

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

**Subject:** DHS proposes expanding facial-recognition scans to US citizens

(b)(7)(E)

**Legal Deadline:** None

**Timetable:**

Action	Date	FR Cite
NPRM	07/00/2020	

**Regulatory Flexibility Analysis Required:**

Undetermined

**Government Levels Affected:** Undetermined

**Federalism:** Undetermined

**Included in the Regulatory Plan:** No

**RIN Data Printed in the FR:** No

**Agency Contact:**

(b)(6); (b)(7)(C)

Director, Entry/Exit Policy and Planning

Department of Homeland Security

U.S. Customs and Border Protection

1300 Pennsylvania Avenue NW, Office of Field Operations, (b)(6);

Washington, DC 20229 (b)(7)(C)

Phone: 202 325 (b)(6);

Email: (b)(6); (b)(7)(C) @cbp.dhs.gov

---

**From:** Holz, Jordan (b)(6); (b)(7)(C) @ice.dhs.gov>

**Sent:** Tuesday, December 3, 2019 1:32 PM

**To:** (b)(6); (b)(7)(C) @ice.dhs.gov>

**Cc:** (b)(6); (b)(7)(C) @ice.dhs.gov>; (b)(6); (b)(7)(C)

(b)(6); (b)(7)(C) @ice.dhs.gov>; (b)(6); (b)(7)(C) @ice.dhs.gov>; (b)(6); (b)(7)(C)

(b)(6); (b)(7)(C) @ice.dhs.gov>; (b)(6); (b)(7)(C) @ice.dhs.gov>

(b)(6); (b)(7)(C) @associates.ice.dhs.gov>; (b)(6); (b)(7)(C) @associates.ice.dhs.gov>;

(b)(6); (b)(7)(C) @associates.ice.dhs.gov>; (b)(6); (b)(7)(C)

(b)(6); (b)(7)(C) @ice.dhs.gov>

**Subject:** RE: 2019 Federal Privacy Summit: Registration Confirmation

Thanks, (b)(6); (b)(7)(C) 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-(b)(6);

Mobile: 202-70 (b)(7)(C)

Main: 202-732-3300

---

**From:** (b)(6); (b)(7)(C) @ice.dhs.gov>

**Sent:** Tuesday, December 3, 2019 1:19 PM

**To:** Holz, Jordan (b)(6); (b)(7)(C) @ice.dhs.gov>

**Subject:** FW: 2019 Federal Privacy Summit: Registration Confirmation

It was (b)(6); (b)(7)(C) 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.

(b)(6); (b)(7)(C) also brought up her concerns about AI, and Hiring. She asked if anyone new 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 a 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.

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

## Building an Artificial Intelligence Ethics Framework for Your Agency

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

*Panelists:* (b)(6); (b)(7)(C)

From: (b)(6); (b)(7)(C)@gsa.gov <(b)(6); (b)(7)(C)@gsa.gov> 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](mailto: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](mailto:privacy.council@gsa.gov).

--

**Federal Privacy Council**

[FPC.gov](http://FPC.gov)

**From:** (b)(6); (b)(7)(C)  
**Sent:** Fri, 13 Mar 2020 19:42:32 +0000  
**To:** (b)(6); (b)(7)(C)  
**Subject:** RE: facial recognition

Come at me ACLU, I'm ready.

Best,

(b)(6); (b)(7)(C)

Mobile: 202-8 (b)(6); (b)(7)(C)

---

**From:** (b)(6); (b)(7)(C)@ice.dhs.gov>  
**Sent:** Friday, March 13, 2020 3:41 PM  
**To:** (b)(6); (b)(7)(C)@ice.dhs.gov>  
**Subject:** FW: facial recognition

<https://www.washingtonpost.com/technology/2020/03/12/aclu-sues-federal-agencies-seeking-records-facial-recognition-use-airports-us-border/>

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Thursday, February 27, 2020 9:42 AM  
**To:** (b)(6); (b)(7)(C)@ice.dhs.gov>  
**Subject:** FW: facial recognition

<https://www.washingtonpost.com/technology/2020/02/26/ice-has-run-facial-recognition-searches-millions-maryland-drivers/>

