PROJECT ON GOVERNMENT OVERSIGHT

Attorney General Merrick Garland
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530-0001

March 10, 2021

Dear Attorney General Garland:

President Joe Biden has pledged to begin the new administration with a renewed commitment to civil rights and equity.[1]

Pervasive surveillance and indiscriminate police action are incompatible with these goals. Surveillance tools are often directed with disproportionate breadth and intensity at marginalized communities, deployed without checks to prevent abuse, and authorized absent safeguards to protect individual rights. Overbroad surveillance chills constitutionally protected activities, and can result in denial of basic dignity. These problems are at their most extreme in how they harm people of color, religious minorities, and other vulnerable communities. In addition to how it harms individuals, overbroad surveillance also engenders mistrust and undermines police-community relations.

We at the Project On Government Oversight (POGO) are committed to addressing each of these issues. POGO is a nonpartisan independent watchdog that investigates and exposes waste, corruption, abuse of power, and when the government fails to serve the public or silences those who report wrongdoing. We champion reforms to achieve a more effective, ethical, and accountable federal government that safeguards constitutional principles. The Constitution Project at POGO strives to protect individuals from improper and overbroad surveillance.

Fortunately, there is much that the Department of Justice can do to address these urgent issues regarding surveillance, both in directly improving federal law enforcement practices, as well as serving as a guide to state and local law enforcement. In order to effectively pursue President Biden's goals of advancing civil rights, civil liberties, and equity, as well as restoring faith in government, we recommend the department immediately adopt the following policy measures:

1) Require a warrant for use of face recognition

Face recognition is a powerful surveillance tool that the FBI frequently uses for its own investigations, as well as to process requests from state and local law enforcement. While this

[1] Joseph Biden, "Remarks by President Biden at Signing of an Executive Order on Racial Equity" (Speech, The White House, Washington, DC, January 26, 2021). https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/01/26/remarks-by-president-biden-at-signing-of-an-executive-order-on-racial-equity/

technology could aid select law enforcement operations, it also creates unparalleled potential for invasive surveillance. Some authoritarian regimes, like the governments of China and Russia, already use face recognition to stockpile records of individuals' daily lives and suppress vital activities such as protests and free exercise of religion.[2] But abuse is not limited to those nations: Misuse of face recognition already occurs in the United States.[3] And even absent intentional misuse, face recognition creates serious dangers. Face recognition sometimes receives too much weight in investigations despite its limits and potential for error, and use of face recognition is often hidden from defendants, who are entitled to know how it impacted their arrest.[4]

By placing reasonable restrictions on the use of face recognition technology, the federal government can simultaneously safeguard the civil liberties of the U.S. public, and provide space for the technology to become a safer and more consistent tool. Foremost among the steps needed is to enact a warrant requirement for any federal law enforcement use of face recognition, as well as to process state and local requests for face recognition scans.[5]

Because most uses of face recognition involve identifying an individual photographed during alleged commission of a crime, a warrant requirement would not undermine proper uses of this technology or impede investigations. Instead, by requiring judicial authorization and suspicion of wrongdoing, a warrant requirement would prevent mission creep and willful abuse.

2) Limit face recognition to investigation of serious offenses

Face recognition can be highly prone to error based on circumstance and manner of use, and people of color are more likely to be misidentified by this technology in the U.S. Misidentifications pose a serious threat to public safety, civil liberties, effective law enforcement operations, and police-community relations.[6] Face recognition should not be used to stockpile suspects for minor offenses—where oversight of investigations and prosecutions often receive too little scrutiny—yet police are already using face recognition to prosecute minor offenses such as shoplifting less than $15 of goods or stealing a pack of beer from a store.[7]

---

[2] Paul Mozur and Aaron Krolik, "A Surveillance Net Blankets China's Cities, Giving Police Vast Powers," *New York Times*, December 17, 2019. https://www.nytimes.com/2019/12/17/technology/china-surveillance.html; Paul Mozur, "One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority," *New York Times*, April 14, 2019. https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html; James Vincent, "Moscow rolls out live facial recognition system with an app to alert police," *Verge*, January 30, 2020. https://www.theverge.com/2020/1/30/21115119/moscow-live-facial-recognition-roll-out-ntechlab-deployment

[3] Kevin Rector and Alison Knezevich, "Social media companies rescind access to Geofeedia, which fed information to police during 2015 unrest," *The Baltimore Sun*, October 11, 2016. https://www.baltimoresun.com/news/crime/bs-md-geofeedia-update-20161011-story.html

[4] Jennifer Valentino-DeVries, "How the Police Use Facial Recognition, and Where It Falls Short," *New York Times*, January 12, 2020. https://www.nytimes.com/2020/01/12/technology/facial-recognition-police.html

[5] This rule could include commonsense exceptions, such as emergency situations where prompt action is required to prevent loss of life, and identification of victims and missing persons.

