ELIJAH E. CUMMINGS, MARYLAND
CHAIRMAN

ONE HUNDRED SIXTEENTH CONGRESS

JIM JORDAN, OHIO
RANKING MINORITY MEMBER

Congress of the United States

House of Representatives

COMMITTEE ON OVERSIGHT AND REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6143

MAJORITY (202) 225–5051
MINORITY (202) 225–5074

http://oversight.house.gov

MEMORANDUM

May 20, 2019

To: Members of the Committee on Oversight and Reform

Fr: Majority Staff

Re: Hearing on "Facial Recognition Technology (Part 1): Its Impact on Our Civil Rights and Liberties"

On **Wednesday, May 22, 2019, at 10:00 a.m., in room 2154 of the Rayburn House Office Building**, the Committee will hold a hearing examining the use of facial recognition technology by government and commercial entities and the need for oversight on how this technology is used on civilians.

I. BACKGROUND

Facial recognition technology uses an automated process to analyze faces captured in images and video to identify or confirm the identity of individuals. It is a form of facial analysis technology, or technology that analyzes human faces for the detection of facial attributes, such as gender, age, race, or identity.[1] Currently, one in two American adults are in a facial recognition database accessible by police.[2]

Law enforcement entities, including the Federal Bureau of Investigation (FBI) and state and local law enforcement agencies, use facial recognition for a variety of functions. The most common functions include identifying individuals during traffic stops who refuse to identify themselves; entering individual mugshots into police facial recognition databases after arrests; using images or videos to search databases to find a suspect matches; and using "real time video surveillance" to compare faces captured from a continuous surveillance feed to faces in video on a continuing basis to identify matches and alert police.[3]

---

[1] *Response: Racial and Gender Bias in Amazon Rekognition—Commercial AI System for Analyzing Faces,* Medium (Jan. 25, 2019) (online at https://medium.com/@Joy.Buolamwini/response-racial-and-gender-bias-in-amazon-rekognition-commercial-ai-system-for-analyzing-faces-a289222eeced).

[2] *The Perpetual Lineup: Unregulated Police Face Surveillance in America,* Georgetown Law Center on Privacy and Technology (Oct. 18, 2016) (online at www.perpetuallineup.org/).

[3] *Id.*

Other federal government agencies are also actively using facial recognition. Customs and Border Protection and the Transportation Security Administration are currently using facial recognition technology to confirm the identities of travelers for international air and land travel and are working to expand the program to apply to domestic travel.[4]

Private sector entities are using facial recognition technology for various commercial uses, including for advertising and for security at large stadium events.[5]

There are currently no federal regulations regarding the use of facial recognition technology for commercial or government use. On March 6, 2017, President Trump issued an executive order directing the Department of Homeland Security to expedite completion of the Entry-Exit facial recognition system.[6]

On the state and local level, San Francisco banned the use of facial recognition technology by law enforcement and other local government agencies on May 14, 2019. Similar bans are being considered in Oakland, California and Somerville, Massachusetts.[7] Other cities are expanding its use in the absence of regulation. Detroit, Chicago, Orlando, Washington, D.C., Los Angeles, West Virginia, Seattle, Dallas, and New York City have started using real-time video facial recognition, have plans to begin using the technology, or have acquired and have the capability to use the technology.[8]

II. CONSTITUTIONALITY OF GOVERNMENT USE OF FACIAL RECOGNITION TECHNOLOGY ON AMERICAN CITIZENS

The Fourth Amendment of the Constitution protects citizens from "unreasonable searches and seizures," and the First Amendment prohibits any law "abridging the freedom of speech … or the right of the people peaceably to assemble."

The bounds of these protections, as applied to government use of facial recognition technology, are untested, and the Supreme Court has not directly ruled on the constitutionality of police using facial recognition technology on citizens. However, the Supreme Court has ruled on the use of technology to aggregate data on private citizens, as discussed below.

---

[4] *See* Transportation Security Administration, *Biometrics Technology* (online at www.tsa.gov/biometrics-technology); *see also* Customs and Border Protection, *Biometrics* (online at www.cbp.gov/travel/biometrics).

[5] *San Francisco Bans Facial Recognition Technology*, New York Times (May 14, 2019) (online at www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html?module=inline).

[6] The White House, *Executive Order Protecting the Nation from Foreign Terrorist Entry Into the United States* (Mar. 6, 2017) (online at www.whitehouse.gov/presidential-actions/executive-order-protecting-nation-foreign-terrorist-entry-united-states-2/).

[7] *San Francisco Bans Facial Recognition Technology*, New York Times (May 14, 2019)(online at www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html?module=inline).

[8] *America Under Watch: Face Surveillance in the United States*, Georgetown Law Center on Privacy and Technology (online at www.americaunderwatch.com/).

A. Fourth Amendment Rights

The Fourth Amendment protects citizens from unreasonable searches of spaces that people reasonably expect to be private. The Supreme Court held in *Katz v. United States* that the "Fourth Amendment protects people, not places." The Court added: "[W]hat he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[9]

The Supreme Court has since applied this line of Fourth Amendment jurisprudence and used Justice Harlan's *Katz* concurrence—stating that persons are entitled to a "constitutionally protected reasonable expectation of privacy"—to its analysis of the protections afforded citizens from police uses of technology.[10]

In *United Sates v. Jones*, the Supreme Court signaled that digital aggregation of data could constitute a search, even if individual data points would not have been protected.[11] In *Jones*, the Court found that the government's application of a GPS device on the undercarriage of a car, which collected locational data for 28 days, comprised a search. Justice Sotomayor, in her concurrence, wrote:

> I would take these attributes of GPS monitoring into account when considering the existence of a reasonable societal expectation of privacy in the sum of one's public movements. I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on.[12]

In last summer's *Carpenter v. United States*, the Supreme Court placed further bounds on police use of emerging technologies as a Fourth Amendment intrusion upon privacy rights, in the context of records of physical movements as obtained from a third party. The government's surveillance involved access to third party records—cell phone location data—that users had willingly exposed to industry. Nonetheless, the Supreme Court found that police acquisition of such records constituted a search.[13]

The *Carpenter* Court stated:

> [C]ell-site records present even greater privacy concerns than the GPS monitoring of a vehicle we considered in *Jones*. Unlike the bugged container in *Knotts* or the car in *Jones*, a cell phone—almost a "feature of human anatomy"—tracks nearly exactly the movements of its owner.[14]

---

[9] 389 U.S. 347, 351 (1967).

[10] *Id.* at 360.

[11] 565 U.S. 400 (2012).

[12] *Id.* at 416.

[13] 138 S. Ct. 2206 (2018).

[14] *Id.* at 2218.

Facial recognition technology makes use of the human face—a feature most certainly part of the human anatomy. Taken together, it seems possible that the Supreme Court would rule that large-scale police monitoring through the use of facial recognition technology, often obtained from private third-party actors, would constitute a search.

Citizens likely have a reasonable expectation of privacy in their facial features and that their facial features will not be logged and tracked. Even though citizens often display their faces in public spaces, the quick ease of mass surveillance and aggregation of facial data, including acquisition of locational information, creates a new Constitutional calculus. As stated by the Court in *Carpenter*, "A person does not surrender all Fourth Amendment protection by venturing into the public sphere."[15]

B. Implications on First and Fourteenth Amendment Protections

Government use of facial recognition technology to identify citizens could produce a chilling effect on freedom of speech, and in turn, stifle First Amendment rights to protest and peaceably assemble. A citizen's presence at a political rally often hinges on anonymity. Though in relation to printed pamphlets, the Supreme Court has previously ruled to protect the right of citizens to exercise anonymous free speech.

In *McIntyre v. Ohio Elections Commission*, the Supreme Court banned a state law that prohibited dissemination of anonymous political pamphlets. The Court ruled that "identification of the author against her will is particularly intrusive; it reveals unmistakably the content of her thoughts on a controversial issue."[16]

The Court explained:

> Anonymity is a shield from the tyranny of the majority. It thus exemplifies the purpose behind the Bill of Rights, and of the First Amendment in particular: to protect unpopular individuals from retaliation—and their ideas from suppression—at the hand of an intolerant society.[17]

Previously, in *Talley v. California*, the Court had prohibited distribution of a pamphlet which did not have an identifying author or sponsor's name. The Court stated, "There can be no doubt that such an identification requirement would tend to restrict freedom to distribute information and thereby freedom of expression."[18]

The Court also wrote:

> [A]nonymous pamphlets, leaflets, brochures, and even books have played an important

---

[15] *Id.* at 2217.

[16] 514 U.S. 334 (1995).

[17] *Id.* at 357.

[18] 362 U.S. 60, 64 (1960).

> role in the progress of mankind. Persecuted groups and sects from time to time throughout history have been able to criticize oppressive practices and laws either anonymously or not at all.[19]

The Supreme Court has held that the Fourteenth Amendment includes a right to freedom of association. In *NAACP v. Alabama*, the Court prohibited the state of Alabama from obtaining membership lists from the NAACP. The Court stated:

> It is beyond debate that freedom to engage in association for the advancement of beliefs and ideas is an inseparable aspect of the "liberty" assured by the Due Process Clause of the Fourteenth Amendment, which embraces freedom of speech.[20]

The Court continued:

> Compelled disclosure of membership in an organization engaged in advocacy of particular beliefs is of the same order. Inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs.[21]

In practice, the ubiquitous use of facial recognition technology could amount to real-time identification of group members. In such instances, group members would be instantly identified and associated with a host of political or religious causes, effectively amounting to a state-compelled list.

In Justice Sotomayor's *Jones* concurrence, she warned of the increasing measure of surveillance facilitated by emerging technology:

> GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations. The government can store such records and efficiently mine them for information years into the future. … Awareness that the Government may be watching chills associational and expressive freedoms.[22]

III. PAST COMMITTEE WORK ON FACIAL RECOGNTION

During the 115th Congress, the Committee launched an investigation into federal law enforcement's use of facial recognition technology. During its investigation, the Government Accountability Office (GAO) issued a report in May 2016 recommending that the FBI make numerous changes to its facial recognition database to improve its data security and ensure privacy, accuracy, and transparency. In April 2019, GAO released a letter to the Department of

---

[19] *Id.*

[20] 357 U.S. 449, 460 (1958).

[21] *Id.* at 462.

[22] 565 U.S. at 415.

Justice highlighting six priority open recommendations that the FBI has yet to fully implement.[23]

On March 22, 2017, the Committee held a hearing to review federal law enforcement's uses and policies on facial recognition technology. The Committee found that 18 states have memoranda of understanding with the FBI to share their databases and that, as a result, more than half of American adults are part of facial recognition databases. It also found that facial recognition technology misidentifies women and minorities and a much higher rate than white males, increasing the risk of racial and gender bias.[24]

IV. WITNESSES

Ms. Joy Buolamwini
Founder
Algorithmic Justice League

Mr. Andrew Ferguson
Professor of Law
University of the District of Columbia David A. Clarke School of Law

Ms. Clare Garvie
Senior Associate
Center on Privacy and Technology, Georgetown University Law Center

Ms. Neema Singh Guliani
Senior Legislative Counsel
American Civil Liberties Union

Dr. Cedric Alexander
Former President
National Organization of Black Law Enforcement Executives

Staff contacts: Yvette Badu-Nimako and Gina Kim at (202) 225-5051.

---

[23] *Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy*, Government Accountability Office (May 16, 2019) (online at www.gao.gov/products/GAO-16-267); *Priority Recommendations: Department of Justice*, Government Accountability Office (Apr. 10, 2019) (online at www.gao.gov/products/GAO-19-361SP).

[24] Committee on Oversight and Government Reform, *Hearing on Committee to Review Law Enforcement's Policies on Facial Recognition Technology*, 115th Cong. (Mar. 22, 2017) (online at https://republicans-oversight.house.gov/hearing/law-enforcements-use-facial-recognition-technology/).