---

**From:** (b)(6); (b)(7)(C)  
**Sent:** Monday, February 24, 2020 10:06 AM  
**To:** (b)(6); (b)(7)(C)@ice.dhs.gov>  
**Subject:** RE: facial recognition

Title changed: S.3284 - Ethical Use of Facial Recognition

<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>

(b)(6); (b)(7)(C)

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

**From:** (b)(6); (b)(7)(C)@ice.dhs.gov>  
**Sent:** Tuesday, February 18, 2020 12:06 PM  
**To:** (b)(6); (b)(7)(C)@ice.dhs.gov>  
**Subject:** RE: facial recognition

Thanks! Let me know if/when there are updates

Best,

(b)(6); (b)(7)(C)

Mobile: 202-87 (b)(6); (b)(7)(C)

**From:** (b)(6); (b)(7)(C)@ice.dhs.gov>  
**Sent:** Tuesday, February 18, 2020 12:05 PM  
**To:** (b)(6); (b)(7)(C)@ice.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://thehill.com/policy/technology/482815-booker-merkley-propose-facial-recognition-moratorium>

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

4 OF 19 RESULTS

**S.3284 - A bill to create a moratorium on the government use of facial recognition technology until a Commission recommends the appropriate guidelines and limitation for use of facial recognition technology.**  
116th Congress (2019-2020) | [Get alerts](#)

**BILL** Hide Overview

**Sponsor:** Sen. Merkley, Jeff [D-OR] (Introduced 02/12/2020)

**Committees:** Senate - Homeland Security and Governmental Affairs

**Latest Action:** Senate - 02/12/2020 Read twice and referred to the Committee on Homeland Security and Governmental Affairs. [\(All Actions\)](#)

**Tracker:**

Introduced → Passed Senate → Passed House → To President → Became Law

**More on This Bill**  
[CBO Cost Estimates \[0\]](#)

**Get more information**  
[See Coverage Dates for Legislative Information](#) and learn about other sources.

Summary (0) **Text** Actions (1) Titles (1) Amendments (0) Cosponsors (1) Committees (1) Related Bills (0)

**Text: S.3284 — 116th Congress (2019-2020)** [All Information \(Except Text\)](#)

As of 02/18/2020 text has not been received for S.3284 - A bill to create a moratorium on the government use of facial recognition technology until a Commission recommends the appropriate guidelines and limitation for use of facial recognition technology.

Bills are generally sent to the Library of Congress from GPO, the Government Publishing Office, a day or two after they are introduced on the floor of the House or Senate. Delays can occur when there are a large number of bills to prepare or when a very large bill has to be printed.

**From:** (b)(6); (b)(7)(C)  
**Sent:** Wed, 25 Sep 2019 19:19:04 +0000  
**To:** Holz, Jordan  
**Subject:** RE: Social Media Project  
**Attachments:** DHS Component Social Media PIAs-Summary of Issues and Uses (IGP 09 25 2019).docx

Hi Jordan,

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

(b)(6); (b)(7)(C)  
**Privacy Compliance Specialist, CIPP/G**  
**Information Governance and Privacy (IGP)**  
**U.S. Immigration & Customs Enforcement**  
**Direct: (202) 734-(b)(6);**  
**Main: (202) 734-(b)(7)(C)**

---

**From:** Holz, Jordan (b)(6); (b)(7)(C) <[redacted]@ice.dhs.gov>  
**Sent:** Wednesday, September 25, 2019 10:15 AM  
**To:** (b)(6); (b)(7)(C) <[redacted]@ice.dhs.gov>  
**Subject:** Social Media Project

Hi (b)(6); (b)(7)(C)

(b)(5); (b)(7)(E)

**Jordan Holz**  
Acting Privacy Officer  
Office of Information Governance and Privacy  
U.S. Immigration and Customs Enforcement  
Desk: 202-732-4-(b)(6); (b)(7)(C)  
Mobile: 202-701-3-(b)(6); (b)(7)(C)  
Main: 202-732-3-(b)(6); (b)(7)(C)

## DHS Component Social Media Privacy Impact Assessments (PIAs) – Summary of Issues and Uses

- A. Publicly Available Social Media Monitoring and Situational Awareness Initiative, DHS/CBP/PIA-058 (March 25, 2019), <https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp58-socialmedia-march2019.pdf>