[6] Numerous reported improper arrests—all of black men—have already occurred based on faulty face recognition matches. Kashmir Hill, "Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match," *New York Times*, December 29, 2020. https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html

[7] Drew Harwell, "Oregon became a testing ground for Amazon's facial-recognition policing. But what if Rekognition gets it wrong?" *Washington Post*, April 30, 2019.

Using a pervasive surveillance technology like face recognition to respond to minor offenses could also facilitate improper selective use and selective prosecution. For example, in 2015, Baltimore police used face recognition to target demonstrators protesting the death of Freddie Gray in police custody, scanning the crowd with the technology to find and arrest anyone that had an outstanding warrant for any offense.[8]

And despite congressional inquiries, we currently have no knowledge of the set of offenses the FBI uses face recognition for in its own investigations, or in support of requests by state and local police.[9] Absent such limits, the FBI could—without even being aware of the nature of the requests—be running face recognition searches for local police investigations of low-level offenses that are selectively enforced, targeting people of color and exacerbating disparate enforcement practices. Face recognition searches could also be used as the backbone of cases where potentially erroneous matches are poorly corroborated by further investigative work prior to filing charges.

The United States has long embraced the idea that certain invasive surveillance technologies, such as wiretaps and surveillance bugs, should only be used for serious offenses. This places a check on extraordinary law enforcement powers, preventing it from being abused to selectively prosecute petty offenses, or used as a pretense for pervasive monitoring. Given the immense power of face recognition, it is fitting to limit its use in a similar manner. Setting a serious crime limit modeled after the investigating offenses listed in the Wiretap Act—and offenses centered around Uniform Crime Reporting Title 1 crimes for state and local requests—would prevent misuse, while still allowing face recognition to aid critical investigations of violent crimes.[10]

3) Require a warrant for all location tracking

A warrant requirement for electronic location tracking is a critical privacy safeguard for the digital age. Location tracking allows the government to monitor the sensitive details of Americans' lives just as intimately as if it were snooping inside your house or going through your laptop. The Supreme Court established a warrant requirement to track individuals'

---

https://www.washingtonpost.com/technology/2019/04/30/amazons-facial-recognition-technology-is-supercharging-local-police/; Ebony Bowden, "How cops used a photo of Woody Harrelson to catch a beer thief," *New York Post*, May 16, 2019. https://nypost.com/2019/05/16/how-cops-used-a-photo-of-woody-harrelson-to-catch-a-beer-thief/

[8] Kevin Rector and Alison Knezevich, "Social media companies rescind access to Geofeedia, which fed information to police during 2015 unrest," *The Baltimore Sun*, October 11, 2016. https://www.baltimoresun.com/news/crime/bs-md-geofeedia-update-20161011-story.html

[9] During a House Judiciary Committee hearing on February 5, 2020, Representative Sylvia Garcia (D-TX) asked FBI Director Christopher Wray whether the FBI could provide a list of offenses for which face recognition was used to investigate, including requests from state and local police. Director Wray responded, "I don't know that I have a list of crimes that we use it for." *Oversight of the Federal Bureau of Investigation: Hearing before the House Judiciary Committee*, 116th Cong. (February 5, 2020). https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=2780

[10] The Constitution Project at POGO's task force on face recognition created a specific category of offenses revolved around Uniform Crime Reporting Title 1 crimes to serve this specific purpose. Task Force on Facial Recognition Surveillance, Project On Government Oversight, *Facing the Future of Surveillance* (March 4, 2019). https://www.pogo.org/report/2019/03/facing-the-future-of-surveillance/

cellphones in its 2018 Carpenter v. United States decision, a critical step forward in protecting privacy rights.[11]

However, Carpenter must be treated as a starting point rather than an endpoint for location privacy. Just as the warrant requirement for wiretapping established by the Katz decision in 1967 was followed by more nuanced and extensive protections in the Wiretap Act, we need statutes and policies to build on the principles established in Carpenter.[12] The lack of agency rules and statutory limits has left major loopholes and ambiguities in how location tracking law will be applied to emerging technologies.

For example, in recent years government entities have resorted to purchasing cellphone location records from third-party brokers, essentially paying a premium to circumvent the warrant requirements in Carpenter. The FBI, Department of Homeland Security, Customs and Border Protection, the Secret Service, Immigration and Customs Enforcement, U.S. Special Operations Command, and the Defense Intelligence Agency all purchase cellphone location data that they should not be able to obtain without a warrant.[13]

Until clear statutory limits are established—a measure the administration should urge Congress to take on—these loopholes must not be left to be exploited. The Department of Justice should establish a clear policy that electronic location tracking requires a warrant and as a matter of law cannot be circumvented through means such as purchase through third-party brokers.

