Congress of the United States
Washington, DC 20510

December 19, 2022

Christopher A. Wray
Director
Federal Bureau of Investigation
935 Pennsylvania Avenue, NW
Washington, D.C. 20535-0001

Dear Director Wray:

We request information regarding facial recognition technology, a powerful surveillance and analysis tool. The FBI's Facial Analysis, Comparison, and Evaluation Services Unit can identify individuals based on reference databases of hundreds of millions of photos, including all driver's license photos from over a dozen states,[1] and its Next Generation Identification-Interstate Photo System (NGI-IPS) processes thousands of facial recognition scans per month from state and local law enforcement.[2]

It is critical that Congress understands fully how the FBI uses facial recognition and how state and local law enforcement use NGI-IPS. Please send my office all FBI policy guidelines on facial recognition, training materials employed for FBI officials reviewing matches, and answers to the specific inquiries outlined below.

Facial recognition has helped identify criminal suspects who committed a serious violent crime, such as homicide. It has also been used to enforce minor offenses such as shoplifting less than $15 of goods.[3] Among our principal concerns are First Amendment issues related to the use of facial recognition. In China, facial recognition is used to identify, discourage, and detain protesters, as well as for social control by targeting minor infractions like jaywalking or removing toilet paper from public restrooms, part of China's unprecedented system of AI-powered surveillance.[4] We believe we must guard against the risk of such abuses in the United States and be vigilant against risks associated with the creep of ubiquitous facial recognition into Americans' daily lives.

[1] Clare Garvie, Alvaro Bedoya, Jonathan Frankle, Georgetown Law Center on Privacy and Technology, The Perpetual Line-Up: Unregulated Police Face Recognition in America (October 18, 2016), Appendix: Federal Bureau of Investigations, https://www.perpetuallineup.org/jurisdiction/federal-bureau-investigation.

[2] Congressional Research Service, Federal Law Enforcement Use of Facial Recognition Technology (October 27, 2020), https://sgp.fas.org/crs/misc/R46586.pdf; "November 2017 Next Generation Identification (NGI) System Fact Sheet," https://www.eff.org/files/2018/02/11/november_2017_ngi_system_fact_sheet_-_fbi.pdf.

[3] Drew Harwell, "Oregon became a testing ground for Amazon's facial-recognition policing. But what if Rekognition gets it wrong?" the *Washington Post*, April 30, 2019, https://www.washingtonpost.com/technology/2019/04/30/amazons-facial-recognition-technology-is-supercharging-local-police/?utm_term=.edb99d0f2961.

[4] Paul Mozur, "In Hong Kong Protests, Faces Become Weapons," the *New York Times*, July 26, 2019, https://www.nytimes.com/2019/07/26/technology/hong-kong-protests-facial-recognition-surveillance.html; Alfred Ng, "How China uses facial recognition to control human behavior," *CNet*, August 11, 2020, https://www.cnet.com/news/in-china-facial-recognition-public-shaming-and-control-go-hand-in-hand/.

Unfortunately, facial recognition has already been used to surveil protesters in the United States.[5] The information requested by this letter will help the American people's lawful representatives better understand how the FBI – and law enforcement agencies using the FBI's tools – are employing facial recognition technology.

Congress and the public must have a full understanding of how facial recognition is used, and what offenses and behavior it is used to investigate and monitor. Specifically, please provide:

- The full list of federal offenses that the FBI has used facial recognition to investigate and the number of times facial recognition was used for each type of offense.

- The full list of offenses for which NGI-IPS has been used by state and local police investigations and the number of times facial recognition was used for each type of offense.

The Fourth Amendment's prohibition against unreasonable searches and the relevant case law limit when, where, how, and upon whom the government may conduct surveillance. Generally, law enforcement agents must articulate some reasonable belief that a person has or is engaged in criminal activity before intensive surveillance is authorized.

- Does FBI policy require that, for use of a facial recognition system by the FBI or local law enforcement to match someone's identity with an image, the individual to be identified must be suspected of wrongdoing? If so, please specify what relevant policies exist, and what level of suspicion is required to conduct the scan for matches.

- How does the FBI oversee state and local police use of NGI-IPS to ensure that they comply with the FBI's use policies?

Powerful surveillance tools like facial recognition can present a major risk to our constitutionally protected freedoms when they are used to identify, deter, or retaliate against peaceful protesters. Unfortunately, facial recognition has already been used in this manner. In 2020, police in Fort Lauderdale, Boca Raton, and the Broward County Sheriff's Office each ran numerous facial recognition searches on the state's FACES (Face Analysis Comparison & Examination System) image matching database to identify demonstrators during peaceful protests.[6]

According to an FBI Privacy Impact Assessment, FBI policy allows state and local law enforcement to use NGI-IPS to scan and identify photos of individuals engaged in First Amendment-protected activities — such as peaceful protest — so long as doing so is "pertinent

[5] In 2015, Baltimore police used face recognition to scan demonstrators in order to find individuals with previously unenforced bench warrants for unrelated offenses and arrest them directly from the crowd. Kevin Rector and Alison Knezevich, "Social media companies rescind access to Geofeedia, which fed information to police during 2015 unrest," *Baltimore Sun*, October 11, 2016, https://www.baltimoresun.com/news/crime/bs-md-geofeedia-update-20161011-story.html.