### **Summary of issues discussed:**

(b)(5)

### **Principal of Data Quality and Integrity**

(b)(5)

### **Principal of Security**

(b)(5)



(b)(5)

#### **First Amendment Protections**

(b)(5)

#### **Principal of Use Limitation**

(b)(5)

#### **Operational Uses:**

(b)(5)

(b)(5)

- B. Fraud Detection and National Security Directorate, DHS/USCIS/PIA-013-01(a), [https://www.dhs.gov/sites/default/files/publications/privacy-pia-uscis-013-01-fdns-july2019\\_0.pdf](https://www.dhs.gov/sites/default/files/publications/privacy-pia-uscis-013-01-fdns-july2019_0.pdf) (July 26, 2019)

**Summary of issues discussed:**

(b)(5)

**Principal of Purpose Specification**

(b)(5)

### **Principal of Data Quality and Integrity**

(b)(5)



### **Principal of Security**

(b)(5)



(b)(5)

**Accountability:**

(b)(5)

**Operational Uses:**

(b)(5)

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

**Summary of issues discussed:**

(b)(5)

**Principal of Purpose Specification**

(b)(5)

**Data Quality and Integrity**

(b)(5)

**Principal of Use Limitation**

(b)(5)

**Operational Uses:**

(b)(5)



**From:** (b)(6); (b)(7)(C)  
**Sent:** Tue, 21 Jan 2020 14:51:33 +0000  
**To:** Holz, Jordan  
**Subject:** RE: Pending Assignments with me  
**Attachments:** RE: Social Media Project, Copy of Copy of IGP Privacy Division FY2020 Training Efforts Metrics ((b)(6); (b)(7)(C)) 01 09 2020).xlsx

Hi Jordan,

I have attached a copy of FY2020 training efforts metrics. The only person that did not complete is (b)(6); (b)(7)(C) 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.

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

---

**From:** Holz, Jordan (b)(6); (b)(7)(C) @ice.dhs.gov>  
**Sent:** Tuesday, January 21, 2020 9:43 AM  
**To:** (b)(6); (b)(7)(C) @ice.dhs.gov>  
**Subject:** RE: Pending Assignments with me

Thanks, (b)(6); (b)(7)(C) Just flagged it.

**Jordan Holz**  
Privacy Officer  
Office of Information Governance and Privacy  
U.S. Immigration and Customs Enforcement  
Desk: 202-732-(b)(6); (b)(7)(C)  
Mobile: 202-70-(b)(7)(C)  
Main: 202-732-3300

---

**From:** (b)(6); (b)(7)(C) @ice.dhs.gov>  
**Sent:** Tuesday, January 21, 2020 9:36 AM  
**To:** Holz, Jordan (b)(6); (b)(7)(C) @ice.dhs.gov>  
**Subject:** RE: Pending Assignments with me

Good morning,

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

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)

(b)(6); (b)(7)(C) ice.dhs.gov> (b)(6); (b)(7)(C) e.dhs.gov>; (b)(6); (b)(7)(C)  
ice.dhs.gov> ice.dhs.gov>  
(b)(6); (b)(7)(C) ice.dhs.gov> (b)(6); (b)(7)(C) @associates.ice.dhs.gov>

2021-ICLI-00005 2220



**From:** (b)(6); (b)(7)(C)  
**Sent:** Wed, 25 Sep 2019 19:19:04 +0000  
**To:** Holz, Jordan  
**Subject:** RE: Social Media Project  
**Attachments:** DHS Component Social Media PIAs-Summary of Issues and Uses (IGP 09 25 2019).docx

Hi Jordan,

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

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

---

**From:** Holz, Jordan (b)(6); (b)(7)(C) @ice.dhs.gov>  
**Sent:** Wednesday, September 25, 2019 10:15 AM  
**To:** (b)(6); (b)(7)(C) @ice.dhs.gov>  
**Subject:** Social Media Project

Hi (b)(6); (b)(7)(C)

(b)(5)

**Jordan Holz**  
Acting Privacy Officer  
Office of Information Governance and Privacy  
U.S. Immigration and Customs Enforcement  
Desk: 202-732-(b)(6); (b)(7)(C)  
Mobile: 202-700-(b)(6); (b)(7)(C)  
Main: 202-732-(b)(6); (b)(7)(C)

**From:** (b)(6); (b)(7)(C)  
**Sent:** Fri, 5 Jun 2020 16:10:45 +0000  
**To:** Holz, Jordan  
**Cc:** (b)(6); (b)(7)(C)  
(b)(6); (b)(7)(C)  
**Subject:** ICE Monthly Report  
**Attachments:** ICE Privacy Report, Operational Only, 20200603.pdf, ICE Monthly Status Report, May 2020.pdf

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,

(b)(6); (b)(7)(C)  
Privacy Analyst  
Contractor supporting the DHS Privacy Office  
Phone: (202) 343- (b)(6); (b)(7)(C)  
Email: (b)(6); (b)(7)(C)@associates.hq.dhs.gov

**From:** (b)(6); (b)(7)(C)  
**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.

(b)(7)(E)

(b)(6); (b)(7)(C)

**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)

**From:** (b)(6); (b)(7)(C)  
**Sent:** Fri, 22 Mar 2019 17:26:46 +0000  
**To:** (b)(6); (b)(7)(C)  
**Subject:** Learning Hour: Artificial Intelligence, Machine Learning and Data Ethics  
12/7/2018

Learning Hour: Artificial Intelligence, Machine Learning and Data Ethics  
12/7/2018, IAPP

**From:** (b)(6); (b)(7)(C)  
**Sent:** Thu, 5 Mar 2020 14:30:35 +0000  
**To:** (b)(6); (b)(7)(C)  
**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]

(b)(7)(E)

(b)(6); (b)(7)(C)

Privacy Compliance Specialist, CIPP/G  
Information Governance and Privacy (IGP)  
U.S. Immigration & Customs Enforcement  
Direct: (202) 733-(b)(6);  
Main: (202) 733-(b)(7)(C)

~~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.

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

3 **SECTION 1. SHORT TITLE.**

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

6 **SEC. 2. DEFINITIONS.**

7 In this Act:

8 (1) AGENCY.—The term “agency” has the  
9 meaning given the term in section 551 of title 5,  
10 United States Code.

1           (2) COVERED COURT ORDER.—The term “cov-  
2       ered court order” means a court order obtained in  
3       accordance with rule 41 of the Federal Rules of  
4       Criminal Procedure and in connection with the in-  
5       vestigation of an offense for which an order could be  
6       sought under section 2516 of title 18, United States  
7       Code.

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

13          (4) ONGOING SURVEILLANCE.—The term “on-  
14      going surveillance”—

15                (A) means the utilization of facial recogni-  
16      tion technology to engage in a sustained effort  
17      to track the physical movements of an identified  
18      individual through 1 or more public places  
19      where such movements occur over a period of  
20      time greater than 72 hours, whether in real  
21      time or through application of such technology  
22      to historical records; and

23                (B) does not include instances where facial  
24      recognition technology is utilized for a single  
25      identification or attempted identification of an

1 individual, if no subsequent attempt is made to  
2 track that individual's movement in real time or  
3 through the use of historical records after the  
4 individual has been identified.

5 **SEC. 3. LIMITATION ON USE OF FACIAL RECOGNITION**  
6 **TECHNOLOGY.**

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

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

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

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

20 (i) reasonably determines that exigent cir-  
21 cumstances and compelling law enforcement  
22 needs make it impractical to obtain a covered  
23 court order;



1 (ii) reasonably determines that there are  
2 grounds for which a covered court order could  
3 be obtained under subparagraph (A); and

4 (iii) causes an application for a covered  
5 court order to be made in accordance with sub-  
6 paragraph (A) not later than 48 hours after the  
7 use of facial recognition technology to engage in  
8 ongoing surveillance.

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

13 (c) DURATION OF ORDERS.—

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

20 (2) REQUIREMENT.—The 30-day period de-  
21 scribed in paragraph (1) shall begin on the earlier  
22 of—

23 (A) the date on which the agency begins to  
24 use facial recognition technology; or

1 (B) the date that is 10 days after the  
2 court order is issued.

3 (3) EXTENSION.—A court may grant an exten-  
4 sion of the 30-day period described in paragraph (1)  
5 if the extension satisfies the requirements of sub-  
6 section (a)(2)(A) and such extension may last not  
7 longer than 30 days.

