

Congress of the United States
Washington, DC 20515

June 9, 2020

The Honorable Christopher A. Wray,
Director
Federal Bureau of Investigation
935 Pennsylvania Avenue, N.W.
Washington, D.C. 20535

The Honorable Timothy Shea,
Acting Administrator
Drug Enforcement Administration
600-700 Army-Navy Drive
Arlington, Virginia 22202

General Joseph L. Lengyel,
Chief
National Guard Bureau
111 South George Mason Drive
Arlington, Virginia 22204

The Honorable Mark A. Morgan,
Acting Commissioner
Customs and Border Protection
1300 Pennsylvania Avenue, N.W.
Washington, D.C. 20229

Dear Director Wray, General Lengyel, Acting Administrator Shea, and
Acting Commissioner Morgan,

We write to you to express our deep and profound concerns that the surveillance tactics of the Federal Bureau of Investigation (FBI), the National Guard Bureau, the Drug Enforcement Administration (DEA), and Customs and Border Protection (CBP) during the recent protests across the U.S. are significantly chilling the First Amendment rights of Americans. We demand that you cease any and all surveilling of Americans engaged in peaceful protests.

George Floyd and Breonna Taylor are only the most recent cases of Black Americans who've been murdered by law enforcement officials in our country. We stand with the millions of Americans in hundreds of communities who are peacefully calling for transformational changes to better our nation by addressing the systemic racism and injustice embedded in our society.

The First Amendment protects the right of Americans to assemble and protest government actions. Further, the Fourth Amendment protects "[t]he right of the people to be secure in their persons...against unreasonable searches and seizures," a restriction that applies to the agencies you lead.

While the job of law enforcement is to protect Americans, limited actions may be necessary if a demonstration turns violent. However, this authority does not grant the agencies you lead to surveil American citizens or collect vast amounts of personal information. Recent press reports indicate that:

- the FBI and National Guard flew RC-26B aircraft equipped with infrared and electro-optical cameras over Washington, D.C. and Las Vegas;¹
- the FBI may have flown Cessna 560 aircraft equipped with 'dirtboxes,' equipment that can collect cell phone location data, over Washington, D.C.;²

- the CBP flew Predator drones that collected and disseminated live video feeds over Minneapolis, San Antonio, and Detroit;³ and
- the DEA was granted broad authority to “conduct covert surveillance” over protesters responding to the death of George Floyd.⁴

Aside from these documented examples of vast overreach of federal government surveillance in just the last 10 days, we know that federal agencies, including the ones you lead, have used other technologies to surveil Americans, such as Stingrays, which mimic cell towers to collect location, call, text, and browsing data of nearby cellular devices;⁵ facial recognition technology;⁶ and automated license plate readers.⁷

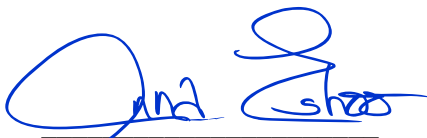
Americans have a healthy fear of government surveillance that started at the founding of our country and has continued to modern times. Polls show that seven in ten Americans believe the government surveils their phone calls and emails.⁸ In November 2019, nearly two-thirds of Americans said they were concerned about how the government collects and uses data about citizens.⁹

Government surveillance has a chilling effect. Downloads for encrypted messaging apps have spiked during recent demonstrations,¹⁰ showing a broad concern of surveillance among protesters. As further evidence of the concerns of protesters, the following headlines have appeared in popular publications or on the websites of civil society groups over the 10 days, aiming to help Americans considering protesting protect themselves:

- *Washington Post*, “Your protest is being watched. Here's how to protect your privacy”¹¹
- *Vice*, “How to Protest Without Sacrificing Your Digital Privacy”¹²
- *The Verge*, “How to secure your phone before attending a protest”¹³
- *WIRED*, “How to Protest Safely in the Age of Surveillance”¹⁴
- *Consumer Reports*, “How to Protect Phone Privacy and Security During a Protest”¹⁵
- *Electronic Frontier Foundation*, “Surveillance Self-Defense: Attending Protests in the Age of COVID-19,”¹⁶
- *Project on Government Oversight*, “How to Respond to Risk of Surveillance While Protesting”¹⁷

Americans should not have to take proactive measures to protect themselves from government surveillance before engaging in peaceful demonstration. The fact that the agencies you lead have created an environment in which such headlines are common is, in and of itself, an indication of the chilling effect of government surveillance on law-abiding Americans. For these reasons, we demand you cease surveilling peaceful protests immediately and permanently.

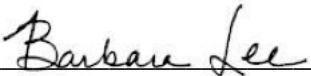
Most gratefully,



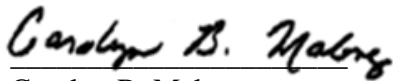
Anna G. Eshoo
Member of Congress




Bobby L. Rush
Member of Congress

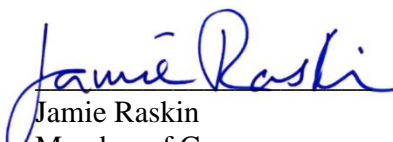

Barbara Lee
Member of Congress

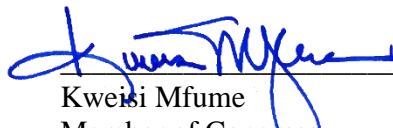

Zoe Lofgren
Member of Congress

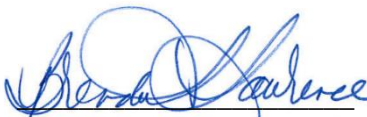

Carolyn B. Maloney
Member of Congress



Alexandria Ocasio-Cortez
Member of Congress

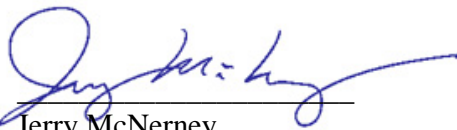

Eleanor Holmes Norton
Member of Congress

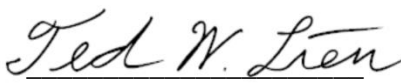

Jamie Raskin
Member of Congress

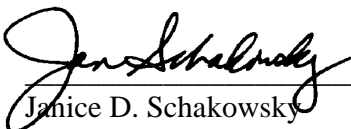

Kweisi Mfume
Member of Congress



Brenda L. Lawrence
Member of Congress


Ro Khanna
Member of Congress

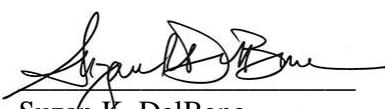

Jerry McNerney
Member of Congress


Ted W. Lieu
Member of Congress

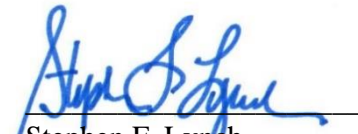

Janice D. Schakowsky
Member of Congress


Deb Haaland
Member of Congress

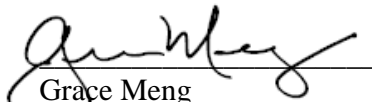

Peter Welch
Member of Congress



Suzan K. DelBene
Member of Congress



Denny Heck
Member of Congress



Stephen F. Lynch
Member of Congress



Mark Takano
Member of Congress


Grace Meng
Member of Congress

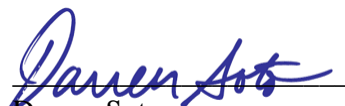

Raul M. Grijalva
Member of Congress



José E. Serrano
Member of Congress


Rashida Tlaib
Member of Congress

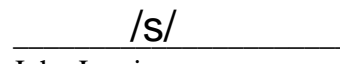

Salud O. Carbajal
Member of Congress

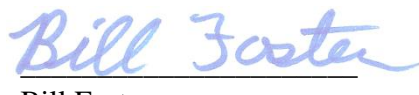

Peter A. DeFazio
Member of Congress

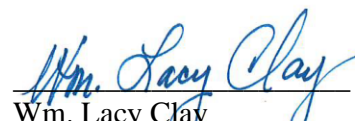

Darren Soto
Member of Congress


Michael F. Doyle
Member of Congress


Doris Matsui
Member of Congress

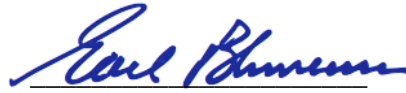

John Lewis
Member of Congress


Bill Foster
Member of Congress

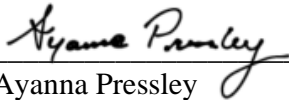

Wm. Lacy Clay
Member of Congress

/s/

Tim Ryan
Member of Congress



Earl Blumenauer
Member of Congress



Ayanna Pressley
Member of Congress

cc: The Honorable William P. Barr, Attorney General
The Honorable Mark T. Esper, Secretary of Defense
The Honorable Chad F. Wolf, Acting Secretary of Homeland Security

¹ Joseph Cox, “The Military and FBI Are Flying Surveillance Planes Over Protests,” *Vice Motherboard*, June 3, 2020, https://www.vice.com/en_us/article/y3zvwj/military-fbi-flying-surveillance-planes-george-floyd-protesters.

² *Id.*

³ Jason Koebler, Joseph Cox, and Jordan Pearson, “Customs and Border Protection Is Flying a Predator Drone Over Minneapolis,” *Vice Motherboard*, May 29, 2020, https://www.vice.com/en_us/article/5dzbe3/customs-and-border-protection-predator-drone-minneapolis-george-floyd; Joseph Cox, “The Government Is Regularly Flying Predator Drones Over American Cities,” *Vice Motherboard*, June 3, 2020, https://www.vice.com/en_us/article/n7wnzm/government-flying-predator-drones-american-cities; Zolan Kanno-Youngs and Katie Benner, “Trump Deploys the Full Might of Federal Law Enforcement to Crush Protests,” *The New York Times*, June 2, 2020, sec. U.S., <https://www.nytimes.com/2020/06/02/us/politics/trump-law-enforcement-protests.html>.

⁴ Jason Leopold and Anthony Cormier, “The DEA Has Just Been Authorized to Conduct Surveillance on Protesters,” *BuzzFeed News*, June 2, 2020, <https://www.buzzfeednews.com/article/jasonleopold/george-floyd-police-brutality-protests-government>.

⁵ “Stingray Tracking Devices: Who’s Got Them?,” November 2018, <https://www.aclu.org/issues/privacy-technology/surveillance-technologies/stingray-tracking-devices-whos-got-them>.

⁶ Ryan Mac, Caroline Haskins, and Logan McDonald, “Clearview’s Facial Recognition App Has Been Used By The Justice Department, ICE, Macy’s, Walmart, And The NBA,” *BuzzFeed News*, February 27, 2020, <https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement>.

⁷ “EPIC FOIA: Automated License Plate Readers (FBI)” (Electronic Privacy Information Center), accessed June 5, 2020, <https://epic.org/foia/fbi/lpr/>.

⁸ “Most in U.S. Say Government Could Be Monitoring Their Phone Calls, Emails” (Pew Research Center, September 27, 2017), <https://www.pewresearch.org/fact-tank/2017/09/27/most-americans-think-the-government-could-be-monitoring-their-phone-calls-and-emails/>.

⁹ Brooke Auxier et al., “Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information” (Pew Research Center, November 15, 2019), <https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/>.

¹⁰ Nicolas Rivero, “Signal App Downloads Spike as US Protesters Seek Message Encryption,” *Quartz*, June 4, 2020, <https://qz.com/1864846/signal-app-downloads-spike-as-us-protesters-seek-message-encryption/>.

¹¹ James Pace-Cornsilk and Jonathan Baran, *Your Protest Is Being Watched. Here’s How to Protect Your Privacy*. (Washington Post, 2020), https://www.washingtonpost.com/video/technology/your-protest-is-being-watched-heres-how-to-protect-your-privacy/2020/06/03/3badf963-ef49-47f9-8228-2d8bfb8c88b3_video.html.

¹² Joseph Cox and Lorenzo Franceschi-Bicchieri, “How to Protest Without Sacrificing Your Digital Privacy,” *Vice Motherboard*, June 1, 2020, https://www.vice.com/en_us/article/gv59jb/guide-protect-digital-privacy-during-protest.

¹³ Aliya Chaudhry, “How to Secure Your Phone before Attending a Protest,” *The Verge*, June 4, 2020, <https://www.theverge.com/21276979/phone-protest-demonstration-activism-digital-how-to-security-privacy>.

¹⁴ Andy Greenberg and Lily Hay Newman, “How to Protest Safely in the Age of Surveillance,” *Wired*, accessed June 5, 2020, <https://www.wired.com/story/how-to-protest-safely-surveillance-digital-privacy>.

¹⁵ Thomas Germain, “How to Protect Phone Privacy and Security During a Protest,” *Consumer Reports*, June 3, 2020, <https://www.consumerreports.org/privacy/protect-phone-privacy-security-during-a-protest/>.

¹⁶ Bill Budington, “Surveillance Self-Defense: Attending Protests in the Age of COVID-19,” *Electronic Frontier Foundation*, June 2, 2020, <https://www.eff.org/deeplinks/2020/06/surveillance-self-defense-attending-protests-age-covid-19>.

¹⁷ Jake Laperruque, “How to Respond to Risk of Surveillance While Protest,” *Project On Government Oversight*, June 4, 2020, <https://www.pogo.org/analysis/2020/06/how-to-respond-to-risk-of-surveillance-while-protesting/>.



U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535-0001

July 2, 2020

The Honorable Anna G. Eshoo
U.S. House of Representatives
Washington, D.C. 20515

Dear Representative Eshoo:

On behalf of the Federal Bureau of Investigation (FBI), this responds to your letter, dated June 9, 2020, regarding the FBI's recent efforts across the United States to prevent violence and criminal activity in protection of lawful protests. Identical responses are being sent to the co-signers of your letter.

The FBI's mission is to protect the American people and uphold the Constitution of the United States. The FBI respects and supports those who are exercising their First Amendment rights, including the right to peacefully protest. The acts of violence, potential threats to life, color of law and civil rights violations, and destruction of property that have occurred across the United States in recent weeks interfere with the rights and safety of First Amendment protected peaceful demonstrators, as well as all other citizens. The FBI is committed to identifying, apprehending, and supporting prosecutions of violent instigators who exploit legitimate, peaceful protests and engage in violations of federal law. The FBI does not conduct surveillance based solely on First Amendment protected activity. It would not be appropriate to disclose law enforcement sensitive information about specific operations, methods, and assets that can be lawfully utilized to prevent and detect criminal activity, including activity intended to disrupt the exercise of Constitutional rights.

Thank you for your support of the FBI, its mission, and its people.

Sincerely,

A handwritten signature in blue ink, appearing to read "Jill C. Tyson", is positioned above the typed name.

Jill C. Tyson
Assistant Director
Office of Congressional Affairs



**U.S. Customs and
Border Protection**

Commissioner

July 1, 2020

The Honorable Anna G. Eschoo
U.S. House of Representatives
Washington, DC 20515

Dear Representative Eschoo:

This letter is in response to your June 9, 2020 letter to U.S. Customs and Border Protection (CBP) regarding the use of CBP's unmanned aircraft system (UAS).

We share your concerns over the tragic death of Mr. George Floyd and fully support the right of Americans to peacefully demonstrate, as guaranteed by the First Amendment.

Air and Marine Operations (AMO) operates under Title 6 of U.S.C. § 211, and authorities under Public Law 116-93, which authorize the Agency to conduct aviation and maritime operations in support of federal, state, local, tribal, and international law enforcement agencies. Supporting our law enforcement partners, while ensuring the safety of all Americans, is a key mission of AMO.

On May 29, 2020, at the request of federal law enforcement on the ground in Minneapolis, Minnesota, AMO's National Air Security Operations Center-Grand Forks responded to an air support request for aerial video downlink with an UAS. The UAS flew over Minneapolis for approximately two hours, but was unable to observe activities on the ground due to cloud cover. The request was withdrawn and the UAS redirected to the northern border area for its routine patrol. AMO did not operate a UAS over Detroit, Michigan, nor San Antonio, Texas, during demonstrations in those cities.

CBP's UAS helps to enhance situational awareness and increase public and officer safety by providing aerial support to officers on the ground. Due to altitude restrictions imposed by the Federal Aviation Administration, the onboard camera cannot provide enough detail for an operator to identify a person—that is, the camera onboard CBP's UAS cannot discern physical characteristics such as height, weight, eye color, and hairstyle, nor a facial image. The imaging systems onboard these aircraft alone cannot be used to identify a person, nor collect any Personally Identifiable Information, thereby assuring a person's privacy and protecting his or her constitutional rights. The camera can only provide enough detail to identify whether an individual is carrying a long gun or wearing a backpack.

The UAS operated by AMO do not collect data on individuals. These aircraft are equipped only with cameras, radar, and other technologies to support CBP components in patrolling the border; conducting surveillance as part of a law enforcement investigation or tactical operation; and gathering raw footage that may assist in disaster relief or responses to other emergencies. AMO aircraft can provide real-time, live video feeds to ground-based law enforcement officials, giving them situational awareness; maximizing public safety; and minimizing the threat to personnel and assets. Any captured footage from the UAS cameras typically cannot be shared with other law enforcement agencies, unless it is needed for an investigation or in connection with a law enforcement activity. Even then, requests for footage must be processed and reviewed by CBP's Office of Intelligence before dissemination.

Enclosed is CBP's Privacy Impact Assessment. As authorized by law, AMO will continue to use the appropriate assets to support the efforts of federal, state, local, and tribal law enforcement in enforcing the laws of the United States.

Thank you again for sharing this important letter. Should you need additional assistance or would like to schedule a briefing, please do not hesitate to contact me or have a member of your staff contact Stephanie A. Talton, Acting Assistant Commissioner, Office of Congressional Affairs, at 202-344-1760. The co-signers of your letter will receive a separate, identical response.

Sincerely,

A handwritten signature in black ink, appearing to read "Mark A. Morgan". The signature is fluid and cursive, with the first name "Mark" and last name "Morgan" clearly distinguishable.

Mark A. Morgan
Chief Operating Officer and
Senior Official Performing the Duties of the Commissioner

Enclosure



NATIONAL GUARD BUREAU

1636 DEFENSE PENTAGON
WASHINGTON, DC 20301-1636

JUN 15 2020

The Honorable Anna Eshoo
United States House of Representatives
202 Cannon House Office Building
Washington, DC 20515

Dear Representative Eshoo:

This is an interim response to your inquiry regarding concerns over tactics used by the National Guard during the recent protests across the United States. Your important inquiry is currently under review by the National Guard Bureau. Upon completion of the review, a response will be provided addressing your concerns.

I appreciate your patience in this matter and trust this information is helpful.