4) Place strict limits on location-tracking tools that impact individuals not suspected of wrongdoing

Among the especially concerning components of location surveillance are the tools and techniques that capture all data in a given area, such as cell-site simulators (also known as "IMSI catchers" and "stingrays"), geofence orders, and cell-tower dumps. These methods do not track an individual's movements, but rather collect location data from all individuals in a given area. Because these methods by nature do not have one person as a target, they sweep up innocent individuals' data and cause collateral damage to privacy. They are also particularly vulnerable to abuse: Collecting all cellphone data for a given area could allow the government to catalog groups of protesters, attendees at a religious ceremony, or patients at a health clinic.

---

[11] Carpenter v. United States, 138 S. Ct. 2206 (2018).

[12] The Supreme Court ruled that a warrant was necessary for wiretaps in Katz in 1967 (Katz v. United States, 389 U.S. 347). The following year Congress passed detailed requirements for wiretap warrants that went beyond the Katz ruling in Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (18 USC 2510 *et seq*.).

[13] Sara Morrison, "A surprising number of government agencies buy cellphone location data. Lawmakers want to know why," *Vox*, December 2, 2020. https://www.vox.com/recode/22038383/dhs-cbp-investigation-cellphone-data-brokers-venntel; Charles Levinson, "Through apps, not warrants, 'Locate X' allows federal law enforcement to track phones," *Protocol*, March 5, 2020. https://www.protocol.com/government-buying-location-data; Joseph Cox, "How the U.S. Military Buys Location Data from Ordinary Apps," *Vice*, November 16, 2020. https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x; Charlie Savage, "Intelligence Analysts Use U.S. Smartphone Location Data Without Warrants, Memo Says," *New York Times*, January 22, 2021. https://www.nytimes.com/2021/01/22/us/politics/dia-surveillance-data.html.

In 2015, the Department of Justice created a policy guidance requiring a warrant for the use of cell-site simulators.[14] However, this measure alone is not sufficient, given the collateral damage to privacy that area-focused location surveillance causes. In order to reduce the harm to individuals not suspected of wrongdoing, department policy should mandate that cell-site simulators only be permitted after exhaustion requirements are satisfied, both in terms of traditional investigative techniques as well as targeted location-tracking methods that avoid incidental collection.[15] Further, rules limiting the use of cell-site simulators should have strict minimization rules that require prompt deletion of data concerning individuals whose location information is not necessary for the relevant investigation. Finally, these rules should also apply to geofence orders and cell-tower dumps.[16]

5) Provide basic transparency on how the government interprets Fourth Amendment requirements

The Carpenter decision not only established a warrant requirement for electronic location tracking, it also significantly limited the third-party doctrine, which the executive branch has long relied on for a variety of sweeping surveillance and data-collection activities. The court stated, "The fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection."[17] A host of sensitive data—such as communications records, web browsing activities, and purchase records—might now be excluded from the third-party doctrine and entitled to greater Fourth Amendment protection from government seizure.

It is critical that the public can find out how broadly the executive branch believes the third-party doctrine applies in the wake of Carpenter, and is able to examine the legal rationale that the government deploys in making this assessment. Unfortunately, Congress's efforts to increase transparency and gain access to materials on how the department interprets Carpenter and its general impact on the third-party doctrine have not yielded critical information on how this ruling is applied.[18]

---

[14] "Policy Guidance: Use of Cell-Site Simulator Technology," Department of Justice, September 3, 2015. https://www.justice.gov/opa/file/767321/download

[15] Jake Laperruque, "Privacy After Carpenter: We Need Warrants for Real-Time Tracking and 'Electronic Exhaustion,'" Project On Government Oversight, July 2, 2018. https://www.pogo.org/analysis/2018/07/privacy-after-carpenter-we-need-warrants-for-real-time-tracking-and-electronic-exhaustion/

[16] Such rules would prevent overbroad surveillance and abuse, but would not prevent use of these techniques in the limited circumstances when they genuinely provide novel value compared to targeted electronic location tracking, such as use to identify rioters at the Capitol on January 6. Bruce Leshan, "DC residents get visits from FBI as agents track cell phones that pinged near the Capitol," *WUSA9*, January 19, 2021. https://www.wusa9.com/article/features/producers-picks/fbi-tracks-cell-phones-that-were-near-capitol-insurrection-and-riot/65-ca268165-a5c5-46a4-8b88-943a8517343a

[17] Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).