8 (d) MINIMIZATION REQUIREMENT.—Any use of fa-  
9 cial recognition technology pursuant to a covered court  
10 order shall be conducted in such a way as to minimize  
11 the acquisition, retention, and dissemination of informa-  
12 tion about the individuals other than those for whom there  
13 was probable cause to seek the covered court order ob-  
14 tained under subsection (a)(2)(A).

15 (e) MOTION TO SUPPRESS.—

16 (1) IN GENERAL.—Except as provided in para-  
17 graph (2), any aggrieved individual who has been  
18 the subject of ongoing surveillance using facial rec-  
19 ognition technology, in any trial, hearing, or pro-  
20 ceeding in or before any court, department, officer,  
21 agency, regulatory body, or other authority of the  
22 United States, a State, or a political subdivision  
23 thereof, may move to suppress information directly  
24 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

1       therefrom, shall be treated as having been obtained  
2       in violation of this section.

3           (4) INSPECTION OF INFORMATION.—The judge,  
4       upon the filing of a motion under this subsection by  
5       the aggrieved individual, may in his or her discretion  
6       make available to the aggrieved individual or counsel  
7       of the aggrieved individual for inspection such por-  
8       tions of the information or evidence derived there-  
9       from as the judge determines to be in the interests  
10      of justice.

11          (5) APPEAL.—In addition to any other right to  
12      appeal, the United States shall have the right to ap-  
13      peal from an order granting a motion to suppress  
14      made under this subsection, or the denial of an ap-  
15      plication for an order of approval, if the United  
16      States attorney shall certify to the judge or other of-  
17      ficial granting such motion or denying such applica-  
18      tion that the appeal is not taken for purposes of  
19      delay. Such appeal shall be taken within 30 days  
20      after the date the order was entered and shall be  
21      diligently prosecuted.

22          (6) LIMITATION.—The remedies and sanctions  
23      described in this subsection with respect to the use  
24      of facial recognition technology are the only judicial

1 remedies and sanctions for nonconstitutional viola-  
2 tions of this section involving such technology.

3 (f) FOREIGN INTELLIGENCE INFORMATION.—Noth-  
4 ing in this section shall be construed to affect the use of  
5 facial recognition technology to engage in ongoing surveil-  
6 lance connected with the acquisition of foreign intelligence  
7 information, as defined in section 101(e) of the Foreign  
8 Intelligence Surveillance Act of 1978 (50 U.S.C. 1801(e)).

9 **SEC. 4. REPORTS ON GOVERNMENT USE OF FACIAL REC-**  
10 **OGNITION TECHNOLOGY.**

11 (a) REPORT BY JUDGE.—Not later than 30 days  
12 after issuance of a covered court order under section  
13 3(a)(2)(A) or an extension thereof under section 3(c)(3),  
14 or the denial of such a warrant or extension, the issuing  
15 or denying judge shall report to the Administrative Office  
16 of the United States Courts—

17 (1) the fact that a warrant or extension was ap-  
18 plied for;

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

21 (3) the period of time for which the warrant ap-  
22 proves the use of facial recognition technology, and  
23 the number and duration of any extensions; and

24 (4) the offense specified in the warrant or ap-  
25 plication.

1 (b) REPORTS.—Beginning 1 year after the date of  
2 enactment of this Act, and not later than September 30  
3 of each year thereafter, the Director of the Administrative  
4 Office of the United States Courts shall transmit to the  
5 Committee on the Judiciary of the Senate and the Com-  
6 mittee on the Judiciary of the House of Representatives,  
7 and make available to the public, a full and complete re-  
8 port summarizing the data required to be filed with the  
9 Administrative Office under subsection (a), including—

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

12 (2) the number of covered court orders and ex-  
13 tensions granted or denied during the preceding fis-  
14 cal year;

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

17 (A) the period of time for which the war-  
18 rant approves the use of facial recognition tech-  
19 nology, and the number and duration of any ex-  
20 tensions;

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

24 (C) the identity of the applying investiga-  
25 tive or law enforcement officer and agency mak-

1 ing the application and the person authorizing  
2 the application; and

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

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

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

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

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

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

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

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

4 **SEC. 5. HUMAN REVIEW AND TESTING.**

5 (a) HUMAN REVIEW OF FACIAL RECOGNITION TECH-  
6 NOLOGY.—An agency shall require a trained officer to ex-  
7 amine the output or recommendation of any facial recogni-  
8 tion system before the agency investigates or otherwise  
9 interacts with an individual identified by the system in  
10 connection with a covered court order issued under section  
11 3(a)(2)(A) or in connection with an emergency under sec-  
12 tion 3(a)(2)(B).

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

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

21 (2) identify relative performance across dif-  
22 ferent subpopulations, including error rates when  
23 the system is tested across subpopulations, alone  
24 and in combination with, different skin tones, ages,  
25 and genders; and



1           (3) review such tests and take action to improve  
2       the accuracy of the system across subpopulations  
3       upon a finding indicating there are disparate error  
4       rates when the system is tested across subpopula-  
5       tions.

○

**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)

(b)(6); (b)(7)(C)

**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)**

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.

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

3 **SECTION 1. SHORT TITLE.**

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

6 **SEC. 2. DEFINITIONS.**

7 In this Act:

8 (1) AGENCY.—The term “agency” has the  
9 meaning given the term in section 551 of title 5,  
10 United States Code.

1 (2) COVERED COURT ORDER.—The term “cov-  
2 ered court order” means a court order obtained in  
3 accordance with rule 41 of the Federal Rules of  
4 Criminal Procedure and in connection with the in-  
5 vestigation of an offense for which an order could be  
6 sought under section 2516 of title 18, United States  
7 Code.

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

13 (4) ONGOING SURVEILLANCE.—The term “on-  
14 going surveillance”—

15 (A) means the utilization of facial recogni-  
16 tion technology to engage in a sustained effort  
17 to track the physical movements of an identified  
18 individual through 1 or more public places  
19 where such movements occur over a period of  
20 time greater than 72 hours, whether in real  
21 time or through application of such technology  
22 to historical records; and

23 (B) does not include instances where facial  
24 recognition technology is utilized for a single  
25 identification or attempted identification of an

1 individual, if no subsequent attempt is made to  
2 track that individual's movement in real time or  
3 through the use of historical records after the  
4 individual has been identified.

5 **SEC. 3. LIMITATION ON USE OF FACIAL RECOGNITION**  
6 **TECHNOLOGY.**

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

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

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

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

20 (i) reasonably determines that exigent cir-  
21 cumstances and compelling law enforcement  
22 needs make it impractical to obtain a covered  
23 court order;

1 (ii) reasonably determines that there are  
2 grounds for which a covered court order could  
3 be obtained under subparagraph (A); and

4 (iii) causes an application for a covered  
5 court order to be made in accordance with sub-  
6 paragraph (A) not later than 48 hours after the  
7 use of facial recognition technology to engage in  
8 ongoing surveillance.

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

13 (c) DURATION OF ORDERS.—

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

20 (2) REQUIREMENT.—The 30-day period de-  
21 scribed in paragraph (1) shall begin on the earlier  
22 of—

23 (A) the date on which the agency begins to  
24 use facial recognition technology; or

1 (B) the date that is 10 days after the  
2 court order is issued.

3 (3) EXTENSION.—A court may grant an exten-  
4 sion of the 30-day period described in paragraph (1)  
5 if the extension satisfies the requirements of sub-  
6 section (a)(2)(A) and such extension may last not  
7 longer than 30 days.

8 (d) MINIMIZATION REQUIREMENT.—Any use of fa-  
9 cial recognition technology pursuant to a covered court  
10 order shall be conducted in such a way as to minimize  
11 the acquisition, retention, and dissemination of informa-  
12 tion about the individuals other than those for whom there  
13 was probable cause to seek the covered court order ob-  
14 tained under subsection (a)(2)(A).

15 (e) MOTION TO SUPPRESS.—

16 (1) IN GENERAL.—Except as provided in para-  
17 graph (2), any aggrieved individual who has been  
18 the subject of ongoing surveillance using facial rec-  
19 ognition technology, in any trial, hearing, or pro-  
20 ceeding in or before any court, department, officer,  
21 agency, regulatory body, or other authority of the  
22 United States, a State, or a political subdivision  
23 thereof, may move to suppress information directly  
24 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



1       therefrom, shall be treated as having been obtained  
2       in violation of this section.

3           (4) INSPECTION OF INFORMATION.—The judge,  
4       upon the filing of a motion under this subsection by  
5       the aggrieved individual, may in his or her discretion  
6       make available to the aggrieved individual or counsel  
7       of the aggrieved individual for inspection such por-  
8       tions of the information or evidence derived there-  
9       from as the judge determines to be in the interests  
10      of justice.

11          (5) APPEAL.—In addition to any other right to  
12      appeal, the United States shall have the right to ap-  
13      peal from an order granting a motion to suppress  
14      made under this subsection, or the denial of an ap-  
15      plication for an order of approval, if the United  
16      States attorney shall certify to the judge or other of-  
17      ficial granting such motion or denying such applica-  
18      tion that the appeal is not taken for purposes of  
19      delay. Such appeal shall be taken within 30 days  
20      after the date the order was entered and shall be  
21      diligently prosecuted.

22          (6) LIMITATION.—The remedies and sanctions  
23      described in this subsection with respect to the use  
24      of facial recognition technology are the only judicial

1 remedies and sanctions for nonconstitutional viola-  
2 tions of this section involving such technology.

3 (f) FOREIGN INTELLIGENCE INFORMATION.—Noth-  
4 ing in this section shall be construed to affect the use of  
5 facial recognition technology to engage in ongoing surveil-  
6 lance connected with the acquisition of foreign intelligence  
7 information, as defined in section 101(e) of the Foreign  
8 Intelligence Surveillance Act of 1978 (50 U.S.C. 1801(e)).

9 **SEC. 4. REPORTS ON GOVERNMENT USE OF FACIAL REC-**  
10 **OGNITION TECHNOLOGY.**

11 (a) REPORT BY JUDGE.—Not later than 30 days  
12 after issuance of a covered court order under section  
13 3(a)(2)(A) or an extension thereof under section 3(c)(3),  
14 or the denial of such a warrant or extension, the issuing  
15 or denying judge shall report to the Administrative Office  
16 of the United States Courts—

17 (1) the fact that a warrant or extension was ap-  
18 plied for;

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

21 (3) the period of time for which the warrant ap-  
22 proves the use of facial recognition technology, and  
23 the number and duration of any extensions; and

24 (4) the offense specified in the warrant or ap-  
25 plication.

1 (b) REPORTS.—Beginning 1 year after the date of  
2 enactment of this Act, and not later than September 30  
3 of each year thereafter, the Director of the Administrative  
4 Office of the United States Courts shall transmit to the  
5 Committee on the Judiciary of the Senate and the Com-  
6 mittee on the Judiciary of the House of Representatives,  
7 and make available to the public, a full and complete re-  
8 port summarizing the data required to be filed with the  
9 Administrative Office under subsection (a), including—

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

12 (2) the number of covered court orders and ex-  
13 tensions granted or denied during the preceding fis-  
14 cal year;

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

17 (A) the period of time for which the war-  
18 rant approves the use of facial recognition tech-  
19 nology, and the number and duration of any ex-  
20 tensions;

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

24 (C) the identity of the applying investiga-  
25 tive or law enforcement officer and agency mak-

1 ing the application and the person authorizing  
2 the application; and

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

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

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

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

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

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

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

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

4 **SEC. 5. HUMAN REVIEW AND TESTING.**

5 (a) HUMAN REVIEW OF FACIAL RECOGNITION TECH-  
6 NOLOGY.—An agency shall require a trained officer to ex-  
7 amine the output or recommendation of any facial recogni-  
8 tion system before the agency investigates or otherwise  
9 interacts with an individual identified by the system in  
10 connection with a covered court order issued under section  
11 3(a)(2)(A) or in connection with an emergency under sec-  
12 tion 3(a)(2)(B).

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

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

21 (2) identify relative performance across dif-  
22 ferent subpopulations, including error rates when  
23 the system is tested across subpopulations, alone  
24 and in combination with, different skin tones, ages,  
25 and genders; and

1           (3) review such tests and take action to improve  
2           the accuracy of the system across subpopulations  
3           upon a finding indicating there are disparate error  
4           rates when the system is tested across subpopula-  
5           tions.

○