Sincerely,

A handwritten signature in black ink, appearing to read "J. Lengyel", is positioned above the printed name.

Joseph L. Lengyel
General, U.S. Air Force
Chief, National Guard Bureau



Privacy Impact Assessment
for the

Aircraft Systems

DHS/CBP/PIA-018

September 9, 2013

Contact Point

Lothar Eckardt

Executive Director, National Air Security Operations

Office of Air & Marine

U.S. Customs and Border Protection

(202) 344-3950

Reviewing Official

Jonathan R. Cantor

Acting Chief Privacy Officer

Department of Homeland Security

(202) 343-1717



Abstract

The Department of Homeland Security (DHS), U.S. Customs and Border Protection (CBP) employs several types of aircraft including manned helicopters and fixed-wing aircraft, and Unmanned Aircraft Systems (UAS) for border surveillance and law enforcement purposes. These aircraft are equipped with video, radar, and/or other sensor technologies to assist CBP in patrolling the border, conducting surveillance as part of a law enforcement investigation or tactical operation, or gathering raw data that may assist in disaster relief or responses to other emergencies. Video, images, and sensor data collected through these Aircraft Systems alone cannot be used to identify a person, but they may later be associated with a person as part of a law enforcement investigation or encounter with CBP officers or agents. DHS/CBP is conducting this Privacy Impact Assessment to evaluate the privacy impact of these technologies on persons.

Introduction

The Department of Homeland Security (DHS), U.S. Customs and Border Protection (CBP) is responsible for guarding nearly 7,000 miles of land border the United States shares with Canada and Mexico and 2,000 miles of coastal waters surrounding the Florida peninsula and off the coast of Southern California. The agency also protects 95,000 miles of maritime border in partnership with the United States Coast Guard. To achieve these missions, CBP employs several types of aircraft, including manned helicopters and fixed-wing aircraft, and Unmanned Aircraft Systems (UAS) for border surveillance and law enforcement purposes. These aircraft are equipped with video, radar, and/or other sensor technologies to assist CBP in patrolling the border, conducting surveillance as part of a law enforcement investigation or tactical operation, or gathering raw data that may assist in disaster relief or other emergencies. This Privacy Impact Assessment (PIA) is necessary because the aircraft are equipped with technology that captures information that may be associated with persons whom CBP encounters.

Overview

CBP employs several types of aircraft to achieve its mission objectives. All aircraft, manned or unmanned, have some type of imaging capability such as video, still images collection, and/or radar. The UAS differ from CBP's manned aircraft only in that the pilot controls the aircraft from the ground and the aircraft are capable of flying farther distances and longer hours continuously. All aircraft are owned and operated by the Office of Air and Marine (OAM); the Office of Intelligence and Investigative Liaison (OIIL) is responsible for processing, exploitation, and dissemination (PED) of imagery transmitted from aircraft.

CBP aircraft, both manned and unmanned, are used in the following scenarios: (1) to patrol the border; (2) to conduct surveillance for investigative operations; (3) to conduct damage assessment in disaster situations; and (4) in response to officer safety scenarios. While CBP also



allocates its air assets in a manner that reflects this prioritization, CBP reviews and considers all requests for assistance. Lastly, CBP does not equip its aircraft with weapons. While the crew in all manned aircraft and the officers and agents onboard the aircraft during tactical missions do carry weapons, the various aircraft are not equipped with armaments.

Helicopters

CBP operates several types of manned rotary-wing aircraft (helicopters) in support of its mission, notably, the American Eurocopter AS-350, Augusta Westland AW-139, Bell Huey UH-1, and Sikorsky UH-60. CBP uses helicopters for observation, for tracking suspects and supporting ground units, aerial reconnaissance of moving objects and persons, external lift capability for seizures and equipment delivery, and tactical support and transportation for law enforcement activities. Areas of operation include the border environment, both land and sea, to observe and interdict unlawful crossings of persons and goods, the airspace surrounding defined DHS National Special Security Events or critical venues, and populated or unpopulated areas that are the subject of defined law enforcement activity or investigation. CBP's helicopter fleet operates out of 30 locations maintained by OAM across the United States.

Fixed-wing Aircraft

CBP has manned fixed-wing P-3 AEW/LRT Orion aircraft operating out of specific operations centers in Corpus Christi, TX and Jacksonville, FL. CBP practices a defense in depth strategy of the borders of the United States and in active prosecution of attempts to smuggle persons or contraband by extending surveillance over international and coastal waters. As part of this strategy and as a means of integrating with the overall U.S. Government strategy to interdict the flow of narcotics and controlled substances across the U.S. southern borders, this defense in depth includes expanding the area of patrol to include the Caribbean and Eastern Pacific waters that border Source and Transit Zone countries.¹ Together the operations centers operate the P-3 aircraft primarily in Central and South America. Certain P-3s are used to intercept and track both aircraft and vessels for hours at a time while maintaining a covert standoff. CBP also operates several smaller, manned, fixed-wing aircraft out of OAM operational locations. These fixed-wing aircraft include piston-engine propeller-powered aircraft (Cessna models), larger turbo-prop powered aircraft (Bombardier Dash Eight, Pilatus, and Beechcraft Super King Air), and jet aircraft (Cessna Citation). These aircraft variously perform surveillance, tracking, interdiction, intercept, and information gathering roles. Fixed-Wing Aircraft employ various types of sensor technology including video, still, and radar images, and Law Enforcement Technical Collection (LETC) (electronic signals information across the electromagnetic spectrum).

¹ Source and Transit Zone countries are those nations working in partnership with the United States to interdict the flow of narcotics and controlled substances to the United States through the Caribbean Basin and along the coastal waters of the eastern Pacific Ocean. <http://www.whitehouse.gov/ondcp/transit-zone-operations>.



UAS

A UAS encompasses an unmanned aircraft, digital network, and personnel on the ground who operate the aircraft. CBP currently owns and operates ten such aircraft. The UAS aircraft include the Predator B² and the maritime variant of the Predator B, the Guardian, which allows CBP to conduct missions in areas that are remote, too rugged for ground access, or otherwise considered too high-risk for manned aircraft or personnel on the ground. The aircraft are stationed and principally controlled at four locations: Sierra Vista, AZ (4 aircraft); Grand Forks, ND (2 aircraft); Corpus Christi, TX (2 aircraft); and Cape Canaveral, FL (2 aircraft). CBP's UAS operate in accordance within the Federal Aviation Administration (FAA) Certificate of Authorization (COA) process. CBP works with the FAA to develop the COAs to define airspace for UAS operation. Consistent with the primary mission for the UAS, these COAs, which are in effect for a period of two years, define airspace (altitude, latitude, and longitude (geography)) along the border and outside of urban areas to support CBP UAS flight operations. As the FAA develops its roadmap to integrate UAS into the National Airspace System (NAS)³, CBP will adjust to these new requirements and continue to employ UAS in pursuit of its primary border security mission.

Uses of Aircraft

Patrol

CBP uses all of its aircraft to patrol different parts of the border based on the specific strengths of the different aircraft. CBP P-3s patrol in a 42-million square mile area of the Western Caribbean and Eastern Pacific, known as the Source and Transit Zone, in search of drugs that are in transit towards U.S. shores. The P-3's distinctive detection capabilities allow highly-trained crews to identify emerging threats well beyond U.S. land borders. By providing surveillance of known air, land, and maritime smuggling routes in an area that is twice the size of the continental U.S., the P-3s detect, monitor, and disrupt smuggling activities before they reach shore.⁴ As part of this patrol responsibility, images and radar information obtained in detecting, monitoring, or supporting activities is collected and maintained either for direct case support or to permit historical trend analysis regarding smuggling routes.

Along both the northern and southern borders CBP also employs UAS and smaller manned aircraft to help agents detect, identify, apprehend, and remove individuals and

² The General Atomics Aeronautical Systems MQ-9 Predator B is a mid-size Unmanned Aerial Vehicle (UAV) approximately thirty-six feet in length, with a maximum gross weight of 10,500 pounds and a wing span of sixty-six feet.

³ See, *FAA Modernization and Reform Act of 2012*, Pub. L. No. 112-95, sec. 331, 126 Stat. 11, 72, which mandates that the FAA prepare a roadmap to integrate UAS into the NAS by 2015.

⁴ The Anti-Drug Abuse Act of 1988 established the Office of National Drug Control Policy (ONDCP) to set priorities, implement a national strategy, and certify Federal drug-control budgets. Interdiction of the flow of illicit drugs through the Source and Transit Zone is a critical component of the National Drug Control Strategy prepared annually by ONDCP.



contraband illegally entering the United States at and between Ports of Entry (POE). The COA defined airspace establishes operational corridors for UAS activity both along and within 100 miles of the border for the northern border, and along and within 25 to 60 miles of the border for the southern border, exclusive of urban areas. CBP helicopters and manned fixed-wing aircraft may operate in and around urban areas; however, the principal mission remains focused on those areas between the POE. Images, LETC, and radar information, specifically with respect to border areas between the POEs, are collected in support of case development or to permit trend analysis.

Following a flight, the images are provided to OIIL for processing, exploitation, and dissemination. Subsequently, and only upon request, OIIL provides access to the forensic analysis of a particular image and area to authorized persons who have a “need to know;” when the dissemination is in response to a particular law enforcement activity or case, that analysis may include PII.

Persons who are apprehended and who were video recorded from a UAS or a manned aircraft may have the video of their crossing and/or apprehension associated with a case file that contains their PII.

Separately, CBP also deploys manned fixed-wing aircraft with LETC sensors over the border area in support of its counter-terrorism and interdiction of smuggling operations. The LETC sensors permit surveillance of the electromagnetic spectrum for the purpose of identifying organized border crossing activity between the ports of entry.

Investigative Operations

CBP uses both UAS and manned aircraft in support of other DHS components, such as U.S. Immigration and Enforcement (ICE), or other federal law enforcement agencies, such as the Federal Bureau of Investigation (FBI) or Drug Enforcement Agency (DEA). Requests for aircraft support that are related to the border surveillance must be directed to the Assistant Commissioner, OIIL, for authorization. Each request for information follows a standard process and is reviewed and considered in terms of the requesting agencies’ authorities to receive the sought after information, CBP’s own authority to lend assistance, and CBP’s ability to integrate the information collection into its mission. Separately, OAM must determine the availability of aircraft type and the integration of the requested activity into its flight operations.

Typical support missions include overhead observation of previously identified persons, specified locations, and particular conveyances for enhanced situational awareness and increased officer safety. For example, the UAS could conduct surveillance over a building to inform ground units of the general external layout of the building or provide the location of vehicles or individuals outside the building. When flying a UAS in support of another component or government agency for an investigative operation, CBP may provide the other agency with a direct video feed through access controls or with a downloaded video recording of the operation,



in whole or in part, based on the request. Similarly, CBP may deploy a helicopter or manned fixed-wing aircraft to provide over top visibility into a developing incident. Video images from the Electrical Optical/Infrared ball (EO/IR) ball are fed through the DHS firewall to “Big Pipe,” a video and image distribution network operating within the CBP/DHS firewall, to identified users, analysts, and decision makers for real-time mission support and border protection.

Disasters

The P-3 may be used to conduct reconnaissance missions during natural disasters in support of FEMA. During these missions, P-3s can provide near real-time, high quality video of affected areas to first responders and FEMA. P-3s are equipped with similarly capable EO/IR Ball cameras; the images are also fed through a transmission to a ground station where the video is decrypted and fed to Big Pipe to disseminate inside the DHS firewall to authorized users within DHS and any other requesting agency.

UAS may also be used outside existing COAs during natural disasters once the government has issued a disaster declaration. For example, the UAS may fly missions in support of other government agencies such as the National Oceanic and Atmospheric Administration (NOAA) or FEMA to provide video or radar images of flooding. In disaster situations, CBP works with the FAA to construct a COA defining the airspace where a CBP UAS may operate. The UAS may provide a real-time feed during flight through Big Pipe or, subsequently, an analyzed image comparing the raw feed to an image with identified details, noting changes, to FEMA, state emergency operations centers, United States Geological Survey (USGS), and/or the Army Corps of Engineers. Video from these operations are not used to identify individuals. As with other requests for support, disaster area overflight requests are assigned in accordance with the national policy regarding the tasking of CBP air assets.

Officer Safety and Support to State and Local Law Enforcement

State and local law enforcement officials may request aircraft support (e.g., UH-60, P-3, UAS) in emergency situations; often this involves circumstances when officer safety is implicated, and in which aerial surveillance is necessary or the terrain would be too difficult for law enforcement personnel to navigate. OIIL reviews each request to determine whether to respond and OAM reviews how and in what context it may respond. Based on both organizations within CBP, a decision is made whether to provide assistance. Access to video taken during emergency situations may be provided, either at a DHS/CBP facility or by temporarily granting direct access through the DHS firewall. Sharing of this information with state, local, or other government agencies is on a case by case basis as determined through CBP’s Request for Information process.

As in the mission uses discussed above, UAS and manned aircraft offer several options for deploying information gathering equipment. The UAS can serve as force multiplier insofar as the UAS enables the monitoring of large areas of land more efficiently and with fewer



personnel than other aviation assets. UAS can enhance situational awareness and increase officer safety by providing aerial support to officers on the ground by monitoring a fixed location while flying at a high altitude to reduce the likelihood of detection. Manned aircraft offer the ability to fly in more congested airspace and to transport officers, agents, equipment, and seized assets.

Technology on Board the Aircraft

The various aircraft have different types of surveillance technology. Most aircraft, manned and unmanned have an EO/IR ball attached to provide a means of collecting information. The EO/IR ball installed on the UAS also assists the pilot during take-off and landing. While the cameras on each aircraft are not identical, they have almost identical performance specifications. The EO/IR ball is a camera, which employs a fixed-focus lens, that is capable of providing video at any altitude and allows operators, using digital zooming (software based image enhancement), to take small-scale aerial video images of buildings, vehicles, and people. Aircraft altitude directly affects a fixed-focus camera's performance; the higher the aircraft's altitude, the less detail an operator is able to see.

A lower altitude permits the EO/IR ball to provide greater detail in an image, which may permit identification; this observation activity, however, does not occur unnoticed or subject to attempts at evasion, and therefore is more often part of a defined law enforcement operation. Persons are often successful at hiding their identity from known surveillance aircraft by simply looking away.

At present, the flight and mission parameters for the UAS place their operation within an altitude block of 19,000 to 28,000 feet, thereby effectively limiting the altitude for the EO/IR ball on a UAS to a minimum of 19,000 feet. At this minimum altitude, the camera does not provide enough detail for an operator to identify a person (that is to discern physical characteristics such as height, weight, eye color, hair style, or a facial image). The camera operator may have enough detail to identify whether an individual is carrying a long gun or wearing a back pack. At an altitude of 19,000 feet the camera operator cannot read a license plate, nor are license plate readers effective.

Conversely, the flight parameters for helicopters and fixed-wing aircraft are broader in terms of altitude and geography; their flight operations are integrated into the NAS and do not require a COA. The mission parameters and physical capabilities for helicopters and manned fixed-wing aircraft, however, place different operational restrictions upon the aircraft.

The EO/IR ball can provide daytime or nighttime visual video observation of movement or objects on the ground. The images, depending upon the aircraft deploying the camera, tend to be small in scale, to provide environmental context. A principal purpose for tracking a person or vehicle from an aircraft with an EO/IR ball is to assist CBP or law enforcement personnel on the ground with information to permit a safe encounter—this requires environmental context more



than a best possible close-up of a face. When viewing vehicles, an operator can distinguish a car from a truck, and depending on the altitude at which the aircraft is flying, may be able to identify the model of the vehicle. During daytime flights, an operator may also be able to determine the color of the vehicle. The images of vehicles and/or individuals recorded by the EO/IR ball are not associated with any biographical information unless the individual is apprehended, at which point the video may be associated with the Personally Identifiable Information (PII) contained within the individual's case file.

In addition to EO/IR CBP deploys a UAS stationed along the Southwestern border in Sierra Vista, AZ, with the Wide Area Surveillance System (WASS). WASS uses a sensor mounted to the wing of a UAS to sweep large areas of border territory (approximately six kilometers in width) as the aircraft moves along its flight path. WASS alerts CBP to the existence of persons and/or vehicles along the border and provides coordinates to determine their location. The UAS pilot and sensor operator can then inform ground units of the location so that Border Patrol may coordinate an interdiction of the persons or vehicles. WASS provides a radar sensor image, which CBP may share through Big Pipe during operation.

Some manned and unmanned aircraft are also equipped with synthetic aperture radar that can provide black and white images in all weather. This radar can provide silhouettes of people and vehicles, but provides no identifying details. Using this technology, an operator is not able to pick up identifying characteristics of a person or a vehicle. The synthetic aperture radar is primarily used for change detection. For example, the operator can identify tire tracks on the ground that were not present in prior images provided by the radar. Similarly, an operator can use the synthetic aperture radar to determine the extent of flooding in a particular region by noting the changes to the topography.

Certain manned fixed-wing aircraft deploy LETC sensors used to detect electronic signals in the electromagnetic spectrum. These specifically designed aircraft operate in support of counter-terrorism efforts and to interdict organized smuggling (people, contraband, and controlled substances) operations within the border area. Like with the EO/IR ball, information from LETC sensors may be employed to support officers and agents on the ground as they move to a position where they can safely encounter observed persons. LETC aircraft sensors are solely deployed on manned fixed-wing aircraft.

Data on the digital video recorders on CBP aircraft are maintained for a maximum of 30 days and then overwritten by new data. The images and related data from CBP aircraft, both manned and unmanned, are provided through Big Pipe to identified users, analysts, and decision makers for real-time mission support and border protection. Images from the EO/IR ball mounted on the UAS are sent by an encrypted transmission, first to the satellite providing the control signals, and then, again by encrypted transmission, to the ground control station where the pilot and sensor operator are located. The image data is decrypted and brought inside the



DHS firewall at the ground control station, where Big Pipe can ingest the data and provide a feed to assigned users and analysts.