[18] *Oversight of the Foreign Intelligence Surveillance Act: Hearing before the House Judiciary Committee*, 116th Cong. (September 18, 2019). https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=2239; Letter from Senator Ron Wyden to Director of National Intelligence Daniel Coats requesting information on government interpretations of Fourth Amendment requirements, July 30, 2019. https://int.nyt.com/data/documenthelper/1528-wyden-letter-to-dni-re-215-and/6e12df714de6eb7df542/optimized/full.pdf#page=1.

The Department of Justice should release all legal memoranda and opinions on Carpenter and the third-party doctrine, and should commit to timely release of any future materials on these issues that impact department actions and policies.

6) Provide meaningful rules and limits on federal grant funding that could augment surveillance by state and local law enforcement

Federal law enforcement grants provide significant resources to state and local law enforcement to purchase and expand use of invasive surveillance tools. Any adoption of powerful surveillance tools such as face recognition, video surveillance networks, or aerial surveillance should not occur without community dialogue and engagement. And state and local law enforcement should only deploy new technologies with safeguards deemed necessary by the affected population.

Large-scale funding for such technology absent rules, limits, or even basic transparency requirements encourages rushed adoption of surveillance tools without responsible checks. Police body camera programs in dozens of major cities are funded by Department of Justice grants, yet many lack the basic policies and rules necessary for these devices to serve their intended goal of increasing accountability.[19] In Baltimore, a private donation allowed the city to adopt a massive aerial surveillance program in secret, without the knowledge or consent of the public, who strongly disapproved of the program when it was revealed.[20] Hundreds of police departments are investing in drones,[21] sweeping video surveillance networks,[22] and face recognition,[23] but these systems often lack basic safeguards to prevent misuse.[24]

It is critical that the Department of Justice treats grant funding to state and local law enforcement as tied to a responsibility to ensure proper use, and does not facilitate expanded unchecked use of surveillance tools. Federal grants should require effective safeguards if they are to be used to fund certain technologies. For example, grants should condition any use of face recognition and location tracking on the recipient's adopting limits akin to those recommended above for federal use. The Department of Justice should only fund other technologies, such as police body cameras, if police departments commit to a broad set of policies that will ensure the technologies

---

[19] "Police Body Worn Cameras: A Policy Scorecard," The Leadership Conference on Civil and Human Rights and Upturn (November 2017). https://www.bwcscorecard.org/

[20] Conor Friedersdorf, "The Sneaky Program to Spy on Baltimore From Above," *The Atlantic*, August 26, 2016. https://www.theatlantic.com/politics/archive/2016/08/the-sneaky-program-to-spy-on-baltimore-from-above/497588/; Sidney Fussell, "As Cities Curb Surveillance, Baltimore Police Took to the Air," *Wired*, November 27, 2020. https://www.wired.com/story/cities-curb-surveillance-baltimore-police-took-air/ ("The planes were grounded amid backlash from residents and civil liberties groups, who called for the immediate suspension of the program and details on what data the city had been collecting.")

[21] Jake Laperruque and David Janovsky, "These Police Drones are Watching You," Project On Government Oversight, September 25, 2018. https://www.pogo.org/analysis/2018/09/these-police-drones-are-watching-you/

[22] Jake Laperruque, "A Million Little Eyes: Building Networks for Facial Recognition Surveillance," 2018 Cato Institute Surveillance Conference, December 14, 2018. https://cdn.cato.org/archive-2018/cc-12-14-18-02.mp4

[23] 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). https://www.perpetuallineup.org

[24] Clare Garvie, "Garbage In, Garbage Out: Face Recognition on Flawed Data," Georgetown Law Center on Privacy & Technology, May 16, 2019. https://www.flawedfacedata.com/

help achieve the aim of preventing misconduct.[25] And the use of federal grants for certain novel technologies like real-time face recognition that are undeveloped and dangerously prone to error—multiple pilot programs for real-time face recognition have produced error rates over 90%—should be prohibited entirely.[26]

We look forward to the opportunity to work with you on these and other important issues to safeguard civil rights and civil liberties from overbroad surveillance.

Sincerely,

Danielle Brian
Executive Director

Jake Laperruque
Senior Counsel, The Constitution Project

CC: Dick Durbin, Chair, Senate Judiciary Committee; Charles Grassley, Ranking Member, Senate Judiciary Committee; Jerry Nadler, Chair, House Judiciary Committee; Jim Jordan, Ranking Member, House Judiciary Committee

[25] The Constitution Project Committee on Policing Reforms, The Constitution Project, *Guidelines for the Use of Body-Worn Cameras By Law Enforcement* (December 2016). https://archive.constitutionproject.org/wp-content/uploads/2016/12/BodyCamerasRptOnline.pdf

[26] Big Brother Watch, *Face Off: The Lawless Growth of Facial Recognition in UK Policing* (May 2018), 3-4. https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf