVERNMENT USE OF FACIAL RECOGNITION TECHNOLOGY.**

(a) **REPORT BY JUDGE.**—Not later than 30 days after issuance of a covered court order under section 3(a)(2)(A) or an extension thereof under section 3(c)(3), or the denial of such a warrant or extension, the issuing or denying judge shall report to the Administrative Office of the United States Courts—

1. the fact that a warrant or extension was applied for;
2. the fact that the warrant or extension was granted as applied for, was modified, or was denied;
3. the period of time for which the warrant approves the use of facial recognition technology, and the number and duration of any extensions; and
4. the offense specified in the warrant or application.
(b) REPORTS.—Beginning 1 year after the date of enactment of this Act, and not later than September 30 of each year thereafter, the Director of the Administrative Office of the United States Courts shall transmit to the Committee on the Judiciary of the Senate and the Committee on the Judiciary of the House of Representatives, and make available to the public, a full and complete report summarizing the data required to be filed with the Administrative Office under subsection (a), including—

(1) the number of applications for covered court orders and extensions authorizing delayed notice;

(2) the number of covered court orders and extensions granted or denied during the preceding fiscal year;

(3) for each covered court order or extension granted—

(A) the period of time for which the warrant approves the use of facial recognition technology, and the number and duration of any extensions;

(B) the offense specified in the covered court order or application, or extension of an order;

(C) the identity of the applying investigative or law enforcement officer and agency mak-
ing the application and the person authorizing
the application; and

(D) the nature of the facilities or cameras
from which the data analyzed by facial recogni-
tion technology came from;

(4) a general description of the identifications
made under a covered court order or extension, in-
cluding—

(A) the approximate nature and frequency
of use of the facial recognition technology;

(B) the approximate number of persons
who were subjected to analysis using the facial
recognition technology; and

(C) the approximate nature, amount, and
cost of the manpower and other resources dur-
ing the use of the facial recognition technology;
and

(5) the number of misidentifications, including
any arrest of an individual that does not result in
charges being entered against the individual, made
based upon information directly obtained through
the use of facial recognition technology, or evidence
derived therefrom.

(c) REGULATIONS.—The Director of the Administra-
tive Office of the United States Courts, in consultation

---
with the Attorney General, may issue guidance regarding
the content and form of the reports required to be filed
under subsection (a).

SEC. 5. HUMAN REVIEW AND TESTING.

(a) Human Review of Facial Recognition Technology.—An agency shall require a trained officer to ex-
amine the output or recommendation of any facial recogni-
tion system before the agency investigates or otherwise
interacts with an individual identified by the system in
connection with a covered court order issued under section
3(a)(2)(A) or in connection with an emergency under sec-
tion 3(a)(2)(B).

(b) Testing.—The head of each agency, in consulta-
tion with the Director of the National Institute of Stand-
ards and Technology, shall establish testing procedures re-
garding all facial recognition technology systems used by
the agency, including a process to—

(1) periodically undertake independent tests of
the performance of the system in typical operational
conditions;

(2) identify relative performance across dif-
ferent subpopulations, including error rates when
the system is tested across subpopulations, alone
and in combination with, different skin tones, ages,
and genders; and
(3) review such tests and take action to improve the accuracy of the system across subpopulations upon a finding indicating there are disparate error rates when the system is tested across subpopulations.
From:       [b](6), [b](7)(C)  
Sent:      Thu, 9 Jan 2020 21:18:36 +0000  
To:        Holz, Jordan  
Subject:   “Facial Recognition Technology Warrant Act of 2019”  
Attachments:  BILLS-116s2878is.pdf  

[b](5)
To limit the use of facial recognition technology by Federal agencies, and for other purposes.

IN THE SENATE OF THE UNITED STATES

NOVEMBER 14, 2019

Mr. COONS (for himself and Mr. LEE) introduced the following bill; which was read twice and referred to the Committee on the Judiciary

A BILL

To limit the use of facial recognition technology by Federal agencies, and for other purposes.

Be it enacted by the Senate and House of Representa-
tives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the “Facial Recognition Technology Warrant Act of 2019”.

SEC. 2. DEFINITIONS.

In this Act:

(1) AGENCY.—The term “agency” has the meaning given the term in section 551 of title 5, United States Code.
(2) COVERED COURT ORDER. — The term “covered court order” means a court order obtained in accordance with rule 41 of the Federal Rules of Criminal Procedure and in connection with the investigation of an offense for which an order could be sought under section 2516 of title 18, United States Code.

(3) FACIAL RECOGNITION TECHNOLOGY. — The term “facial recognition technology” means technology that analyzes facial features and is used for the unique personal identification of individuals in still or video images.

(4) ONGOING SURVEILLANCE. — The term “ongoing surveillance” —

(A) means the utilization of facial recognition technology to engage in a sustained effort to track the physical movements of an identified individual through 1 or more public places where such movements occur over a period of time greater than 72 hours, whether in real time or through application of such technology to historical records; and

(B) does not include instances where facial recognition technology is utilized for a single identification or attempted identification of an
individual, if no subsequent attempt is made to
track that individual’s movement in real time or
through the use of historical records after the
individual has been identified.

SEC. 3. LIMITATION ON USE OF FACIAL RECOGNITION
TECHNOLOGY.

(a) IN GENERAL.—Subject to subsection (b), an offi-
cer or employee of an agency may not use facial recogni-
tion technology to engage in ongoing surveillance of an
individual or group of individuals in a public space, un-
less—

(1) the use of the facial recognition technology
is in support of a law enforcement activity; and

(2)(A) a covered court order has been obtained
to allow the use of facial recognition technology for
ongoing surveillance of the individual or group of in-
dividuals; or

(B) an investigative or law enforcement offi-
cer—

(i) reasonably determines that exigent cir-
cumstances and compelling law enforcement
needs make it impractical to obtain a covered
court order;
(ii) reasonably determines that there are grounds for which a covered court order could be obtained under subparagraph (A); and

(iii) causes an application for a covered court order to be made in accordance with subparagraph (A) not later than 48 hours after the use of facial recognition technology to engage in ongoing surveillance.

(b) REQUIREMENT.—If an application for a covered court order made under subsection (a)(2)(B) is denied, the use of facial recognition technology shall terminate at the time of the denial.

(c) DURATION OF ORDERS.—

(1) IN GENERAL.—Subject to paragraph (2), a covered court order may only authorize ongoing surveillance until the date on which the objective of the order is satisfied, except that such order may not authorize ongoing surveillance for a period of longer than 30 days.

(2) REQUIREMENT.—The 30-day period described in paragraph (1) shall begin on the earlier of—

(A) the date on which the agency begins to use facial recognition technology; or
(B) the date that is 10 days after the court order is issued.

(3) EXTENSION.—A court may grant an extension of the 30-day period described in paragraph (1) if the extension satisfies the requirements of subsection (a)(2)(A) and such extension may last not longer than 30 days.

(d) MINIMIZATION REQUIREMENT.—Any use of facial recognition technology pursuant to a covered court order shall be conducted in such a way as to minimize the acquisition, retention, and dissemination of information about the individuals other than those for whom there was probable cause to seek the covered court order obtained under subsection (a)(2)(A).

(e) MOTION TO SUPPRESS.—

(1) IN GENERAL.—Except as provided in paragraph (2), any aggrieved individual who has been the subject of ongoing surveillance using facial recognition technology, in any trial, hearing, or proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, may move to suppress information directly obtained through the use of facial recognition tech-
ology, or evidence derived therefrom, in violation of this section, on the grounds that—

(A) the information was unlawfully obtained;

(B) the order of authorization or approval under which the information was obtained is insufficient on its face; or

(C) the use of facial recognition technology was not used in conformity with the order of authorization or approval.

(2) EXCEPTION.—Evidence obtained through the use of facial recognition technology in violation of this section shall not be suppressed under paragraph (1) if the evidence was acquired by an officer or an employee of an agency with an objectively reasonable belief that the use of facial recognition technology was in compliance with this section.

(3) REQUIREMENT.—A motion described in paragraph (1) shall be made before the trial, hearing, or proceeding unless there was no opportunity to make such motion or the individual was not aware of the grounds of the motion. If the motion is granted, the information directly obtained through the use of facial recognition technology, or evidence derived
therefrom, shall be treated as having been obtained in violation of this section.

(4) INSPECTION OF INFORMATION.—The judge, upon the filing of a motion under this subsection by the aggrieved individual, may in his or her discretion make available to the aggrieved individual or counsel of the aggrieved individual for inspection such portions of the information or evidence derived therefrom as the judge determines to be in the interests of justice.

(5) APPEAL.—In addition to any other right to appeal, the United States shall have the right to appeal from an order granting a motion to suppress made under this subsection, or the denial of an application for an order of approval, if the United States attorney shall certify to the judge or other official granting such motion or denying such application that the appeal is not taken for purposes of delay. Such appeal shall be taken within 30 days after the date the order was entered and shall be diligently prosecuted.

(6) LIMITATION.—The remedies and sanctions described in this subsection with respect to the use of facial recognition technology are the only judicial
remedies and sanctions for nonconstitutional violations of this section involving such technology.

(f) FOREIGN INTELLIGENCE INFORMATION.—Nothing in this section shall be construed to affect the use of facial recognition technology to engage in ongoing surveillance connected with the acquisition of foreign intelligence information, as defined in section 101(e) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801(e)).

SEC. 4. REPORTS ON GOVERNMENT USE OF FACIAL RECOGNITION TECHNOLOGY.

(a) REPORT BY JUDGE.—Not later than 30 days after issuance of a covered court order under section 3(a)(2)(A) or an extension thereof under section 3(c)(3), or the denial of such a warrant or extension, the issuing or denying judge shall report to the Administrative Office of the United States Courts—

(1) the fact that a warrant or extension was applied for;

(2) the fact that the warrant or extension was granted as applied for, was modified, or was denied;

(3) the period of time for which the warrant approves the use of facial recognition technology, and the number and duration of any extensions; and

(4) the offense specified in the warrant or application.
(b) Reports.—Beginning 1 year after the date of enactment of this Act, and not later than September 30 of each year thereafter, the Director of the Administrative Office of the United States Courts shall transmit to the Committee on the Judiciary of the Senate and the Committee on the Judiciary of the House of Representatives, and make available to the public, a full and complete report summarizing the data required to be filed with the Administrative Office under subsection (a), including—

(1) the number of applications for covered court orders and extensions authorizing delayed notice;

(2) the number of covered court orders and extensions granted or denied during the preceding fiscal year;

(3) for each covered court order or extension granted—

(A) the period of time for which the warrant approves the use of facial recognition technology, and the number and duration of any extensions;

(B) the offense specified in the covered court order or application, or extension of an order;

(C) the identity of the applying investigative or law enforcement officer and agency mak-
ing the application and the person authorizing
the application; and

(D) the nature of the facilities or cameras
from which the data analyzed by facial recogni-
tion technology came from;

(4) a general description of the identifications
made under a covered court order or extension, in-
cluding—

(A) the approximate nature and frequency
of use of the facial recognition technology;

(B) the approximate number of persons
who were subjected to analysis using the facial
recognition technology; and

(C) the approximate nature, amount, and
cost of the manpower and other resources dur-
ing the use of the facial recognition technology;

and

(5) the number of misidentifications, including
any arrest of an individual that does not result in
charges being entered against the individual, made
based upon information directly obtained through
the use of facial recognition technology, or evidence
derived therefrom.

(c) REGULATIONS.—The Director of the Administra-
tive Office of the United States Courts, in consultation
with the Attorney General, may issue guidance regarding
the content and form of the reports required to be filed
under subsection (a).

SEC. 5. HUMAN REVIEW AND TESTING.

(a) HUMAN REVIEW OF FACIAL RECOGNITION TECHNOLOGY.—An agency shall require a trained officer to ex-
amine the output or recommendation of any facial recogni-
tion system before the agency investigates or otherwise
interacts with an individual identified by the system in
connection with a covered court order issued under section
3(a)(2)(A) or in connection with an emergency under sec-
tion 3(a)(2)(B).

(b) TESTING.—The head of each agency, in consulta-
tion with the Director of the National Institute of Stand-
ard and Technology, shall establish testing procedures re-
garding all facial recognition technology systems used by
the agency, including a process to—

(1) periodically undertake independent tests of
the performance of the system in typical operational
conditions;

(2) identify relative performance across dif-
ferent subpopulations, including error rates when
the system is tested across subpopulations, alone
and in combination with, different skin tones, ages,
and genders; and
(3) review such tests and take action to improve the accuracy of the system across subpopulations upon a finding indicating there are disparate error rates when the system is tested across subpopulations.