Big Pipe is a fully distributed network hosted by CBP and supports not only event-based law enforcement missions, but also FEMA's National Response Framework.⁵ Big Pipe employs role-based access controls to provide users possessing a need to know access to distinct video feeds at command centers, other CBP/DHS locations, and for authorized persons with technical access through the DHS firewall. OAM retains control over defining users for Big Pipe and assigning access. After the creation of live mission data, Big Pipe manages the transmission, processing, distribution, consumption, and storage of the live mission data. Big Pipe archives selective mission data on a Big Pipe server hard drive for a maximum of 7 days, after which the data is deleted. Big Pipe does not use PII to retrieve stored mission data. Stored data is retrieved based on the date and time of the mission and only by authorized users on a need to know basis. If data is used for investigative purposes, and associated with a particular individual it goes into a case management system, which is covered by the corresponding Privacy Act System of Records Notice (SORN) for the case management system. Big Pipe, separately, provides a feed of video and radar images from UAS to the Air and Marine Operations Center (AMOC), where OIIL operates one of several PED cells to review this data over time to perform trend analysis and change detection. Video and radar images maintained by a PED cell, such as at the AMOC, are stored on a separate server dedicated to the PED cell mission for up to five years. The analyzed images may be shared by OIIL in response to law enforcement needs.

Summary of Privacy Risks

The use of these aircraft and accompanying surveillance technologies presents several privacy concerns. The first concern is ensuring that CBP's collection and use of data from aerial surveillance remains within the scope of its authorities to protect the border and provide support for law enforcement activities, while continuing to preserve a person's right to privacy. CBP's border security mission has a broad mandate to determine the admissibility of persons and ensure that goods are not introduced into the United States contrary to law.⁶ Similarly, the statutory language in CBP's annual appropriations directs CBP Air and Marine to provide integrated and coordinated border interdiction and law enforcement support for homeland security missions, including assistance to federal, state, and local agencies and emergency humanitarian efforts; to provide airspace security for high-risk areas or National Special Security Events⁷; and to combat

⁵ The National Response Framework is a DHS/FEMA led effort, which provides the guiding principles that establish a comprehensive, national, all-hazards approach to domestic incident response—from the smallest incident to the largest catastrophe. <http://www.fema.gov/pdf/emergency/nrf/nrf-core.pdf>.

⁶ Title 8, United States Code (U.S.C.), sections 1225, 1357, other pertinent provisions of the immigration laws and regulations; 19 U.S.C. §§ 482, 507, 1461, 1496, 1581, 1582, 1595a(d), and other pertinent provisions of customs laws and regulations.

⁷ See Title 18 U.S.C. Section 3056, which authorizes the designation of National Special Security Events.



efforts to smuggle narcotics and other contraband into the United States⁸. Deploying OAM's various air assets to support these missions improves DHS/CBP's capability to obtain streaming video, and to assess critical infrastructure before and after events.

CBP's use of manned and unmanned aircraft to conduct aerial observations is consistent with CBP's authorities and obligations. To the extent that aircraft flying in support of tactical operations overfly private residences, there is a minimal risk that a person's privacy might be unintentionally violated. The images captured are not personally identifiable without further investigative information. Neither manned nor unmanned aircraft physically intrude upon or disturb the use of private property. Further, the cameras deployed on UAS or manned aircraft do not have the capability to see through walls or otherwise collect information regarding what occurs in the interior of a building, nor is that their purpose. UAS operate primarily at an altitude between 19,000 and 28,000 feet pursuant to their COA approved by the FAA, and are focused as previously described.

A second privacy concern, specific to UAS, is that they present a perceived risk to privacy because they are able to fly for longer hours than manned aircraft and conduct surveillance undetected. Like other aircraft, UAS are useful for monitoring remote land border areas where patrols cannot easily travel and infrastructure is difficult or impossible to build. Unlike manned aircraft, UAS are operated by personnel on the ground, allowing the crew to be relieved while the UAS is still in the air. This capability allows UAS to provide long-range surveillance for greater lengths of time than manned aircraft. Because of their small size compared to manned aircraft, and the altitude at which UAS can operate, these physical attributes may serve to conceal the presence of a UAS and reduce detection of their operating noise while still being able to maneuver over a small area and provide surveillance. Other OAM operated long range fixed-wing aircraft cannot steadily monitor a set location because of their size and turning radius. Helicopters are more easily detected because of their noise and lower operational altitudes. This means that, unlike fixed-wing aircraft and helicopters, UAS can monitor either a moving target or a fixed location for relatively longer periods of time without the likelihood of detection.

While UAS can fly for longer periods of time, they are equipped with the same technology to conduct surveillance that is presently deployed on CBP manned aircraft. The only sensor available on UAS that is not used by CBP manned aircraft currently is the WASS sensor. The WASS sensor can only detect the presence of a person and track his or her movements (much the same way other radar technology can detect an object and track its movement); it cannot be used to identify a person. The WASS sensor is designed to sweep large areas of land and is only used to patrol along the southwest border and to assist with interdictions. Other technologies on the UAS are shared by CBP's manned aircraft. Putting these technologies on a

⁸ See National Drug Control Strategy, <http://www.whitehouse.gov/ondcp/2013-national-drug-control-strategy>.



UAS only enhances CBP's ability to perform its existing functions. For instance, CBP's surveillance video of a location used to smuggle persons or contraband using a UAS instead of a P-3 may be longer in duration with less interruption and less likelihood of detection.

To mitigate the risk presented by longer sustained surveillance of an individual or residence without the individual's knowledge, CBP has strict mission priorities for UAS and all aircraft operations. For instance, CBP aircraft may only be used in support of an authorized mission or investigation, the video or other data collected from CBP aircraft may only be accessed by authorized personnel with an authorized need to know, and the CBP-held video or other data is controlled through chains of custody and stored in secure locations until it is destroyed. In addition, the FAA requires CBP to construct a COA, in the instance of deploying a UAS, for a duration determined by the investigative activity or emergency circumstance, before conducting an operation away from the border and already established COAs.

The third privacy concern, unique to UAS, pertains to the security of the system itself and the potential for hijacking of the unmanned aircraft. CBP has taken several steps to protect UAS against potential hackers. All UAS are controlled and monitored at all times by operators in ground control stations using satellite communication that is relayed through an encrypted data feed. The ability to interfere with such an encrypted data feed requires disrupting the signal from satellite to UAS, for the purpose of acquiring the data feed or controlling the UAS. In the event that the ground control station loses its ability to control the UAS, another ground control station can pick up control of that UAS. The UAS use redundant navigation systems and GPS receivers so that if a signal is lost or someone attempts to override the signal, the UAS relies on these other systems and the GPS receivers for flight operations. In order to protect the airspace, the FAA is notified immediately if a UAS loses its signal. Furthermore, if communication between ground control and the UAS is ever interrupted or lost, the UAS are pre-programmed to fly to a pre-coordinated point in a remote location to orbit while waiting for the signal to be reestablished, or to continue to orbit this Flight Termination Point until the aircraft runs out of fuel and crashes.

Because of the unique privacy concerns raised by CBP's use of Aircraft Systems, CBP has conducted this PIA to evaluate the privacy risks associated with the use of Aircraft Systems and to enhance public understanding of the authorities, policies, procedures, and privacy controls related to that use.

Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974 articulates concepts of how the Federal government should treat individuals and their information and imposes duties upon Federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information. Section 222(2) of the Homeland Security Act of 2002 states that the Chief Privacy Officer shall assure



that information is handled in full compliance with the fair information practices as set out in the Privacy Act of 1974.

In response to this obligation, the DHS Privacy Office developed a set of Fair Information Practice Principles (FIPPs) from the underlying concepts of the Privacy Act to encompass the full breadth and diversity of the information and interactions of DHS.⁹ The FIPPs account for the nature and purpose of the information being collected in relation to DHS's mission to preserve, protect, and secure.

DHS conducts Privacy Impact Assessments on both programs and information technology systems, pursuant to the E-Government Act of 2002, Section 208, and the Homeland Security Act of 2002, Section 222. Given that Aircraft Systems and their associated devices are mechanical and operational systems rather than a distinct information technology system or collection of records pertaining to an individual that would be subject to the parameters of the Privacy Act, this PIA is conducted to relate the use of these observation and data collection platforms to the DHS construct of the FIPPs. This PIA examines the privacy impact of Aircraft Systems operations as it relates to the DHS FIPPs.

1. Principle of Transparency

Principle: DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of PII. Technologies or systems using PII must be described in a SORN and PIA, as appropriate. There should be no system the existence of which is a secret.

This PIA provides a level of transparency to the public about the current surveillance programs undertaken by CBP. The video, still images, signals information, and/or radar images do not clearly identify individuals. The only information about individuals that is collected and/or retained is the indication of a human form. These images, however, may be associated with a person if the person is apprehended. For example, video collected by an EO/IR ball may show several individuals traversing the land border and being intercepted by officers or agents of CBP. While the video resolution or radar mapping images are not sufficiently precise to permit actual identification, the circumstances of CBP interdiction and apprehension of a suspect in conjunction with the aerial surveillance are sufficient to link the indistinct images of persons traversing the ground to the case file. Individuals who are apprehended by CBP as a result of observation by aircraft at or near the border may have video of their crossing and apprehension associated with their enforcement case file. CBP obtains biographical data pertaining to the apprehended person at the moment of apprehension. CBP stores all biographical information

⁹ DHS Privacy Policy Guidance Memorandum 2008-01, *The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security*, December 29, 2008.



obtained from apprehended individuals and any video or radar images of their movement obtained from the aircraft in the appropriate law enforcement case management system.

When CBP associates video, still images, signals information, and/or radar images with an individual after apprehension, that information becomes subject to the requirements of the Privacy Act in the same manner and to the same extent that the apprehension of the individual becomes a record in a Privacy Act system. The Privacy Act requires that agencies publish a SORN in the Federal Register describing the nature, purpose, maintenance, use, and sharing of the information. This PIA serves as notice to the public that information captured by Aircraft Systems may become subject to the Privacy Act once it is associated with an individual.¹⁰ Additionally, the video images associated with an individual's case file are covered by the appropriate law enforcement case management SORN, which maintains the case file. CBP will periodically re-assess the means by which the images from the aircraft are retrieved to determine whether the requirement for a SORN is triggered.

2. Principle of Individual Participation

Principle: DHS should involve the individual in the process of using PII. DHS should, to the extent practical, seek individual consent for the collection, use, dissemination, and maintenance of PII and should provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.

Individual participation provides complementary benefits for the public and the government. The government is able to maintain the most accurate information about the public, and the public is given greater access to the amount and uses of the information maintained by the government. A traditional approach to individual participation is not always practical or possible for CBP, which has law enforcement and national security missions. Aircraft are primarily used to sweep the border area to locate individuals who are crossing the border illegally. Allowing an individual to consent to the collection, use, dissemination, and maintenance of video, still images, and/or radar images would compromise operations and would interfere with the U.S. government's ability to protect its borders, thereby lessening overall homeland security.

Individuals do not have the opportunity to restrict CBP's ability to collect information in the public sphere. Any information associated with an individual is part of a case file that is created as part of a law enforcement investigation or encounter.¹¹ Providing individuals of interest access to information about them in the context of a pending law enforcement

¹⁰ For example, video information from an aircraft of an apprehension of a person at the border that is identified to that person would be referenced in the case notes pertaining to that person's apprehension in TECS (DHS/CBP – 011 TECS System of Records Notice December 19, 2008 73 FR 77778)

¹¹ CBP also incorporates images from surveillance or encounters into reports and analyses maintained in the Analytical Framework for Intelligence (AFI) (DHS/CBP – 017 System of Records June 7, 2012 77 FR 13813).



investigation may alert them to or otherwise compromise the investigation. Consequently, there is no mechanism for correction or redress for the video collected by the aircraft. Once that video is associated with an individual's case file, the individual must follow the procedure outlined in the corresponding privacy documents for that system. While individuals cannot participate in the initial collection of this information, they may contest or seek redress through any resulting proceedings brought against them. More information on redress is provided below.

3. Principle of Purpose Specification

Principle: *DHS should specifically articulate the authority which permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.*

The purpose specification principle requires DHS to 1) articulate the authority to retain the PII in question; and 2) articulate the purpose(s) for which DHS uses the PII.

CBP is authorized to collect video, other images, signals information, and data using aircraft in support of its border security mission and pursuant to the appropriations language mandating support for law enforcement as part of the mission of CBP Air and Marine.¹² Together, these authorities allow CBP to obtain information in support of border interdiction of narcotics and other contraband, the prevention of the illegal entry of aliens into the United States, the security of airspace for high-risk areas or National Special Security Events, and in support of federal, state, and local law enforcement, counterterrorism, and emergency humanitarian efforts.

CBP may use video, still images, signals information, and/or radar images, obtained from aircraft, to apprehend individuals and to provide evidence of an illegal border crossing or other violation of law. Consistent with applicable laws and SORNs, the information may be shared with other state, local, federal, tribal, and foreign law enforcement agencies in furtherance of enforcement of their laws.¹³

Video, still images, and/or radar images collected during investigative operations as part of a law enforcement investigation are used for enhanced situational awareness and increased officer safety, and may be used to provide evidence of a violation of law. These images are maintained in association with the investigative or case file that they support; their retention is managed by the same SORN and follows the handling of the investigative or case file.

¹² See, e.g., H.R. REP. No. 112-91, at 46 (2011) stating "CBP Air and marine provides integrated and coordinated border interdiction and law enforcement support for homeland security missions; provides airspace security for high risk areas or National Special Security Events upon request; and combats efforts to smuggle narcotics and other contraband into the United States. CBP Air and Marine also support counterterrorism efforts of many other law enforcement agencies."

¹³ See Consolidated Appropriations Act of 2012, Pub. L. No. 112-74 (2011), providing for "the interdiction of narcotics and other goods; the provision of support to Federal, State, and local agencies in the enforcement or administration of laws enforced by the Department of Homeland Security; and at the discretion of the Secretary of Homeland Security, the provision of assistance to Federal, State, and local agencies in other law enforcement and emergency humanitarian efforts...."



Video, still images, and/or images collected in natural disaster and/or emergency situations are used for relief work and disaster reconnaissance. CBP typically provides a direct feed of the video captured by aircraft in these scenarios to provide support to FEMA or state emergency operating centers. Video, still images, and/or radar images are not associated with an individual and are only used to indicate where an individual or group of individuals may be for emergency response purposes.

4. Principle of Data Minimization

Principle: DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s). PII should be disposed of in accordance with DHS records disposition schedules as approved by the National Archives and Records Administration (NARA).

CBP seeks to minimize the collection and retention of video, signals information, and radar to that which is necessary and relevant to carry out CBP's mission. Accordingly, when aircraft are flown to patrol the border, they are authorized to fly the designated border surveillance mission area to ensure they are only capturing images and information necessary to detect, identify, apprehend, and remove persons and their possessions illegally entering the United States at and between POE. When aircraft are flown for investigative operations, officer safety incidents, or natural disaster reconnaissance, CBP approves and defines the specific mission that is authorized, and in the case of UAS, works with the FAA to construct a COA to establish airspace for that specific UAS operation. The video (that has not been associated with a case) remains on the digital video recorder originally used for recording until it over-written through re-use, which is after approximately 30 days.

After the creation of live mission data, Big Pipe manages the transmission, processing, distribution, consumption, and storage of the live mission data. Big Pipe archives selective mission data on a Big Pipe server hard drive for a maximum of 7 days, after which the data is deleted. Big Pipe does not use PII to retrieve stored mission data.

The information collected by the aircraft is not subject to the Privacy Act unless it is retrieved by using an individual's name or other unique identifier. If an individual is apprehended by CBP as a result of observation by aircraft or subsequent association from the presence of CBP assets, CBP may have video of that individual's apprehension associated with his or her enforcement case file. That video is retained according to the retention schedule of the SORN of the corresponding case management system. Video and Radar images obtained from UAS patrols of the border are also provided to PED cells operated by OIIL for use in analyses and intelligence products concerning historical, change detection (e.g., natural and man-made alterations to geography) along the border, and patterns of movement of persons across the border. This unassociated data, in conjunction with meta-data (such as latitude, longitude, date and time of the imagery) is retained for a maximum of five years.



5. Principle of Use Limitation

Principle: *DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected.*

CBP only collects video and/or radar images, and signals information via aircraft pursuant to its law enforcement authority, as part of its border security mission, or when flying a mission in support of another agency, and when that other agency's authority covers the mission either through delegation of authority or direct control of the information collected. For example, CBP has provided support to the U.S. Forest Service in response to large scale wild fires to permit an overview of the extent and scale of the fire and identification of hot spots; this activity is pursuant to a request from the Forest Service, is performed pursuant to their authority, and the images are conveyed through designated access to the Big Pipe video distribution service. While the video resolution, radar mapping images, and signals information are not sufficiently precise to permit actual identification of a person, the images or information may be associated with an individual from context within the image, circumstances surrounding the activity occurring in the image, or additional information obtained directly from the person by an officer or agent. The images or information are only associated with an individual if the individual is apprehended or if the images are taken as part of an ongoing law enforcement investigation. Accordingly the data can only be used for the purposes specified in section 3 of this PIA.

CBP has procedures and processes in place for sharing any data collected by aircraft, including when that information becomes associated with a case and is used as evidence against an apprehended individual. In addition, all requests for aerial surveillance for intelligence gathering purposes must receive prior approval by the Assistant Commissioner, OIIL, before the air asset can conduct the flight. Similarly, requests for analytical products incorporating historical analysis of the border topography must be approved by the Assistant Commissioner, OIIL.

6. Principle of Data Quality and Integrity

Principle: *DHS should, to the extent practical, ensure that PII is accurate, relevant, timely, and complete, within the context of each use of the PII.*

As explained in section 4 (above), to ensure that the PII captured by aircraft is relevant and timely, any video, still images, signals information, and/or radar images must be associated within 30 days with the individual CBP apprehends, or the video/digital image is overwritten by OAM. Video and/or radar images are of no continuing value in a law enforcement support context unless they are associated with an individual during an apprehension because the video resolution or radar mapping images are not sufficiently precise to permit actual identification of



individuals. Video and/or radar images that are not associated with a person provide value in an intelligence context for helping to demonstrate the state of change occurring over time along the border. These unassociated images are separately maintained by OIIL for a maximum of five years.

To preserve the quality and integrity of the information collected that is used as evidence, CBP requires its officer/agents to successfully complete training on the proper operation of the recording equipment on its aircraft. The training includes correct techniques to copy recorded evidence from a non-portable hard drive to portable digital media and procedures to ensure that such evidence is not co-mingled with data from other investigations. The training also includes procedures to maintain an adequate chain of custody for all recorded evidence. Each officer/agent making a recording must ensure that the time and date shown in the original recording is accurate. After a mission is completed, the officer/agent must ensure that the original record is transferred entirely, in its original format, to portable media. The transferred data must not be edited or altered in any way. The officer/agent making the recording must label all copies of portable media with the corresponding case number (if available), the date and place of the original recording, and the names of the officer/agent and aircraft commander. The officer/agent making the recording must also label, initial, and maintain possession of the evidence until custody is properly transferred to the appropriate designated evidence custodian, case agent, Assistant United States Attorney, or other appropriate government official. As with any information associated with a case file, once the images are cross referenced to an investigation or case, they become covered by the system of records for that case file system and subject to the access and amendment provision of that system.

7. Principle of Security

Principle: DHS should protect PII (in all forms) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

CBP has taken steps to protect live video feeds, signals information, and recorded video, radar, and/or still pictures captured by its aircraft. Live video and flight information, which are sent from the UAS, are passed along an encrypted feed from the UAS through the satellite relay to the ground control station. Similarly, control information from the ground control station to the UAS also passes along an encrypted feed. Video and data transmitted in real time via Big Pipe, a closed system with restricted access, is subject to access controls and an approval process requiring clearance by one of two CBP/OAM system administrators to ensure that only authorized users with a need to know have access to the video feeds. The real time video feeds are not recorded and archived. Any recorded images that are saved to be used as evidence or for intelligence gathering must be handled in accordance with CBP policy. Images that are used as evidence must be handled according to the procedures detailed in section 6 of this PIA. All



recorded evidence must be kept in a locked container, segregated from other property and/or equipment. Video that is collected during an investigative operation that contains sensitive analytical surveillance, or reconnaissance related data may not be disclosed unless a request for disclosure has been submitted to the OIIL Collections Division Director. The request must include a copy of the information that is to be disclosed, must clearly specify the name of the intended recipient, how the information will be used, and the reasons justifying the disclosure. In the event that the information is disclosed, the OIIL Collections Division Director or his/her designee is required to redact law enforcement sensitive information, PII, and other sensitive related data unless the requestor has a need-to-know.

8. Principle of Accountability and Auditing

Principle: DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and should audit the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

All CBP employees are required to complete annual privacy awareness training, in addition to training on ethics and the CBP Code of Conduct. Access controls, both physical and technological, are in place to ensure only authorized access to the aircraft systems and the collected data/images.

Moreover, CBP requires its employees to successfully complete training on techniques to copy recorded evidence to portable digital media and requires them to follow procedures to ensure that such evidence is not co-mingled with data from other investigations. Employees must follow procedures to maintain an adequate chain of custody in the event that the information is used as evidence.

OIIL has a process in place for restricting the dissemination of video, still images, and radar images and keeps a log of the disclosures. Also, OIIL redacts law enforcement sensitive information, PII, and other sensitive related data unless the requestor has a valid need-to-know. Separately, CBP periodically reviews the logs or disclosure records to ensure compliance with established privacy policies, practices, and procedures for associated systems.



Conclusion

CBP operates aircraft systems in support of its border protection and law enforcement support missions. These systems provide a variety of mobile platforms from which to obtain signals information, video, still, and radar images of persons and vehicles in the border area or that are the subject of an investigation or law enforcement activity. The collection of these images and signals information complies with the same internal procedures and practices required of any surveillance using any means by CBP officers and agents. The distinct capabilities of the different aircraft operated by OAM enhance CBP's ability to conduct certain missions pertaining to information collection, surveillance, or reconnaissance; however, the processes and procedures for authorizing and accounting for how, when, and where information is obtained remain consistent with CBP's traditional border security and law enforcement practices and policy. As technology improves, operating environments change, and policies adapt, this PIA will be updated and amended to refresh the analysis of these changes on the privacy of persons, who directly or indirectly come into contact with the information and data collection activities associated with CBP Air operations.

Responsible Officials

Lothar Eckardt
Executive Director, National Air Security Operations
Office of Air & Marine
U.S. Customs and Border Protection
202-344-3950

Laurence Castelli
CBP Privacy Officer
Office of Privacy and Diversity
Office of the Commissioner
U.S. Customs and Border Protection
202-325-0280

Approval Signature Page

Original signed and on file with the DHS Privacy Office.

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security

Congress of the United States
Washington, DC 20515

July 17, 2020

The Honorable Mark A. Morgan, Acting Commissioner
Customs and Border Protection
1300 Pennsylvania Avenue, N.W.
Washington, D.C. 20229

Dear Acting Commissioner Morgan,

Thank you for your response of July 2, 2020 to our letter of June 9, 2020, about the troubling government surveillance of protesters and the chilling effect it has on peaceful protests. While we appreciate your response, your letter raises several questions which are listed in this letter.

As we stated in our letter, the First and Fourth Amendments protect protesters from government surveillance. The reason our Constitution has such critical protections is that government surveillance has a chilling effect on peaceful protests, and Americans should not have to take proactive measures to protect themselves from government surveillance before engaging in peaceful demonstration.

In order to understand the scope of potential surveillance of protesters by CBP, we respectfully request that you respond to the below questions by July 31, 2020:

- (1) In your letter, you state a CBP unmanned aircraft system (UAS) flew over Minneapolis, Minnesota on May 29th at the request of federal law enforcement but “was unable to observe activities on the ground due to cloud cover.” Press reports based on public flight records indicate this UAS to be CBP-104.¹
 - (a) Which federal law enforcement agency requested this aerial support from CBP? What exactly did the federal agency request? Please share any documentation of such request(s).
 - (b) Which law enforcement agency or agencies (whether federal, state, local, tribal, or international) received information or intelligence derived in whole or in part by the UAS?

¹ Joseph Cox, “The Government Is Regularly Flying Predator Drones Over American Cities,” *Vice Motherboard*, June 3, 2020, https://www.vice.com/en_us/article/n7wnzm/government-flying-predator-drones-american-cities.

- (c) Altitude has a major impact on the capability of any onboard camera(s). Press reports indicate that CBP-104 flew at an altitude of 20,000 feet over Minneapolis.² Is this accurate? If not, at what altitude did CBP-104 fly?
- (d) What surveillance equipment did CBP-104 have on board while it flew over Minneapolis? Please identify whether or not CBP-104 has each of the following types of equipment and whether each was operating during the May 29th flight:
 - (i) fixed or mobile video surveillance systems.
 - (ii) rangefinders.
 - (iii) thermal imaging devices.
 - (iv) radar.
 - (v) ground sensors.
 - (vi) dirtboxes, stingrays, other cell site mimicking equipment, other radio frequency sensors, or other telecommunications interception equipment.
 - (vii) wide-area surveillance system.
- (e) Did the UAS use any information collection technologies other than those identified in the Privacy Impact Assessment (PIA)?
- (f) What is the maximum resolution of the camera system(s) attached to CBP-104?
 - (i) How many pixels does the imaging sensor possess?
 - (ii) Can any camera system discern specific vehicles or individuals, even if it is not able to identify them on its own?
- (g) Did any surveillance equipment on board CBP-104 have associated software for facial recognition, other biometric identification, or automated license plate reading? Was such software used during or after the flight?

² Jason Koebler, Joseph Cox, and Jordan Pearson, “Customs and Border Protection Is Flying a Predator Drone Over Minneapolis,” *Vice Motherboard*, May 29, 2020, https://www.vice.com/en_us/article/5dzbe3/customs-and-border-protection-predator-drone-minneapolis-george-floyd.

- (h) What information was provided to the requesting agency or any other agencies that received footage or any other data from CBP-104?
 - (i) If any video footage was provided, what was the duration of the footage and what was the file size of total video files transferred?
 - (ii) What other data or files were transferred to the requesting agency? What was the total file size of the transfer?
 - (iii) Did CBP edit or alter the video footage or other data in any way before transferring such footage or data to the requesting agency?
- (2) You state that CBP UAs were not flown over Detroit, Michigan or San Antonio, Texas during protests.
 - (a) *The New York Times* reported on June 2nd that “At the request of the Justice Department...[AMO], which uses aircrafts and drones, was directed to provide surveillance of the protests, including demonstrations in Detroit.”³ Is this reporting inaccurate? If not, which part of the article is inaccurate?
 - (b) *Vice Motherboard* reported on June 3rd that “CPB-108 recently flew around half a dozen times above or near San Antonio, Texas”.⁴ Is this reporting inaccurate? If not, which part of the article is inaccurate?
- (3) Please provide a list of all requests for aerial support from federal, state, local, tribal, or international law enforcement agencies that involved any manned or unmanned aerial surveillance over, near, or of cities experiencing protests in the U.S. starting on May 25th.
 - (a) Please provide the documentation related to these requests.
 - (b) Please include whether CBP complied with these requests.
 - (c) For requests that CBP fulfilled, please provide the amount of time CBP aircraft was flown, the amount of footage collected, agencies to which data collected by CBP aircraft was provided, and descriptions of any altering and processing of the data by CBP or about which CBP has knowledge.
- (4) Please provide a list of any CBP manned and unmanned aerial flights not included in the response to question (2) that CBP knows to have collected any video

³ Zolan Kanno-Youngs and Katie Benner, “Trump Deploys the Full Might of Federal Law Enforcement to Crush Protests,” *The New York Times*, June 2, 2020, sec. U.S., <https://www.nytimes.com/2020/06/02/us/politics/trump-law-enforcement-protests.html>.

⁴ Cox, “The Government Is Regularly Flying Predator Drones Over American Cities.”

footage or other data related to protests, whether or not requested by a federal, state, local, tribal, or international law enforcement.

(5) In your letter, you state that “the onboard camera cannot provide enough detail for an operator to identify a person.” Over seven years ago, the military developed cameras powerful enough to identify a six-inch target (i.e., a human face) from 20,000 feet away,⁵ which is the reported altitude of CBP-104’s flight over Minneapolis.⁶ Further, “CBP formed a partnership with the Department of Defense (DoD) to identify and reuse excess DoD technology,” according to CBP documents.⁷

- (a) Does the CBP currently own or operate cameras that can identify individuals from an altitude of 20,000 feet?
- (b) Has CBP developed, leased, purchased, procured, or otherwise used such cameras or is CBP currently developing, leasing, purchasing, procuring, or otherwise aiming to use such cameras?
- (c) Has CBP ever processed images or footage from aerial cameras using facial recognition, gait analysis, or other biometric identification technologies?
- (d) Is CBP aware of federal, state, local, tribal, or international law enforcement agencies that have used CBP footage to identify individuals from footage?

(6) You enclosed a PIA for Aircraft Systems of CBP, as required by federal law.⁸ The enclosed document is dated September 9, 2013. While CBP released a more recent PIA on April 6, 2018 (DHS/CBP/PIA-018(a)), it is largely limited to discussions of only small UAS (sUAS), and not other UAS.⁹

⁵ Sebastian Anthony, “DARPA Shows off 1.8-Gigapixel Surveillance Drone, Can Spot a Terrorist from 20,000 Feet,” *ExtremeTech*, January 28, 2013, https://www.extremetech.com/extreme/146909-darpa-shows-off-1-8-gigapixel-surveillance-drone-can-spot-a-terrorist-from-20000-feet?utm_source=rss&utm_medium=rss&utm_campaign=darpa-shows-off-1-8-gigapixel-surveillance-drone-can-spot-a-terrorist-from-20000-feet.

⁶ Jason Koebler, Joseph Cox, and Jordan Pearson, “Customs and Border Protection Is Flying a Predator Drone Over Minneapolis.”

⁷ “Privacy Impact Assessment Update for the Aircraft Systems DHS/CBP/PIA-018(a)” (Department of Homeland Security / Customs and Border Protection, April 6, 2018), n. 2, <https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp018a-aircraftsystems-april2018.pdf> (Internal quotation marks omitted).

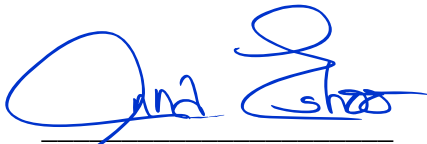
⁸ Section 208(b) of the E-Government Act of 2002 (44 U.S.C. §3501 note)

⁹ “Privacy Impact Assessment Update for the Aircraft Systems DHS/CBP/PIA-018(a).”


- (a) The 2013 PIA states that “As technology improves, operating environments change, and policies adapt, this PIA will be updated and amended to refresh the analysis of these changes...”¹⁰ Are surveillance technologies (equipment and software) on any CBP-operated UAS different from what was used on September 9, 2013?
- (i) If so, what are the new surveillance technologies, including but not limited to all of those discussed in this letter, that are not covered by the 2013 PIA?
 - (ii) If so, why has CBP not updated PIA documentation of these technologies?
 - (iii) If so, when will CBP update its PIA for these new technologies?
- (b) As mentioned in our questions, the 2018 PIA states that “CBP formed a partnership with the Department of Defense (DoD) to identify and reuse excess DoD technology.”¹¹ Does this partnership include any surveillance technologies (equipment and software) on any CBP-operated UAS (excluding sUAS)?
- (i) If so, what are these technologies?
 - (ii) If so, why has CBP not updated PIA documentation of these technologies?
 - (iii) If so, when will CBP update its PIA for these new technologies?

We would appreciate your prompt response to these highly important questions and requests, and we thank you in advance for your cooperation.

Most gratefully,



Anna G. Eshoo
Member of Congress

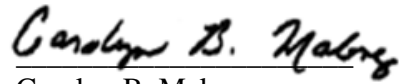


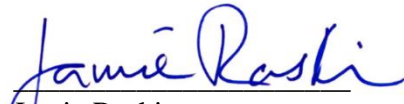
Bobby L. Rush
Member of Congress


¹⁰ “Privacy Impact Assessment for the Aircraft Systems DHS/CBP/PIA-018” (Department of Homeland Security / Customs and Border Protection, September 9, 2013), <https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp-aircraft-systems-20130926.pdf>.

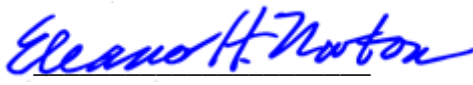
¹¹ “Privacy Impact Assessment Update for the Aircraft Systems DHS/CBP/PIA-018(a)” (Department of Homeland Security / Customs and Border Protection, April 6, 2018), n. 2, <https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp018a-aircraftsystems-april2018.pdf> (Internal quotation marks omitted).

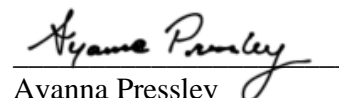

Zoe Lofgren
Member of Congress



Carolyn B. Maloney
Member of Congress



Jamie Raskin
Member of Congress

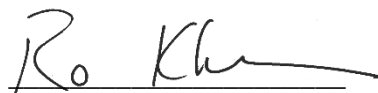

Alexandria Ocasio-Cortez
Member of Congress



Eleanor Holmes Norton
Member of Congress

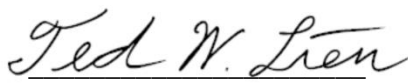

Ayanna Pressley
Member of Congress

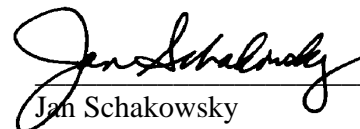

Earl Blumenauer
Member of Congress

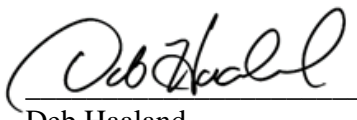

Brenda L. Lawrence
Member of Congress



Ro Khanna
Member of Congress

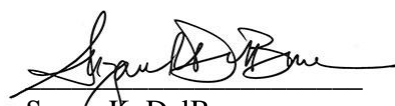

Michael F. Doyle
Member of Congress


Ted W. Lieu
Member of Congress



Jan Schakowsky
Member of Congress


Deb Haaland
Member of Congress



Peter Welch
Member of Congress


Suzan K. DelBene
Member of Congress



Denny Heck
Member of Congress



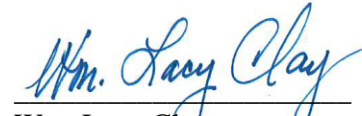
Stephen F. Lynch
Member of Congress



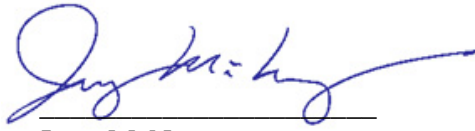
Mark Takano
Member of Congress



Rashida Tlaib
Member of Congress



Wm. Lacy Clay
Member of Congress



Jerry McNerney
Member of Congress

Congress of the United States
Washington, DC 20515

July 17, 2020

Ms. Jill C. Tyson, Assistant Director
Office of Congressional Affairs
Federal Bureau of Investigation
935 Pennsylvania Avenue, N.W.
Washington, D.C. 20535

Dear Ms. Tyson,

Thank you for your response of July 1, 2020 to our letter of June 9, 2020, about the troubling government surveillance of protests and the chilling effect it has on peaceful protests. While we appreciate your response, the lack of any information in your letter is worrying. For that reason, we write this letter including specific questions about the recent actions of the Federal Bureau of Investigation (FBI).

As we stated in our letter, the First and Fourth Amendments protect protesters from government surveillance. The reason our Constitution has such critical protections is that government surveillance has a chilling effect on peaceful protests, and Americans should not have to take proactive measures to protect themselves from government surveillance before engaging in peaceful demonstration.

While your letter states it “would not be appropriate to disclose law enforcement sensitive information about specific operations, methods, and assets,” the total lack of information in your letter ignores the important role of congressional oversight of the Executive Branch, which is enshrined in the constitution. We believe the FBI can, and must, share some information about recent activities without jeopardizing specific law enforcement investigations.

In order to understand the scope of potential surveillance of protesters by the FBI, we respectfully request that you respond to the below questions by July 31, 2020:

- (1) Press reports indicate that the FBI flew an RC-26B aircraft during protests in Washington, D.C., and Las Vegas, Nevada, and that the aircraft may have been equipped with infrared sensors, electro-optical cameras, and ‘dirtboxes,’ which collect cell phone location data.¹ Are these press reports accurate? If not, please identify the inaccuracies with these press reports.
- (2) Other than the reported Washington, D.C. and Las Vegas, Nevada flights, did the FBI use any aircraft – or ask any other federal or state agency to use aircraft – to monitor or surveil protests since May 25th related to the murder of George Floyd,

¹ Joseph Cox, “The Military and FBI Are Flying Surveillance Planes Over Protests,” *Vice Motherboard*, June 3, 2020, https://www.vice.com/en_us/article/y3zvwj/military-fbi-flying-surveillance-planes-george-floyd-protesters.

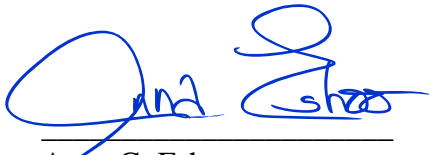
the killings of other Black Americans by law enforcement officials, or Black Lives Matter? If so, please also answer the following about any associated aerial surveillance:

- (a) For what purpose, and under what legal authority, did the FBI conduct such aerial surveillance?
 - (b) How many flights for aerial surveillance over protests has the FBI initiated since May 25th?
 - (c) How many law enforcement actions were investigated or initiated by the FBI based on data collected during aerial surveillance?
 - (d) Has the FBI transferred any data collected through aerial surveillance to other federal, state, local, or international agencies (including law enforcement agencies), to private corporations, or to any other organization? If so, please list what was shared and with which organization.
 - (e) Other than the FBI, which federal, state, or local government agencies, law enforcement or otherwise, participated in or conducted such surveillance that the FBI is aware of?
- (3) If the FBI did fly aircrafts over Washington, D.C., Las Vegas, Nevada, or other U.S. cities as described in question (2), what surveillance equipment did the aircraft have on-board?
- (a) Please identify whether or not each of following the types of equipment was on-board the aircraft and whether each was activated during the associated flights:
 - (i) fixed or mobile video surveillance systems.
 - (ii) rangefinders.
 - (iii) thermal imaging devices.
 - (iv) radar.
 - (v) ground sensors.
 - (vi) dirtboxes, stingrays, other cell site mimicking equipment, other radio frequency sensors, or other telecommunications interception equipment.
 - (vii) wide-area surveillance system.
 - (b) What is the maximum resolution of the camera system(s) attached to associated aircraft?

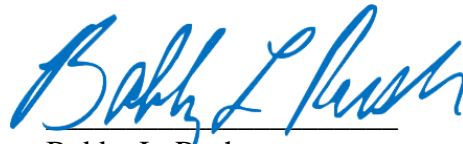
- (i) How many pixels does the imaging sensor possess?
- (ii) Can any camera system discern specific vehicles or individuals, even if it is not able to identify them on its own?
- (c) Did any equipment on-board the aircraft include any equipment that has associated software for facial recognition, other biometric identification, or automated license plate reading? Was such software used during or after the flight?
- (4) What policies, protocols, and procedures – including any Privacy Impact Assessments and System of Records Notices – does the FBI have regarding the use of aerial surveillance? Please provide a copy of any associated documentation for these policies, protocols, and procedures.

We would appreciate your prompt response to these highly important questions and requests, and we thank you in advance for your cooperation.

Most gratefully,



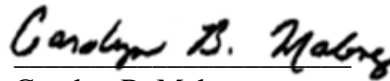
Anna G. Eshoo
Member of Congress



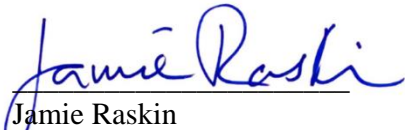
Bobby L. Rush
Member of Congress



Zoe Lofgren
Member of Congress



Carolyn B. Maloney
Member of Congress



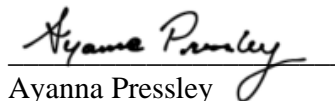
Jamie Raskin
Member of Congress



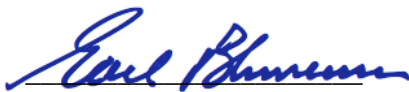
Alexandria Ocasio-Cortez
Member of Congress



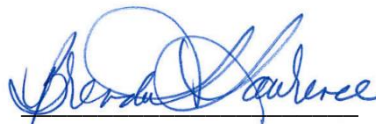
Eleanor Holmes Norton
Member of Congress




Ayanna Pressley
Member of Congress




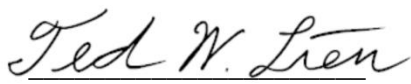
Earl Blumenauer
Member of Congress

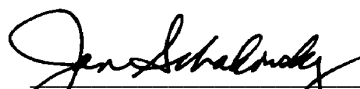



Brenda L. Lawrence
Member of Congress


Ro Khanna
Member of Congress



Michael F. Doyle
Member of Congress


Ted W. Lieu
Member of Congress



Jan Schakowsky
Member of Congress



Deb Haaland
Member of Congress



Peter Welch
Member of Congress



Suzan K. DelBene
Member of Congress



Denny Heck
Member of Congress


Stephen F. Lynch
Member of Congress


Mark Takano
Member of Congress


Rashida Tlaib
Member of Congress


Wm. Lacy Clay
Member of Congress


Jerry McNerney
Member of Congress

United States Senate

July 29, 2020

The Honorable William Barr
Attorney General
U.S. Department of Justice
950 Pennsylvania Avenue
Washington, DC 20530-001

The Honorable Chad F. Wolf
Acting Secretary
U.S. Department of Homeland Security
3801 Nebraska Avenue, NW
Washington, DC 20528

Dear Attorney General Barr and Acting Secretary Wolf:

On June 5, 2020, several Senators requested information about the federal response to protests across the nation in the wake of the police killing of George Floyd. We have yet to receive a response to that request.

There are now disturbing reports that unidentified federal agents are using excessive force against protesters and members of the press in Portland, Oregon. First-hand accounts, corroborated by video evidence, also indicate that peaceful protesters have been detained without cause or explanation. Agents shot one man in the head with a “less-lethal” weapon, fracturing his skull and requiring facial reconstructive surgery. A reporter who identified himself as a member of the press alleges he was shot ten times in the back while fleeing from federal agents, and another reporter claims he witnessed federal agents chase after legal observers from the National Lawyers Guild with “truncheons swinging.” Additionally, media reports indicate that DHS may be collecting information on and monitoring Americans it believes pose a threat to statues or monuments—even those not on federal property or owned by the federal government.

The governor of Oregon and the mayor of Portland have repeatedly asked you to withdraw federal forces in light of these tactics, yet you insist on keeping them there, inflaming tensions in the city. Now, the President is apparently deploying a separate task force coordinated by the Department of Justice to other American cities without a clear objective or the prior permission of these cities’ elected leaders. For example, last week, Acting Secretary Wolf gave repeated assurances to Washington state elected leaders that no additional DHS personnel would be sent to Washington state, and then, on that very same day, a plane with DHS personnel landed near Seattle.

Senators previously asked you to provide, for each of your agencies, an accounting of the forces you have deployed against peaceful protests. Specifically, you were asked:

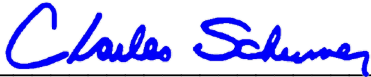
- What forces have DOJ and DHS deployed?
- Where have DOJ and DHS deployed those forces?
- What additional or extraordinary authorities have DOJ and DHS given these forces?
- How are DOJ and DHS ensuring that these forces are respecting protesters' legal rights?

In addition to providing this information, please also explain the authorities, procedures, and rules governing the use of force, identification of personnel, and detention and questioning of civilians by your personnel; the training provided to your personnel on these authorities, procedures, and rules; and what you are doing to ensure your personnel's compliance in the field, including how violators will be held accountable. In particular, we would like to understand what intelligence personnel are being deployed and what domestic collection, analysis, and dissemination activities they are undertaking, especially with respect to non-federal crimes and activities that do not threaten violence against persons or federal property. Finally, please explain any plans for current or future deployments of federal personnel to other cities, describing, for each city, the number of personnel contemplated, their expected mission and duration of deployment, and what steps have been taken to ensure these personnel support state and local law enforcement rather than attempt to supplant them.

Administration officials have claimed that federal forces are necessary to protect federal property in Portland. But this does not justify the use of excessive force or the detention of protestors without probable cause by agents who refuse to identify themselves. These tactics are not consistent with our Constitution or the rule of law. We therefore demand that you remove these forces from Portland, as has been requested by state and local officials. We also urge you to coordinate closely in advance with state and local officials and honor their requests and denials related to deployment of DHS, DOJ or other federal law enforcement personnel in their jurisdictions.

Thank you for your prompt attention to this urgent matter.

Sincerely,



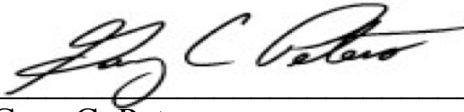
Charles E. Schumer
United States Senator



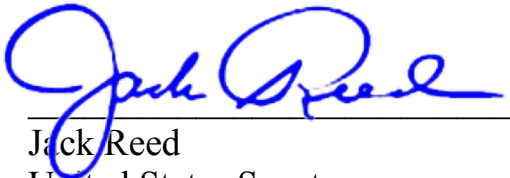
Dianne Feinstein
United States Senator



Richard J. Durbin
United States Senator



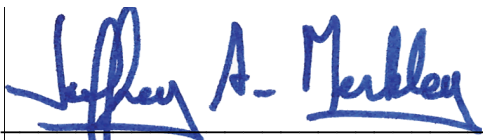
Gary C. Peters
United States Senator



Jack Reed
United States Senator



Mark R. Warner
United States Senator



Jeffrey A. Merkley
United States Senator



Ron Wyden
United States Senator



Patty Murray
United States Senator



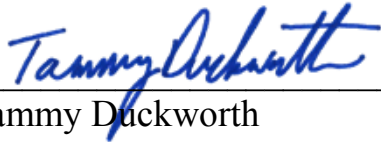
Debbie Stabenow
United States Senator



Martin Heinrich
United States Senator



Tom Udall
United States Senator



Tammy Duckworth
United States Senator



Sherrod Brown
United States Senator



Maria Cantwell
United States Senator

RICHARD BURR, NORTH CAROLINA, CHAIRMAN
MARK R. WARNER, VIRGINIA, VICE CHAIRMAN

JAMES E. RISCH, IDAHO
MARCO RUBIO, FLORIDA
SUSAN M. COLLINS, MAINE
ROY BLUNT, MISSOURI
TOM COTTON, ARKANSAS
JOHN CORNYN, TEXAS
BEN SASSE, NEBRASKA

DIANNE FEINSTEIN, CALIFORNIA
RON WYDEN, OREGON
MARTIN HEINRICH, NEW MEXICO
ANGUS S. KING, JR., MAINE
KAMALA HARRIS, CALIFORNIA
MICHAEL F. BENNET, COLORADO

MITCH MCCONNELL, KENTUCKY, EX OFFICIO
CHARLES SCHUMER, NEW YORK, EX OFFICIO
JAMES M. INHOFE, OKLAHOMA, EX OFFICIO
JACK REED, RHODE ISLAND, EX OFFICIO

CHRISTOPHER A. JOYNER, STAFF DIRECTOR
MICHAEL CASEY, MINORITY STAFF DIRECTOR
KELSEY S. BAILEY, CHIEF CLERK

United States Senate

SELECT COMMITTEE ON INTELLIGENCE

WASHINGTON, DC 20510-6475

July 31, 2020

Mr. Brian Murphy
Acting Under Secretary of Homeland Security for Intelligence and Analysis
Department of Homeland Security
Washington, D.C. 20528

Dear Acting Under Secretary Murphy:

We have grown increasingly concerned about the role and operations of the Department of Homeland Security, and the Office of Intelligence and Analysis (I&A) in particular, with regard to the protests in Portland, Oregon. As a member of the Intelligence Community, I&A is obligated by statute to keep the congressional intelligence committees fully and currently informed of its operations. Given the intense national as well as congressional interest in DHS activities related to protests in Portland and around the country, documents and other information related to I&A's operations should be provided to the Committee pro-actively, and not merely in response to repeated requests or following revelations in the press.

We request that you provide the following information:

1. Of the I&A personnel deployed to, or otherwise who have been assigned to missions connected to the Portland protests, how many are analysts and how many are collectors? What I&A mission centers do they work for? What backgrounds and training do they have that are relevant to the Portland mission?
2. Has I&A employed any contractors for the Portland mission? If yes, please describe their roles.
3. Where have I&A personnel in Portland physically worked and with whom have they been co-located?

4. Please provide a breakdown of the DHS components I&A personnel have supported and a description of the support provided to each such component. To what extent does the chain of command of I&A personnel include those components, as opposed to I&A Headquarters?
5. Please describe interactions and coordination between I&A personnel in Portland and state and local law enforcement and political authorities.
6. Please describe interactions and coordination between I&A personnel in Portland and federal law enforcement, including elements of the Departments of Justice and Homeland Security.
7. A July 9, 2020, I&A document describing “Portland Surge Operation” states that I&A personnel may “collect from incarcerated, detained, or arrested persons” so long as the collection is conducted overtly. You stated during a briefing for Committee staff on July 23, 2020, that I&A personnel have not engaged in custodial debriefings. Please confirm. Have I&A personnel been indirectly engaged with detainee operations, for example, by providing collection requirements or requests, or suggested lines of questioning, to detaining authorities or otherwise requesting or receiving information related to detainees?
8. You also stated during the July 23, 2020, briefing that I&A personnel have not interacted with protesters in any way. Please confirm.
9. During the July 23, 2020, briefing, you stated that I&A had neither collected nor exploited or analyzed information obtained from the devices or accounts of protesters or detainees. Please confirm.
10. Please describe I&A’s open source collection. What rules of engagement apply to open source collection in the context of protests in which the vast majority of participants are exercising their First Amendment rights? What rules or guidance does I&A follow to distinguish actual threats of violence or vandalism from political hyperbole, and what training do I&A personnel receive on the implementation of that guidance?
11. What processes does I&A have to vet the authenticity of open source threat reporting? What processes does I&A have to vet the authenticity of social media accounts in which individuals take credit for acts of violence or vandalism, on their own behalf or on behalf of an ideology? How has this

vetting been conducted prior to disseminating this information, or using it as a basis for analysis?

12. Have I&A operations in connection with the Portland protests been reviewed by an I&A Intelligence Oversight Officer, DHS's Privacy Office and Office for Civil Rights and Civil Liberties, or any other DHS personnel responsible for reviewing the impact of I&A operations on the privacy and civil liberties of U.S. persons? If yes, please describe those reviews.
13. The "Job Aid" document authorizes collection of information that "informs an overall assessment that threats to [law enforcement] personnel, facilities, or resources will materialize." The document includes a similar explicit authorization with regard to public monuments, memorials and statues. Can I&A collect information on U.S. persons who are not threatening violence and, if so, under what circumstances?
14. Has I&A conducted network analysis linking individuals suspected of violence? If yes, please describe how that analysis has been conducted while not collecting on U.S. persons not suspected of violence? Please provide any such analysis.
15. During the July 23, 2020, briefing, you stated that I&A is able to track those who engage in violent acts because "it is the same people who come out after midnight." Please describe how I&A is able to differentiate between peaceful protesters exercising their First Amendment rights and those individuals who have planned or conducted acts of violence, and what information or intelligence is used in making this determination.
16. Has I&A produced or contributed to targeting packages or dossiers on particular suspects? If yes, please provide these to the Committee.
17. On July 16, 2020, the FAA put in place flight restrictions over Portland to prevent drones from flying below 1000 feet. The FAA cited a DHS conclusion that private drone use presented a threat. Please provide any intelligence to support that conclusion.
18. Have I&A personnel obtained or analyzed data from overhead surveillance of protests? If yes, please describe.

19. On July 25, 2020, you sent a memo to I&A personnel in which you stated that individuals in Portland committing acts of violence are “VIOLENT ANTIFA ANARCHIST INSPIRED (VAAI).” Please describe the origin of this designation and the analytical process whereby it was developed and applied.
20. Your July 25, 2020, memo stated that the VAAI designation was informed by FIRs, OSIRs, “baseball cards” and FINTEL. Please provide these documents to the Committee.
21. Please describe how I&A has applied its retention guidelines to information related to the Portland protests. What information has been marked for indefinite retention? How has I&A sought to apply its 180-day retention limitation to information it has disseminated?
22. Please describe what I&A raw reporting has been disseminated to what entities, whether DHS, federal law enforcement, state or local or municipal law enforcement, or the Intelligence Community.
23. Are there limits to I&A’s role in protecting public monuments, memorials or statues absent threat of violence to persons? Does it matter whether such monuments, memorials or statues are on federal, state, local, or private property?
24. What other cities has I&A deployed to, or plans to deploy to in response to protests or associated threats of violence? Please provide any documentation or guidance related to any such deployments.
25. According to press accounts, I&A disseminated Open Source Intelligence Reports on a journalist and a legal scholar who had written about I&A. If that is accurate, provide those reports, a complete description of who they were disseminated to, and an explanation of the purpose and basis for the reports and their dissemination under law and I&A’s intelligence oversight guidelines, including with regard to the identification of any U.S. persons within them.

Please provide responses no later than Thursday, August 6, 2020.
Thank you for your attention to this important and urgent matter.

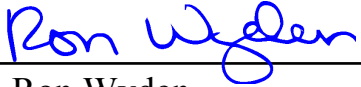
Sincerely,



Mark R. Warner
Vice Chairman



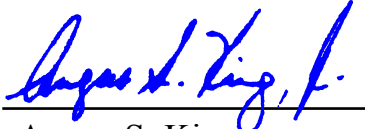
Dianne Feinstein
U.S. Senator



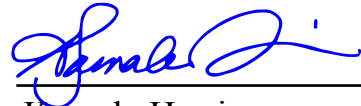
Ron Wyden
U.S. Senator



Martin Heinrich
U.S. Senator



Angus S. King
U.S. Senator



Kamala Harris
U.S. Senator



Michael F. Bennet
U.S. Senator

United States Senate

WASHINGTON, DC 20510-3203

June 5, 2020

Attorney General Barr
Department of Justice

Secretary Esper
Department of Defense

Secretary David Bernhardt
Department of Interior

Acting Secretary Chad F. Wolf
Department of Homeland Security

On June 2, 2020, BuzzFeed reported that Timothy Shea, Acting Director of the Drug Enforcement Agency, requested and was granted expanded authority to conduct covert surveillance, share intelligence, intervene at protests as federal law enforcement, and engage in other enforcement and investigative activity. (“The DEA Has Been Given Permission To Investigate People Protesting George Floyd’s Death,” BuzzFeed News, 6/2/2020). This reporting came just one day after a hybrid force consisting of the U.S. Secret Service, the U.S. Park Police, the D.C. National Guard, and possibly others forcibly removed peaceful protestors from Lafayette Park directly across from the White House using tear gas and rubber bullets.

These are troubling indicators that federal law enforcement and security agencies are being inappropriately mobilized in response to protests over the death of George Floyd – an unarmed black man who was killed by a Minneapolis police officer who knelt on his neck for eight minutes and 46 seconds as he lay handcuffed.

We request you provide, from each of your agencies: what forces you have deployed against these protests; where you have deployed them; what additional or extraordinary authorities these forces are exercising or have been provided (similar to the DEA); and what, if any, steps have been taken to ensure they are respecting the Constitutional rights of the protestors they are now policing in exercising their authorities. Please provide this information by the close of business on June 8, 2020. We would further expect that each agency will offer appropriate officials for follow-on briefings on these subjects in the following week.

The First Amendment protects the rights of all Americans to protest and seek equal justice under the law. While there has been some unacceptable looting, it is unclear what justifies the extraordinary actions of your agencies in the past week, whether by granting DEA the authority and responsibility to conduct “covert surveillance” on Americans exercising their constitutional rights or directing law enforcement or military personnel to engage in a use of force against peaceful protestors. We are deeply concerned that, in the wake of the horrific killing in Minnesota, there is a lack of transparency regarding the forces you have deployed and

under what authorities you have deployed them. These actions only further undermine the American people's faith in their law enforcement.

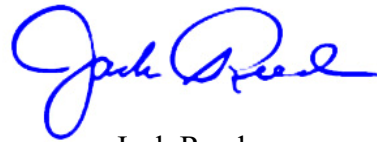
These are incredibly difficult times. Americans across the nation are understandably shaken by all they have experienced and witnessed in recent weeks and months. We expect that each of you will, in addition to providing the information we have requested above, immediately and publicly order your forces to exercise maximum restraint when dealing with peaceful protestors and respect the Constitutional rights of those protestors. We will be closely monitoring how you handle this situation—these protestors are our fellow citizens, not terrorists. You should act accordingly.

We look forward to your reply.

Sincerely,



Charles E. Schumer
Democratic Leader



Jack Reed
Ranking Member SASC



Dianne Feinstein
Ranking Member SJC



Mark R. Warner
Vice Chairman SSCI



Gary Peters
Ranking Member HSGAC

Congress of the United States

Washington, DC 20515

June 24, 2020

Donald W. Washington
Director
United States Marshals Service
Washington, DC 20530-0001

Dear Director Washington:

We write to request information about recent surveillance flights over Portland, reportedly by the U.S. Marshals Service (USMS).

According to media reports, an aircraft previously linked to the USMS circled over Portland for nearly three hours on June 13, 2020, a night in which thousands of Oregonians exercised their First Amendment right to protest. The aircraft that flew over Portland is registered to a company that journalists in 2017 identified as a front company for the USMS. Media reports have previously revealed that the USMS operates a fleet of surveillance aircraft equipped with cellphone surveillance technology capable of secretly gathering information from tens of thousands of phones below.

The cell phone spying technology, known as a cell site simulator, used by the USMS, was originally created for America's military and intelligence community to use overseas. This technology beams tracking signals, indiscriminately, into the homes of innocent Americans, to scoop up data from their phones. According to experts, cell site simulators can identify all the phones in an area, track particular phones, and even intercept calls and text messages. This is an invasive, dragnet surveillance tool, which intrudes into the homes and devices of thousands of innocent people each time it is used. While such large-scale invasions of privacy might be justified in order to protect the public from imminent harm, the decision as to when to conduct bulk surveillance using a technology that intrudes on the privacy of so many innocent people must be made by independent courts and not the government.

Oregonians, like Americans everywhere, are justifiably outraged by recent events, including the murder of George Floyd by the police, which have highlighted longstanding problems in our society and government, including systemic racism and police brutality. Many Oregonians who have protested are justifiably concerned that their participation in these lawful protests will be logged, recorded, and used against them later by the government. As such, Congress has a responsibility to investigate these reports and make sure that the government's powerful surveillance tools are under the close supervision of the courts and that Americans' rights are being protected. To that end, please provide us with answers to the following questions by July 17, 2020:

1. Does the USMS own or operate the Cessna Caravan airplane, tail number N1789M, that reportedly flew 30 loops over Portland on the night of June 13, 2020?

2. Who authorized the use of a front company to register these airplanes? Please provide us with a copy of this authorization.
3. Who authorized the June 13, 2020, flight over Portland? Please provide us with a copy of this authorization.
4. What surveillance equipment was used and what types of data were collected during this operation?
5. Has data collected during this operation been shared with other agencies or any other entity? If so please identify them.
6. If surveillance technology was used, was it authorized by a court? If yes, please provide us with a copy of the court order and the corresponding application.
7. Has data collected on this flight been minimized, destroying data on innocent people who are not the targets of an investigation? If yes, please explain how. If no, please explain why not.

We look forward to your timely response.

Sincerely,



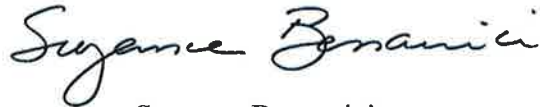
Ron Wyden
United States Senator



Jeffrey A. Merkley
United States Senator



Earl Blumenauer
Member of Congress



Suzanne Bonamici
Member of Congress



Kurt Schrader
Member of Congress



U.S. Department of Justice
United States Marshals Service
Office of Congressional Affairs

Washington, DC 20530-0001

August 19, 2020

The Honorable Ron Wyden
United States Senator
221 Dirksen Senate Office Bldg
Washington, D.C. 20510

Dear Senator Wyden,

This responds to your letter to Director Donald Washington dated June 24, 2020, inquiring about the activities of a United States Marshals Service (USMS) aircraft over Portland, Oregon on June 13, 2020.

We appreciate your concern for the rights of Oregonians, and want you to know that the USMS is committed to protecting the rights of all American citizens while fulfilling our statutory obligation to protect the federal judicial process, members of the court family, and federal courthouses.

As you know, part of the USMS mission is to provide support to varied elements of the federal justice system. USMS provides for the security of federal court facilities and the safety of judges, witnesses, prisoners, and other court personnel. Since the death of George Floyd starting on May 29th and nightly thereafter, there have been peaceful protests every day and evening around the Mark Hatfield U.S. Courthouse in Portland. Unfortunately, every evening violent rioters unaffiliated with peaceful protestors have attacked the courthouse and tried to harm the deputy U.S. Marshals tasked with protecting it. On two occasions, criminals have forced entry into the courthouse building before being arrested or repelled. There have been multiple incidents where individuals have tried to set the courthouse on fire or gain access to destroy it.

On June 13, 2020, USMS management approved deployment of an air asset to assist the ongoing law enforcement challenges on the ground. The aircraft, a single engine Cessna Caravan, is owned and operated by the USMS, and is registered in accordance with standard operating practices for federal law enforcement agencies. The aircraft is equipped with an imaging system (aviation electro-optical and infrared camera) that gave better situational awareness to the small number of deputies who were defending the federal courthouse during a time of great uncertainty.

Cell site simulators were not used during this short deployment, and we hope you understand that USMS can only use equipment like cell site simulators under the supervision of a court order or pursuant to approved exigent circumstances. No other surveillance systems other

than the identified camera platform were utilized and no judicial authorization was required for use of the camera.

The camera provided still pictures of crowds to assist a legitimate law enforcement function. Specifically, images of the identified courthouse(s) and surrounding area, spanning a 1.5 hour period from June 13-14, 2020, were captured by the camera device (no videos were recorded). To the extent people are visible in those images, they appear as indistinct heat signatures with no physical characteristics, biographic identifiers, or personally identifiable information of any kind. What the images show is the influx of crowds approaching the Multnomah County Justice Center and Hatfield U.S. Courthouse within the final hours of June 13 and into the early morning hours of June 14. The collected images were not shared with any other agencies or entities. To help allay your concerns, we have enclosed one of the images taken by the aircraft during that evening.

We hope this information is helpful. A similar letter has been sent to the other cosigners. Please contact this office if we may provide additional assistance regarding this or any other matter.

Sincerely,

William Delaney

William Delaney
Chief, Office of Congressional and Public Affairs

Enclosed: 06132020 Portland Aircraft Imagery

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>

June 5, 2020

The Honorable Chad F. Wolf
Acting Secretary of Homeland Security
245 Murray Lane, S.W.
Washington, D.C. 20528

Dear Acting Secretary Wolf:

We write with grave concern about the use of Department of Homeland Security (DHS) resources—including drones and armed uniformed officers—to surveil and intimidate peaceful protesters who were exercising their First Amendment rights to protest the murder of George Floyd by the Minneapolis Police Department.

On May 29, 2020, the Project on Government Oversight reported that a “Predator Drone CPB104 circling over Minneapolis at 20K feet” had taken off from Grand Forks Air Force Base and was flying above the protests.¹ Customs and Border Protection (CBP) later confirmed the existence of the Unmanned Aircraft System (UAS) mission in Minneapolis.²

This aircraft, commonly known as a “Predator B,” captures full-motion video and synthetic-aperture radar imagery for surveillance.³ While this drone has been used domestically for humanitarian, emergency, and recovery operations, it is primarily used to counter illicit cross-border activities along the northern and southern borders.⁴

¹ *Customs and Border Protection Flew a Predator Surveillance Drone Over Minneapolis Protests Today*, Gizmodo (May 29, 2020) (online at gizmodo.com/customs-and-border-protection-flew-a-predator-surveillance-1843758034?rev=1590777653179).

² Customs and Border Protection, *CBP Statement on the AMO Unmanned Aircraft System in Minneapolis* (May 29, 2020) (online at www.cbp.gov/newsroom/speeches-and-statements/cbp-statement-ammo-unmanned-aircraft-system-minneapolis).

³ *Civilian UAVs: No Pilot, No Problem*, Popular Mechanics (Oct. 1, 2009) (online at <https://www.popularmechanics.com/flight/drones/a4026/4213464/>); *Predator B Data Sheet*, General Atomics Aeronautical (accessed on May 29, 2020) (online at www.ga-asi.com/predator-b).

⁴ Customs and Border Protection, *Unmanned Aircraft System MQ-9 Predator B Fact Sheet* (accessed May 29, 2020) (online at www.cbp.gov/sites/default/files/assets/documents/2019-Feb/air-marine-fact-sheet-uas-predator-b-2015.pdf).

The drone that was flown on May 29, 2020, was reportedly also flown far outside the bounds of CBP's jurisdiction. Federal law authorizes CBP to conduct its missions within a "reasonable distance," not to exceed more than 100 air miles inland, from an external boundary of the United States.⁵

On Monday, DHS confirmed that both CBP and Immigration and Customs Enforcement officers would be deployed nationwide to help monitor the growing protests.⁶ This news is particularly alarming given that, for almost a year, the Committee has been investigating racist, sexist, and xenophobic comments made by CBP employees in secret Facebook groups. CBP has been obstructing the Committee's investigation, and CBP employees who made inappropriate and threatening comments may still be on the job and deployed to silence protesters exercising their Constitutional rights.⁷

This Administration has undermined the First Amendment freedoms of Americans of all races who are rightfully protesting George Floyd's killing. The deployment of drones and officers to surveil protests is a gross abuse of authority and is particularly chilling when used against Americans who are protesting law enforcement brutality.

For these reasons, we request that you produce the following documents and information:

1. A complete list of jurisdictions where DHS conducted or assisted in conducting surveillance of any protests since Monday, May 25, 2020, including:
 - a. who in each jurisdiction requested DHS's assistance and for what purpose;
 - b. whether DHS conducted such surveillance pursuant to mutual aid or similar agreements, and if so, the full terms of those agreements;
 - c. whether DHS received any reimbursement from any state or local jurisdiction to conduct that surveillance, and if so, the amounts;
 - d. whether DHS recorded any data relating to the protests, and if so, how DHS intends to use those recordings, with whom it will share the data, and what data retention and sharing policies apply;

⁵ *ACLU Factsheet on Customs and Border Protection's 100-Mile Zone*, American Civil Liberties Union (accessed June 1, 2020) (online at www.aclu.org/other/aclu-factsheet-customs-and-border-protections-100-mile-zone?redirect=immigrants-rights/aclu-fact-sheet-customs-and-border-protections-100-mile-zone); 8 U.S.C. § 1357.

⁶ *Immigration Agencies to Assist Law Enforcement Amid Unrest*, Roll Call (June 1, 2020) (online at www.rollcall.com/2020/06/01/immigration-agencies-to-assist-law-enforcement-amid-unrest/).

⁷ Letter from Chairwoman Carolyn B. Maloney, Committee on Oversight and Reform, to Mark Morgan, Chief Operating Officer and Senior Official Performing the Duties of the Commissioner, Customs and Border Protection (Feb. 18, 2020) (online at <https://oversight.house.gov/sites/democrats.oversight.house.gov/files/2020-02-18.CBM%20to%20Morgan-USCBP%20re%20Documents%20and%20TIs.pdf>).

- e. whether DHS or any of the local police departments or recipients of the drone video feeds used facial recognition technology, and if so:
 - i. what facial recognition technology was used, including a description of the software and hardware used in each jurisdiction;
 - ii. at whose request it was used;
 - iii. for what purpose;
 - iv. whether the algorithm for the facial recognition technology has been evaluated for accuracy by the National Institute of Standards and Technology or any other entity, including a description of any assessment method and results;
 - v. the source and characteristics of any data used or accessed in connection with the use of facial recognition technology;
 - f. the cost, in each jurisdiction, of DHS's surveillance activity;
2. If CBP has conducted any surveillance or law enforcement activity more than 100 air miles from any external U.S. border, the jurisdictions in which it took place and the legal justification for it;
3. A complete list of jurisdictions where DHS has deployed or plans to deploy officers to assist in policing protests since May 25, 2020, including:
- a. who in each jurisdiction requested DHS's assistance and for what purpose;
 - b. whether DHS deployed officers pursuant to mutual aid or similar agreements, and if so, the full terms of those agreements;
 - c. whether DHS received any reimbursement from any state or local jurisdiction to deploy those officers, and if so, the amounts;
 - d. how many personnel from ICE and CBP were deployed to each jurisdiction;
 - e. the cost, in each jurisdiction, of DHS's police activity; and
4. All communications and documentation regarding the above requests.

Please provide the requested information by June 11, 2020, as well as a briefing to Committee staff by June 15, 2020.

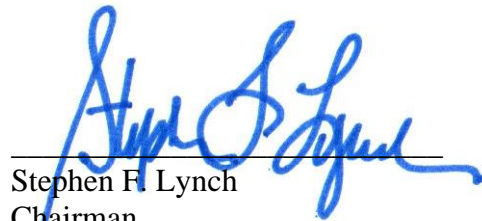
The Committee on Oversight and Reform is the principal oversight committee of the House of Representatives and has broad authority to investigate “any matter” at “any time” under House Rule X.

An attachment to this letter provides additional instructions for responding to the Committee’s request. If you have any questions regarding this request, please contact our staff at (202) 225-5051.

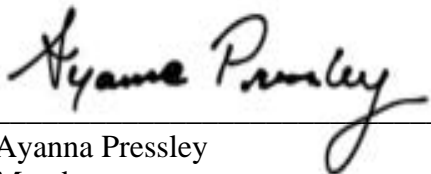
Sincerely,



Carolyn B. Maloney
Chairwoman
Committee on Oversight and Reform



Stephen F. Lynch
Chairman
Subcommittee on National Security



Ayanna Pressley
Member
Subcommittee on Civil Rights and
Civil Liberties



Jamie Raskin
Chairman
Subcommittee on Civil Rights and
Civil Liberties



Alexandria Ocasio-Cortez
Member
Subcommittee on Civil Rights and
Civil Liberties

Enclosure

cc: The Honorable Jim Jordan, Ranking Member
Committee on Oversight and Reform

The Honorable Chip Roy, Ranking Member
Subcommittee on Civil Rights and Civil Liberties

The Honorable Glenn Grothman, Ranking Member
Subcommittee on National Security

Responding to Oversight Committee Document Requests

1. In complying with this request, produce all responsive documents that are in your possession, custody, or control, whether held by you or your past or present agents, employees, and representatives acting on your behalf. Produce all documents that you have a legal right to obtain, that you have a right to copy, or to which you have access, as well as documents that you have placed in the temporary possession, custody, or control of any third party.
2. Requested documents, and all documents reasonably related to the requested documents, should not be destroyed, altered, removed, transferred, or otherwise made inaccessible to the Committee.
3. In the event that any entity, organization, or individual denoted in this request is or has been known by any name other than that herein denoted, the request shall be read also to include that alternative identification.
4. The Committee's preference is to receive documents in electronic form (i.e., CD, memory stick, thumb drive, or secure file transfer) in lieu of paper productions.
5. Documents produced in electronic format should be organized, identified, and indexed electronically.
6. Electronic document productions should be prepared according to the following standards:
 - a. The production should consist of single page Tagged Image File ("TIF"), files accompanied by a Concordance-format load file, an Opticon reference file, and a file defining the fields and character lengths of the load file.
 - b. Document numbers in the load file should match document Bates numbers and TIF file names.
 - c. If the production is completed through a series of multiple partial productions, field names and file order in all load files should match.
 - d. All electronic documents produced to the Committee should include the following fields of metadata specific to each document, and no modifications should be made to the original metadata:

BEGDOC, ENDDOC, TEXT, BEGATTACH, ENDATTACH, PAGECOUNT, CUSTODIAN, RECORDTYPE, DATE, TIME, SENTDATE, SENTTIME, BEGINDATE, BEGINTIME, ENDDATE, ENDTIME, AUTHOR, FROM, CC, TO, BCC, SUBJECT, TITLE, FILENAME, FILEEXT, FILESIZE, DATECREATED, TIMECREATED, DATELASTMOD, TIMELASTMOD,

INTMSGID, INTMSGHEADER, NATIVELINK, INTFILPATH, EXCEPTION,
BEGATTACH.

7. Documents produced to the Committee should include an index describing the contents of the production. To the extent more than one CD, hard drive, memory stick, thumb drive, zip file, box, or folder is produced, each should contain an index describing its contents.
8. Documents produced in response to this request shall be produced together with copies of file labels, dividers, or identifying markers with which they were associated when the request was served.
9. When you produce documents, you should identify the paragraph(s) or request(s) in the Committee's letter to which the documents respond.
10. The fact that any other person or entity also possesses non-identical or identical copies of the same documents shall not be a basis to withhold any information.
11. The pendency of or potential for litigation shall not be a basis to withhold any information.
12. In accordance with 5 U.S.C. § 552(d), the Freedom of Information Act (FOIA) and any statutory exemptions to FOIA shall not be a basis for withholding any information.
13. Pursuant to 5 U.S.C. § 552a(b)(9), the Privacy Act shall not be a basis for withholding information.
14. If compliance with the request cannot be made in full by the specified return date, compliance shall be made to the extent possible by that date. An explanation of why full compliance is not possible shall be provided along with any partial production.
15. In the event that a document is withheld on the basis of privilege, provide a privilege log containing the following information concerning any such document: (a) every privilege asserted; (b) the type of document; (c) the general subject matter; (d) the date, author, addressee, and any other recipient(s); (e) the relationship of the author and addressee to each other; and (f) the basis for the privilege(s) asserted.
16. If any document responsive to this request was, but no longer is, in your possession, custody, or control, identify the document (by date, author, subject, and recipients), and explain the circumstances under which the document ceased to be in your possession, custody, or control.
17. If a date or other descriptive detail set forth in this request referring to a document is inaccurate, but the actual date or other descriptive detail is known to you or is otherwise apparent from the context of the request, produce all documents that would be responsive as if the date or other descriptive detail were correct.