[6] Joanne Cavanaugh Simpson and Marc Freeman, "South Florida police quietly ran facial recognition scans to identify peaceful protestors. Is that legal?" *South Florida Sun Sentinel*, June 26, 2021, https://www.sun-sentinel.com/local/broward/fl-ne-facial-recognition-protests-20210626-7sll5uuaqfbeba32rndlv3xwxi-htmlstory.html.

to and within the scope of an authorized law enforcement activity."[7] We are concerned that this standard may be insufficient to prevent abuse, especially since the mere possibility of abuse can chill Constitutionally-protected speech.

- Has NGI-IPS ever been used to identify individuals engaged in peaceful protest or other First Amendment-protected activities? If so, please document how many times this has occurred.

- Does the FBI require state and local authorities to affirm that they comply with the FBI use policies for NGI-IPS? If so, does the FBI keep records of those affirmations?

- Does the FBI keep records of each usage of NGI-IPS by state and local authorities? Does the FBI log which individual officers access the records? Is supervisor consent required for individual officers to access records?

- What, if any, measures exist to prevent state and local police from using NGI-IPS to identity individuals merely because they are engaged in peaceful protest or other First Amendment-protected activities?

The NGI-IPS Policy Implementation Guide prohibits photos from serving as the sole basis for law enforcement action. However, there are already documented cases in which individuals were wrongfully arrested based entirely on inaccurate facial recognition matches.[8]

- Has the FBI ever used a facial recognition match as the sole basis for an arrest? If so, please document how many times this has occurred.

- What mechanisms exist to ensure state and local police do not use facial recognition matches from NGI-IPS as the sole basis for an arrest?

The accuracy of facial recognition technology is a core issue law enforcement must address. A National Institute of Standards and Technology study found that women and minorities are significantly more likely to be misidentified by a facial recognition system.[9] A 2019 Government Accountability Office (GAO) report found that the FBI "conducted limited assessments of the accuracy of face recognition searches prior to accepting and deploying its face recognition system."[10]

[7] Erin M. Priest, Privacy and Civil Liberties Officer, FBI, Privacy Impact Assessment for the Next Generation Identification-Interstate Photo System (May 2019), https://www.fbi.gov/file-repository/pia-ngi-interstate-photo-system.pdf/view.

[8] Kashmir Hill, "Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match", New York Times, Jan. 6, 2021, https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html.

[9] Drew Harwell, "Federal study confirms racial bias of many facial-recognition systems, casts doubt on their expanding use," The Washington Post, December 16, 2019, https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/.

[10] Gretta L. Goodwin, "Face Recognition Technology: DOJ and FBI Have Taken Some Actions in Response to GAO Recommendations to Ensure Privacy and Accuracy, But Additional Work Remains," Government Accountability Office, June 4, 2019, https://www.gao.gov/assets/gao-19-579t.pdf.

- What, if any, steps has the FBI taken since the GAO report to better ensure the accuracy of its facial recognition capabilities?

- Has the FBI assessed the accuracy of any commercial facial recognition systems it uses? If so, what were the results? Is there data on false matches?

Under the precedent created by the Supreme Court's decision in *Brady v. Maryland*, prosecutors must, upon request, disclose to defendants any potentially exculpatory evidence that is material to either guilt or punishment.[11] Yet the results from use of facial recognition systems are often hidden from defendants.[12]

- How often has FBI use of facial recognition for its own investigations been disclosed to defendants?

- Does FBI policy require that state and local police using NGI-IPS disclose this use to defendants?

Thank you for your prompt attention to this important issue. We look forward to receiving your detailed and specific responses to each question and working with you to ensure necessary safeguards exist for law enforcement use of facial recognition.

Sincerely,

Ted W. Lieu

Ted W. Lieu
Member of Congress

Jon Ossoff
United States Senator

Yvette D. Clarke M.C.

Yvette D. Clarke
Member of Congress

[11] *Brady v. Maryland*, 373 U.S. 83 (1963).
[12] Somil Trevedi & Nathan Wessler, ”Florida Is Using Facial Recognition to Convict People Without Giving Them a Chance to Challenge the Tech”, ACLU.org, Mar. 12, 2019, https://www.aclu.org/blog/privacy-technology/surveillance-technologies/florida-using-facial-recognition-convict-people.