18. This request is continuing in nature and applies to any newly-discovered information. Any record, document, compilation of data, or information not produced because it has not been located or discovered by the return date shall be produced immediately upon subsequent location or discovery.
19. All documents shall be Bates-stamped sequentially and produced sequentially.
20. Two sets of each production shall be delivered, one set to the Majority Staff and one set to the Minority Staff. When documents are produced to the Committee, production sets shall be delivered to the Majority Staff in Room 2157 of the Rayburn House Office Building and the Minority Staff in Room 2105 of the Rayburn House Office Building.
21. Upon completion of the production, submit a written certification, signed by you or your counsel, stating that: (1) a diligent search has been completed of all documents in your possession, custody, or control that reasonably could contain responsive documents; and (2) all documents located during the search that are responsive have been produced to the Committee.

Definitions

1. The term “document” means any written, recorded, or graphic matter of any nature whatsoever, regardless of how recorded, and whether original or copy, including, but not limited to, the following: memoranda, reports, expense reports, books, manuals, instructions, financial reports, data, working papers, records, notes, letters, notices, confirmations, telegrams, receipts, appraisals, pamphlets, magazines, newspapers, prospectuses, communications, electronic mail (email), contracts, cables, notations of any type of conversation, telephone call, meeting or other inter-office or intra-office communication, bulletins, printed matter, computer printouts, teletypes, invoices, transcripts, diaries, analyses, returns, summaries, minutes, bills, accounts, estimates, projections, comparisons, messages, correspondence, press releases, circulars, financial statements, reviews, opinions, offers, studies and investigations, questionnaires and surveys, and work sheets (and all drafts, preliminary versions, alterations, modifications, revisions, changes, and amendments of any of the foregoing, as well as any attachments or appendices thereto), and graphic or oral records or representations of any kind (including without limitation, photographs, charts, graphs, microfiche, microfilm, videotape, recordings and motion pictures), and electronic, mechanical, and electric records or representations of any kind (including, without limitation, tapes, cassettes, disks, and recordings) and other written, printed, typed, or other graphic or recorded matter of any kind or nature, however produced or reproduced, and whether preserved in writing, film, tape, disk, videotape, or otherwise. A document bearing any notation not a part of the original text is to be considered a separate document. A draft or non-identical copy is a separate document within the meaning of this term.
2. The term “communication” means each manner or means of disclosure or exchange of information, regardless of means utilized, whether oral, electronic, by document or otherwise, and whether in a meeting, by telephone, facsimile, mail, releases, electronic

message including email (desktop or mobile device), text message, instant message, MMS or SMS message, message application, or otherwise.

3. The terms “and” and “or” shall be construed broadly and either conjunctively or disjunctively to bring within the scope of this request any information that might otherwise be construed to be outside its scope. The singular includes plural number, and vice versa. The masculine includes the feminine and neutral genders.
4. The term “including” shall be construed broadly to mean “including, but not limited to.”
5. The term “Company” means the named legal entity as well as any units, firms, partnerships, associations, corporations, limited liability companies, trusts, subsidiaries, affiliates, divisions, departments, branches, joint ventures, proprietorships, syndicates, or other legal, business or government entities over which the named legal entity exercises control or in which the named entity has any ownership whatsoever.
6. The term “identify,” when used in a question about individuals, means to provide the following information: (a) the individual’s complete name and title; (b) the individual’s business or personal address and phone number; and (c) any and all known aliases.
7. The term “related to” or “referring or relating to,” with respect to any given subject, means anything that constitutes, contains, embodies, reflects, identifies, states, refers to, deals with, or is pertinent to that subject in any manner whatsoever.
8. The term “employee” means any past or present agent, borrowed employee, casual employee, consultant, contractor, de facto employee, detailee, fellow, independent contractor, intern, joint adventurer, loaned employee, officer, part-time employee, permanent employee, provisional employee, special government employee, subcontractor, or any other type of service provider.
9. The term “individual” means all natural persons and all persons or entities acting on their behalf.

Congress of the United States

Washington, DC 20515

September 25, 2020

The Honorable Chad F. Wolf
Acting Secretary
U.S. Department of Homeland Security
Washington, D.C. 20528

Dear Acting Secretary Wolf:

We write to request information about troubling recent news reports that the Department of Homeland Security (DHS) has conducted surveillance of protesters in Portland, Oregon.

A recent article in The Nation alleges that an interagency task force involving DHS and the Department of Justice (DOJ) conducted surveillance of protesters' phones in Portland. This article alleged both that the government conducted real-time surveillance of protesters' communications and government personnel later extracted data from protester's phones that had been seized.

Congress has enacted strict legal protections which require government agencies to obtain the approval of an independent judge before searching Americans' devices and surveilling their communications — absent an emergency. That is to prevent the government from suppressing legitimate free speech protected by the First Amendment and violating Americans' right to privacy, which is protected by the Fourth Amendment.

These recent reports, which allege that DHS has deployed high-tech surveillance technologies against protesters in Portland, raise serious concerns, which Congress has a responsibility to investigate. To that end, please provide us with answers to the following questions by October 9, 2020:

1. During a July 23, 2020, briefing for Senate intelligence committee staff, Brian Murphy, then the Acting Under Secretary for Intelligence and Analysis (I&A) stated that DHS I&A had neither collected nor exploited or analyzed information obtained from the devices or accounts of protesters or detainees. On July 31, 2020, Senator Wyden and six other Senators on the Senate Select Committee on Intelligence wrote to Mr. Murphy to confirm the statement he had made to committee staff. DHS has yet to respond to that letter. Please confirm whether or not Mr. Murphy's statement during the July 23, 2020, briefing was accurate at the time, and if it is still accurate.
2. Has DHS, whether directly, or with the assistance of any other government agency, obtained or analyzed data extracted from phones of protesters in Portland? If yes, for each phone, did the government obtain prior authorization from a judge before extracting data?
3. Has DHS, whether directly, or with the assistance of any other government agency, obtained or analyzed data collected through the surveillance of protesters' phones, including tracking their locations or intercepting communications content or metadata? If

yes, for each phone that was surveilled, did the government obtain prior authorization from a judge before conducting this surveillance?


4. Has DHS used commercial data sources, including open source intelligence products, to investigate, identify, or track protesters or conduct network analysis? If yes, please identify each commercial data source used by DHS, describe the information DHS obtained, how DHS used it, whether it was subsequently shared with any other government agency, and whether DHS sought and obtained authorization from a court before querying the data source.

Thank you for your attention to this important matter.

Sincerely,



Ron Wyden
United States Senator



Jeffrey A. Merkley
United States Senator



Earl Blumenauer
Member of Congress



Suzanne Bonamici
Member of Congress

Congress of the United States
Washington, DC 20515

June 10, 2020

The Honorable William P. Barr
United States Attorney General
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, D.C. 20530

Dear Attorney General Barr:

We write with great concern about law enforcement agencies targeting and surveilling protesters who are engaged in constitutionally protected expressions of free speech. Specifically, we request information about whether and how powerful surveillance technologies such as cell-site simulators (CSS) are being deployed against protesters, potentially chilling free speech. We are specifically troubled by a recent Justice Department memo authorizing the Drug Enforcement Administration (DEA) to “conduct covert surveillance” and “share intelligence with federal, state, local, and tribal counterparts” with regard to protests in the wake of George Floyd’s murder by Minneapolis police.

We know from House Oversight Committee investigations and the work of civil liberties organizations that the U.S. Government has historically used CSS to track suspects, obtaining massive amounts of data on innocent people in the process. CSS are capable of collecting geolocation information and even the content of SMS messages and phone calls without the knowledge of the cell phone owner. These CSS trick phones into thinking they are interacting with legitimate cell towers, but in reality are connecting to a third party’s device emitting strong broadcast signals. The D.C. Court of Appeals in 2017 ruled that such surveillance absent a warrant constitutes an illegal search in violation of the Fourth Amendment.

According to the *Wall Street Journal*, the Marshals Service – which the President deployed in Washington, D.C., on June 2 in response to protests – has outfitted Cessna planes with CSS known as “Dirtboxes” since at least 2014. The Dirtboxes are designed to pick up phone signals of anyone within range. According to *Wired* magazine, this “means that data on potentially tens of thousands of phones could be collected during a single flight.” More concerning is the fact that CSS technology has been loaned out to other agencies, including local police departments, with little to no oversight over their use, according to reports by WIRED magazine.

Given the lack of transparency and accountability regarding the transfer of this technology between and among agencies, we remain deeply concerned about its potential for surveillance abuse against innocent and vulnerable populations exercising their First Amendment rights. We request answers to the following questions about the Administration’s practices and legal posture with regard to surveillance policies by Friday, June 26 at the latest:

1. Why is the Drug Enforcement Agency involved in law enforcement related to protests protected by the First Amendment? What is the reason for activating the Attorney General's authority under 21 U.S.C. 878(a)(5) to authorize the DEA to enforce non-drug-related crimes?
2. To date, have any agencies within the Department of Justice (DOJ) used CSS, or related technologies, to intercept communications, intentionally disrupt communications to or from phones, track location information, or identify individuals participating in protests in the wake of George Floyd's murder? If yes, was the use of CSS authorized pursuant to a warrant?
3. In 2015, DOJ published a policy governing its use of CSS technology. Please confirm whether this policy is still in effect, and whether all uses of DOJ-owned CSS by government agencies related to the recent protests has complied with this policy.
4. If such technologies are deployed in the context of surveilling protesters, what measures are agencies taking to ensure that data from individuals is minimized and later purged if irrelevant from an investigatory standpoint?

Thank you for your attention to this matter.

Sincerely,



Ted W. Lieu
Member of Congress



Ron Wyden
United States Senator



Anna G. Eshoo
Member of Congress

Congress of the United States
Washington, DC 20515

June 8, 2020

The Honorable William P. Barr
Attorney General
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530

Dear Attorney General Barr:

We are gravely concerned by reports that the Drug Enforcement Administration (DEA) has been granted authority to conduct warrantless surveillance of Americans protesting in support of racial justice and an end to police brutality.¹ We write to ask that the Department of Justice immediately rescind this authority and ensure that DEA activities do not exceed the scope of authority granted to the agency by Congress.

Thousands of Americans have engaged in protests following the May 25, 2020 police killing of George Floyd. According to a Justice Department memo, on May 31, the Department approved a request from acting DEA Administrator Timothy J. Shea for authority to perform the following activities in response to these protests:

“(1) conduct covert surveillance and protect against threats to public safety; (2) share intelligence with federal, state, local, and tribal counterparts; (3) if necessary, intervene as Federal law enforcement officers to protect both participants and spectators in the protests; and (4) if necessary, engage in investigative and enforcement activity including, but not limited to, conducting interviews, conducting searches and making arrests for violations of Federal law.”²

DEA’s stated intention to “conduct covert surveillance” is extremely distressing. First, the memo fails to describe or place any guardrails around such surveillance, thus opening the door to sweeping, warrantless surveillance activities inconsistent with the preservation of civil liberties. The use of the term “covert” suggests that DEA’s actions will not be apparent to the public and could encroach upon activities wherein Americans have a reasonable expectation of privacy. It is also critical to note that Americans engaged in protests are protected by the First Amendment, and that exercising the constitutionally protected right to free speech is not evidence of a crime or intent to commit a crime. This surveillance will unquestionably have a chilling effect on Americans’ exercise of their First Amendment rights and could constitute an unconstitutional violation of their civil liberties.

¹ [Leopold, Jason and Cormier, Anthony. “The DEA Has Been Given Permission To Investigate People Protesting George Floyd’s Death.” *BuzzFeed News*. June 2, 2020.](#)

² [Memorandum for the Deputy Attorney General from Timothy J. Shea, Acting Administrator, Drug Enforcement Administration \(Obtained by *BuzzFeed News*\).](#)

DEA's history with respect to surveillance renders this new authority all the more troubling. In 2013, *Reuters* reported that DEA was "funneling information from intelligence intercepts, wiretaps, informants and a massive database of telephone records to authorities across the nation to help them launch criminal investigations of Americans."³ This report also revealed that DEA agents were "directed to conceal how such investigations truly begin - not only from defense lawyers but also sometimes from prosecutors and judges...federal agents are trained to "recreate" the investigative trail to effectively cover up where the information originated, a practice that some experts say violates a defendant's Constitutional right to a fair trial."⁴ A 2018 report by Human Rights Watch also described several troubling surveillance tactics employed by DEA. One example detailed the case of *United States v. Grobstein* wherein "defense attorneys alleged that a DEA agent secretly (and unlawfully) searched luggage left on a long-distance bus during a layover, then—after the passengers had re-boarded—approached the defendant seeking consent to search his bag."⁵

These examples indicate that DEA has engaged in surveillance practices in the past that were, at best, questionable and, at worst, illegal.

Finally, we are concerned by the Department's expansive interpretation of the law governing DEA authorities. The memo acknowledges that the scope of DEA's mission is statutorily "limited to enforcing Federal crimes related to drugs," but states that "the Attorney General is authorized to designate DEA to perform other law enforcement duties as he may deem appropriate."⁶ The Comprehensive Drug Abuse Prevention and Control Act of 1970 does authorize DEA agents to "perform such other law enforcement duties as the Attorney General may designate."⁷ However, this provision was long understood to refer exclusively to law enforcement activities related to drug laws; in 1988, the Department of Justice Office of Legal Counsel determined that the provision "pertains to general law enforcement work which, while not limited to the investigation of the drug laws, nevertheless arises from or is supplementary to it."⁸ The Office of Legal Counsel reversed that determination in 2003, alleging that there is "no warrant for restricting the provision to the investigation of offenses connected with narcotics cases" and that the legislative history of the law supports its expansive view.⁹ We are disturbed by the Department's decision to grant such broad and extensive authority to DEA based on a provision about which there is not absolute clarity.

To protest is to partake in a great American tradition dating back beyond our country's founding, to the struggle that led to its creation. We strongly oppose any action that infringes

³ [Shiffman, John and Cooke, Kristina. "Exclusive: U.S. directs agents to cover up program used to investigate Americans." *Reuters*. August 5, 2013.](#)

⁴ *Ibid.*

⁵ ["Dark Side: Secret Origins of Evidence in US Criminal Cases." *Human Rights Watch*. January 9, 2018.](#)

⁶ [Memorandum for the Deputy Attorney General from Timothy J. Shea, Acting Administrator, Drug Enforcement Administration \(Obtained by *BuzzFeed News*\).](#)

⁷ [21 U.S. Code § 878. Powers of enforcement personnel.](#)

⁸ ["Scope of the Attorney General's Authority to Assign Duties Under 21 U.S.C. § 878\(a\)\(5\)." Memorandum Opinion for the Deputy Attorney General from Jay S. Bybee, Assistant Attorney General, Office of Legal Counsel. March 24, 2003.](#)

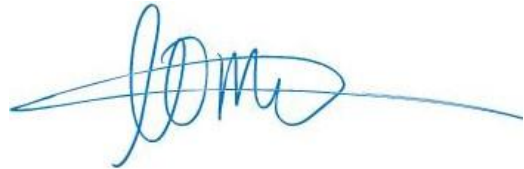
⁹ *Ibid.*

upon Americans' constitutional right to engage in protests and urge the Department to rescind immediately the sweeping authorities it has granted to DEA.

Sincerely,



ANDY LEVIN
Member of Congress



ILHAN OMAR
Member of Congress



JAMIE RASKIN
Member of Congress

Congress of the United States
Washington, DC 20515

September 23, 2020

The Honorable Joseph V. Cuffari,
Inspector General
Department of Homeland Security
245 Murray Lane, S.W.
Washington, D.C. 20528

Mr. Thomas A. Monheim, Acting Inspector
General of the Intelligence Community
Office of the Director of National
Intelligence
Washington, D.C. 20511

The Honorable Michael E. Horowitz,
Inspector General
Department of Justice
950 Pennsylvania Avenue, N.W.
Washington, D.C. 20530

Dear Inspector General Cuffari, Inspector General Horowitz, and Acting Inspector General Monheim,

We are extremely troubled by recent press reports alleging that elements of the Department of Homeland Security (DHS) and the Department of Justice (DOJ) wiretapped cell phone communications of protesters in Portland, Oregon. If these allegations are true, they are an affront to our civil liberties and potentially federal law. We ask that the three offices you lead jointly investigate these allegations immediately and expeditiously.

On September 21, 2020, an investigation published in *The Nation* titled “Federal Agencies Tapped Protesters’ Phones in Portland” reported several alarming allegations. The article reports that “DHS never came clean to the public about the full extent of its intelligence operations in Portland, which consisted of clandestine activities including interceptions of protesters’ phone calls conducted by a task force...” The article goes on to state that the interagency task force, which included DHS and DOJ, “used a sophisticated cell phone cloning attack—the details of which remain classified—to intercept protesters’ phone communications.” The intelligence activities are described as being part of the Low Level Voice Intercept operation, which was “far more invasive than aerial surveillance.” The article says a DHS official used resources of the Drug Enforcement Agency, an agency within DOJ, to access protesters’ phones.

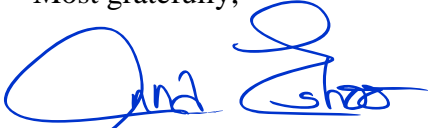
These are highly troubling allegations that, if true, could prove to be violations of law. The article reports that two unnamed intelligence officers “agreed that it had violated protocol,” and one of those officers was quoted as saying, “They were abusing people’s rights.”

Americans have a constitutionally protected right to peacefully protest actions of their government, and any efforts to thwart protests by the government is potentially

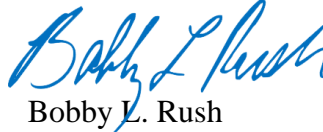
unconstitutional. We ask you to jointly investigate if the alleged surveillance violates the Constitution, federal law, Executive Orders, or departmental policies limiting electronic surveillance, or any other collection of information about U.S. persons.

We look forward to your timely response.

Most gratefully,



Anna G. Eshoo
Member of Congress



Bobby L. Rush
Member of Congress

U.S. House of Representatives
Committee on the Judiciary
Washington, DC 20515-6216
One Hundred Sixteenth Congress

June 5, 2020

The Honorable William P. Barr
Attorney General
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530

The Honorable Timothy J. Shea
Acting Administrator
U.S. Drug Enforcement Administration
8701 Morrisette Drive
Springfield, VA 22152

Dear Attorney General Barr and Acting Administrator Shea:

We are deeply concerned with reports that on May 31, 2020, Deputy Attorney General Jeffrey A. Rosen signed a request by Acting U.S. Drug Enforcement Administration (DEA) Administrator Timothy J. Shea to temporarily expand the law enforcement authority to DEA employees and agents to extend beyond enforcement of Title 21.¹ While there have been instances of unrest, the overwhelmingly peaceful nature of the protests that have taken place around the country do not warrant this expansion of DEA authority, even if it is temporary in nature, especially given the Agency's past record.

The DEA's narcotics interdiction tactics are not appropriate measures to address the limited violence that has taken place over the past few days or to monitor peaceful protests. The DEA's rigid refusal to consider, let alone adopt, even minor reform of the way it carries out business portends a further unnecessary escalation of this week's protests. In the past five years alone, the DEA has suffered from a mounting crisis that includes corruption and firearms offenses.² This is hardly a record that commands confidence that the DEA will appropriately and constitutionally implement its expanded authority, particularly when First Amendment rights are at stake.

Furthermore, the DEA has a history and practice of disproportionately targeting people of color. A 2009 evaluation by the Department of Justice's Bureau of Justice Statistics found that Latino suspects constituted 46% of arrestees although they make up only 16 percent of the general U.S.

¹ Jason Leopold & Anthony Carter, *The DEA Has Been Given Permission to Investigate People Protesting George Floyd's Death*, BuzzFeed, June 2, 2020.

² Assoc. Press, *Very Unprepared: DEA Shakeup Followed Mounting Criticism*, May 21, 2020.

population.³ Of the total arrests of male suspects by the DEA, 25% were marijuana related.⁴ This Administration's counterproductive focus on non-violent drug offenses is a plain reminder that the DEA is out of touch with the Nation's shift from the drug war model to policies of substance abuse treatment, rescheduling drugs, legalizing marijuana, and reducing harsh drug sentences. To the extent the DEA mirrors the views of this Administration, it is out of sync with more evidence-based drug policy trends in the country. Wider deployment of the DEA may only continue the disproportionate arrest trends that, in part, motivate the expressions of outrage that we are witnessing.

The expansion of the DEA's law enforcement authority, including the use of "covert surveillance" and collection of intelligence, is unwarranted and antithetical to the American people's right to peacefully assemble and to exercise their Constitutional rights without undue intrusion. The House Judiciary Committee has a duty to ensure that the administration of justice in our country is fair and that individuals can freely exercise their constitutionally protected rights. For these reasons, we ask that you immediately rescind the expanded authorities Mr. Rosen has granted to the DEA. We also ask that you provide us a briefing detailing the timeline and rationale for the expansion of authority. Please reach out to committee staff to schedule the briefing by no later than June 11, 2020.

Sincerely,



Jerrold Nadler
Chairman



Karen Bass
Chair, Subcommittee on Crime,
Terrorism, and Homeland Security

cc: The Honorable Jim Jordan, Ranking Member, House Committee on the Judiciary

³ Mark Motivans, *Federal Justice Statistics, 2009*, U.S. Dep't of Justice Bureau of Justice Stats., Dec. 2011, <https://www.bjs.gov/content/pub/pdf/fjs09.pdf>; Sharon Ennis, et al., 2010 Census Briefs: The Hispanic Population: 2010, U.S. Dep't of Commerce, May 2011, <https://www.census.gov/prod/cen2010/briefs/c2010br-04.pdf>.

⁴ Motivans, *Federal Justice Statistics, 2009*.



**Permanent Select Committee
on Intelligence
U.S. House of Representatives**

July 22, 2020

The Honorable Chad F. Wolf
Acting Secretary of Homeland Security
U.S. Department of Homeland Security
Washington, D.C. 20528

The Honorable Brian Murphy
Acting Under Secretary
Office of Intelligence and Analysis
U.S. Department of Homeland Security
Washington, D.C. 20528

Dear Acting Secretary Wolf and Acting Under Secretary for Intelligence and Analysis Murphy:

Troubling media accounts suggest that the Department of Homeland Security's (DHS or the Department) Office of Intelligence and Analysis (I&A) and certain other Department components may be engaging in unprecedented, "expanded" intelligence and related activities — in support of a policy that exceeds the Department's historical mission, and contrary to constitutionally-protected rights of speech, assembly, and peaceful protest. Such accounts are especially disturbing as Americans are learning about the Administration's unilateral deployment of federal officers, many apparently from DHS components, in Portland over the objections of state and local officials. These DHS officers reportedly have been wearing camouflage — according to the *New York Times*, also without obvious markings or identification — using unmarked vehicles, and detaining peaceful protestors without clear authority or cause.¹

I thus write to request information about any such activities the Department, I&A, the Homeland Security Intelligence Enterprise, or any of the Department's other components may have undertaken or plan to undertake, or for which support has been requested or suggested, in connection with President Trump's Executive Order on Protecting American Monuments, Memorials, and Statues and Combating Recent Criminal Violence (Executive Order).²

¹ *Federal Agents Unleash Militarized Crackdown on Portland*, The New York Times, July 17, 2020, <https://www.nytimes.com/2020/07/17/us/portland-protests.html?referringSource>; "It Was Like Being Preyed Upon": Portland Protesters Say Federal Officers in Unmarked Vans are Detaining Them, The Washington Post, July 17, 2020, <https://www.washingtonpost.com/nation/2020/07/17/portland-protests-federal-arrests/>.

² *Executive Order on Protecting American Monuments, Memorials, and Statues and Combating Recent Criminal Violence*. The White House. June 26, 2020. <https://www.whitehouse.gov/presidential-actions/executive-order-protecting-american-monuments-memorials-statues-combating-recent-criminal-violence/>.

On July 20, *the Washington Post*³ reported that the Department "has authorized its personnel to collect information on protesters who threaten to damage or destroy public memorials and statues, regardless of whether they are on federal property, a significant expansion of authorities that have historically been used to protect landmarks from terrorist attacks." The document underlying this account, allegedly obtained by the *Post*, has been described as a "job aid" for personnel implementing the Executive Order "targeting protesters who threatened to remove statues honoring Confederate officers and other people they consider racist."

Along similar lines, *Lawfare*⁴ that same day described an unclassified memorandum titled, "Job Aid: DHS Office of Intelligence & Analysis Activities in Furtherance of Protecting American Monuments, Memorials, Statues, and Combatting Recent Criminal Violence." According to *Lawfare*, the memorandum, which contains legal guidance regarding I&A's "expanded" intelligence activities in support of the Executive Order, "covers significantly *more* than just planned attacks on federal personnel or facilities. It appears also to include planned vandalism of Confederate (and other historical) monuments and statues, whether federally owned or not."

If true, this marks a significant change. So far as the Committee is aware, never before has the Department sought to so aggressively counter potential threats of graffiti, vandalism, or other minor damage to monuments, memorials, statutes, and federal buildings – including those not found on federal lands – in the same fashion as it would seek to counter acknowledged threats to U.S. homeland security, such as terrorism, significant cyber intrusions, or attacks against federal facilities or personnel. Nor is the Committee aware that the Department has ever sought to use and so distort its existing authorities to protect such facilities and personnel as justification for directing its limited intelligence authorities to collect information on and to target persons exercising their legal rights and engaging in activity protected under the First Amendment.

To carry out its authorized responsibilities, the House Permanent Select Committee on Intelligence (Committee) thus respectfully requests that, on or before **12 p.m. on Friday, July 24, 2020**, you provide to the Committee:

1. As the Department has committed, a briefing on the allegations raised in the *Washington Post* and *Lawfare* accounts;
2. Unredacted copies of all documents, communications or other materials, regardless of form, produced by or in the custody or control of the Department, I&A, the Homeland Security Intelligence Enterprise, or any Department component, regarding any Department intelligence activities undertaken, requested or planned in connection with the implementation of or support for the Executive Order, including:

³ *DHS authorizes personnel to collect information on protesters it says threaten monuments*, The Washington Post, July 20, 2020. https://www.washingtonpost.com/national-security/dhs-authorizes-personnel-to-collect-information-on-protesters-it-says-threaten-monuments/2020/07/20/6f58867c-cace-11ea-b0e3-d55bda07d66a_story.html.

⁴ *DHS Authorizes Domestic Surveillance to Protect Statues and Monuments*. Lawfare. July 20, 2020. <https://www.lawfareblog.com/dhs-authorizes-domestic-surveillance-protect-statues-and-monuments>.

- a. All memoranda, job aids, and other documents or communications regarding such intelligence activities, to include any legal guidance or analysis of the legal basis for such activities;
 - b. In addition to finished intelligence products already made available to the Committee, all other intelligence products, intelligence reports or other intelligence information collected or otherwise obtained or generated by Department components in connection with implementation of or support for the Executive Order and deployment of DHS officers to Portland and other areas;
 - c. The Department's information or intelligence requirements, and any attendant collection plans or activity.
3. All e-mails, memoranda, or other communications or documents, regardless of form, between the Department and any of its components, and the Department of Justice or the White House, regarding Department intelligence activities undertaken, requested or planned in connection with implementation of or support for the Executive Order.

You are required by law to fulfill these requests. 50 U.S.C. § 3092 obligates the heads of Departments involved in intelligence activities to keep the Committee fully and currently informed of such activities. The statute further obligates such officials, on the Committee's request, to provide "any information or material concerning intelligence activities (including the legal basis under which the intelligence activity is being or was conducted)."

The American people deserve, and expect, that the Intelligence Community and DHS will scrupulously honor obligations to respect civil liberties when conducting the vital mission of keeping our nation safe. At this key moment in our history, it is critical that the public retains confidence and trust in the Intelligence Community and federal law enforcement. The Homeland Security Intelligence Enterprise, sitting uniquely at the intersection of these two institutions, has a special obligation in this regard.

Thank you for your timely cooperation.

Sincerely,



Adam B. Schiff
Chairman

cc: The Honorable Devin Nunes
Ranking Member

EDWARD J. MARKEY
MASSACHUSETTS

COMMITTEES:

ENVIRONMENT AND PUBLIC WORKS

FOREIGN RELATIONS

RANKING MEMBER:

SUBCOMMITTEE ON EAST ASIA, THE PACIFIC,
AND INTERNATIONAL CYBERSECURITY POLICY

COMMERCE, SCIENCE, AND TRANSPORTATION

RANKING MEMBER:

SUBCOMMITTEE ON SECURITY

SMALL BUSINESS AND ENTREPRENEURSHIP

CHAIRMAN:

U.S. SENATE CLIMATE CHANGE TASK FORCE

United States Senate

SUITE SD-255
DIRKSEN BUILDING
WASHINGTON, DC 20510-2107
202-224-2742

975 JFK FEDERAL BUILDING
15 NEW SUDBURY STREET
BOSTON, MA 02203
617-565-8519

222 MILLIKEN BOULEVARD, SUITE 312
FALL RIVER, MA 02721
508-677-0523

1550 MAIN STREET, 4TH FLOOR
SPRINGFIELD, MA 01103
413-785-4610

June 8, 2020

Mr. Hoan Ton-That
Founder & Chief Executive Officer
Clearview AI
214 W 29th St, 2nd Floor
New York, NY 10001

Dear Mr. Ton-That:

I write regarding recent reports that law enforcement agencies in cities experiencing protests inspired by the killing of George Floyd may be utilizing Clearview AI's facial recognition technology.¹ I have previously written to you about law enforcement's use of your technology, expressing my fear that it could infringe on Americans' civil liberties, including their privacy rights, but your responses failed to allay my concerns. In light of the ongoing protests and demonstrations across the country, I write with additional questions and to reiterate the need for your company to take urgent action to prevent the harmful use of its product.

As demonstrators across the country exercise their First Amendment rights by protesting racial injustice, it is important that law enforcement does not use technological tools to stifle free speech or endanger the public. Civil liberties experts have expressed concerns that unregulated deployment of facial recognition technologies could allow law enforcement agencies to identify and arrest protesters long after the demonstrations end.² The prospect of such omnipresent surveillance also runs the risk of deterring Americans from speaking out against injustice for fear of being permanently included in law enforcement databases.³ These concerns do not exist

¹ See Caroline Haskins & Ryan Mac, *Here Are The Minneapolis Police's Tools To Identify Protesters*, BUZZFEED NEWS (May 29, 2020), <https://www.buzzfeednews.com/article/carolinehaskins1/george-floyd-protests-surveillance-technology>.

² *Police can track protesters even after the demonstrations end*, MARKETPLACE TECH (Jun. 2, 2020), <https://www.marketplace.org/shows/marketplace-tech/police-protesters-surveillance-tracking-facial-recognition/>.

³ See Albert Fox Cahn & Zachary Silver, *The long, ugly history of how police have tracked protesters*, FAST COMPANY (Jun. 2, 2020), <https://www.fastcompany.com/90511912/the-long-ugly-history-of-how-police-have-tracked-protesters>.

purely in the abstract; according to reports, they are common among protesters in countries where local law enforcement agencies broadly deploy facial recognition technologies.⁴

Unfortunately, your responses to my previous inquiries have failed to provide the information necessary to assure the public that law enforcement's use of your technology in the United States will not violate Americans' rights. To date, your company has not been adequately transparent about several issues, including how law enforcement agencies procure access to Clearview AI's app; how Clearview AI ensures that the software will not be misused; and whether Clearview AI's technology is free of dangerous biases and inaccurate results. Although you have previously argued that your technology's many potential harms are "speculative,"⁵ waiting for them to occur, especially in the current environment, would be foolhardy.

In light of these concerns, I request responses to the following questions by June 22, 2020:

1. You have previously refused to provide a list of Clearview's clients.⁶ Given the renewed public interest in identifying law enforcement agencies with access to your technology, please list any law enforcement agencies that Clearview AI has marketed to since May 25, 2020.
 - a. In addition, please list any law enforcement agencies that Clearview AI has signed new contracts with since May 25, 2020.
2. Has search traffic on Clearview AI increased, week-over-week, during the weeks of May 25 and June 1, compared to the two prior weeks? If so, by how much?
3. Please describe the process of granting a free trial of Clearview to a potential law enforcement client. What steps does Clearview AI take to verify the identity of the client requesting your services, and what level of authorization does Clearview require from the organization to grant a free trial?
4. In your March 24, 2020 response letter, you failed to indicate whether Clearview AI considers whether law enforcement agencies have a history of unlawful or discriminatory policing practices when deciding to whom it will market or sell its technology.⁷

⁴ See, e.g., Rosalind Adams, *Hong Kong Protesters Are Worried About Facial Recognition Technology. But There Are Many Other Ways They're Being Watched*, BuzzFeed News (Aug. 17, 2019), <https://www.buzzfeednews.com/article/rosalindadams/hong-kong-protests-paranoia-facial-recognition-lasers>; Alexandra Ulmer & Zeba Siddiqui, *India's use of facial recognition tech during protests causes stir*, REUTERS (Feb. 17, 2020), <https://www.reuters.com/article/us-india-citizenship-protests-technology/indias-use-of-facial-recognition-tech-during-protests-causes-stir-idUSKBN20B0ZQ>.

⁵ See Clearview Letter to Senator Edward J. Markey (Mar. 24, 2020) ("We share your concern in preventing abuse of this critical law enforcement tool. To date, we are aware of none. Fortunately, all the harm is speculative.").

⁶ See *id.*

⁷ See *id.*

- a. Please describe the process of forming a contract for Clearview AI with a law enforcement client.
 - b. What steps does Clearview AI take to verify the identity of the client seeking your services?
 - c. What level of authorization does Clearview AI require from the organization to sign a contract?
 - d. What vetting does Clearview AI itself conduct before granting an entity access to your technology?
5. Will you commit to explicitly prohibiting law enforcement agencies or others from using Clearview AI's technology to monitor or identify peaceful protestors? If so, please detail how you will do so. If not, why not?
6. You have acknowledged in previous letters that you have developed a mechanism for individuals to remove individual photos from the Clearview AI database.⁸ Now, presumably to comply with state data privacy laws,⁹ you have established additional mechanisms for California and Illinois residents to opt-out of the Clearview AI database entirely by providing an image of themselves.¹⁰ Will you commit to providing these opt-out mechanisms to residents of all 50 states? If not, why not?
7. Does Clearview AI's opt-out mechanism prevent your company from matching a person's face to images in the Clearview AI database on a permanent and ongoing basis? Or does the mechanism only deindex photos that exist in the database at the time a person requests to opt-out? If the latter, will you commit to developing a tool that allows for people to permanently opt-out?
8. In your May 15, 2020 response letter, you did not commit to submitting Clearview AI's technology for an independent assessment of accuracy and bias by facial recognition experts, including testing for error rates for true negatives, false matches, and people of color, and publish the results of this assessment publicly. Given the concerns raised by civil liberties experts that false positives could lead to innocent protesters (especially women and people of color) being arrested or confronted by police,¹¹ will you now commit to submitting Clearview AI to such an assessment?

⁸ See *id.*; Clearview Letter to Senator Edward J. Markey (May 15, 2020).

⁹ See California Consumer Privacy Act of 2018, Cal.Civ.Code §1798.100 (2018); Biometric Information Privacy Act, 740 ILCS 14 (2008).

¹⁰ *Privacy Request Forms*, CLEARVIEW AI, <https://clearview.ai/privacy/requests>.

¹¹ See Maya Shwayder, *Police facial recognition tech could misidentify people at protests, experts say*, DIGITAL TRENDS (Jun. 2, 2020), <https://www.digitaltrends.com/news/police-protests-facial-recognition-misidentification/>.

Mr. Hoan Ton-That

June 8, 2020

Page 4

9. You have previously confirmed that Clearview AI is engaging with government entities regarding the potential use of Clearview AI's technology for COVID-19 contact tracing efforts.¹² Will you commit to ensuring that any images, personal information, or other data that Clearview AI collects as part of any contact tracing program will not be accessible to law enforcement agencies who contract with it?

Clearview AI has an obligation to proactively ensure that its clients do not use its technology in ways that harm the public. I urge you to take every step necessary to ensure that your technology will not force Americans to choose between sacrificing their rights to privacy or remaining silent in the face of injustice.

Thank you for your continued attention to these important matters. If you have any questions, please contact my office at 202-224-2742.

Sincerely,



Edward J. Markey
United States Senator

¹² See Clearview Letter to Senator Edward J. Markey (May 15, 2020).