April 23, 2013

Docket Operations, M – 30
U.S. Department of Transportation
1200 New Jersey Avenue, SE
Room Wl2-140, West Building Ground Floor
Washington, DC 20590-0001

Re: Federal Aviation Administration: "Unmanned Aircraft System Test Site Program," Docket No. FAA-2013-0061

The Constitution Project (TCP) respectfully submits the following comment in response to the Federal Aviation Administration's (FAA) request for comments regarding the privacy concerns raised by the creation of the unmanned aircraft system (UAS) test site program. TCP was a signer of the coalition petition, organized by the Electronic Privacy Information Center (EPIC), urging the FAA to develop privacy regulations for the use of drones in U.S. airspace. TCP commends the FAA for issuing this request for public comment and welcomes the opportunity to participate in the ongoing discussion of privacy concerns associated with the use of UAS's in domestic airspace.

TCP is a non-profit organization that promotes and defends constitutional safeguards and seeks bipartisan solutions to preserve civil liberties. TCP's bipartisan Liberty and Security Committee, launched in the aftermath of September 11th, brings together members of the law enforcement community, legal academics, former government officials, and advocates from across the political spectrum who develop and advance proposals to protect civil liberties as well as our nation's security. TCP's Liberty and Security Committee has examined a variety of privacy and technology issues including publishing a report in 2007 entitled *Guidelines for Public Video Surveillance: A Guide to Protecting Communities and Preserving Civil Liberties.*[1] This report outlines the privacy concerns raised by the use of public video surveillance systems, recommends best practices for incorporating privacy safeguards into the rules governing such camera systems, and includes model legislation for jurisdictions to adapt and adopt. Many of these same privacy concerns and principles apply to the use of UAS's for surveillance purposes, and by extension, to the operation of the unmanned aircraft system test site programs. Therefore TCP recommends similar public accountability procedures should be adopted to govern operation of the UAS test site program.

[1] The Constitution Project's Liberty and Security Committee, *Guidelines for Public Video Surveillance: A Guide to Protecting Communities and Preserving Civil Liberties* (2007) (hereinafter *TCP Guidelines* Report), available at http://www.constitutionproject.org/pdf/Video_Surveillance_Guidelines_Report_w_Model_Legislation4.pdf .

In this comment, TCP addresses the constitutional rights implicated by the use of unmanned aircraft systems for surveillance purposes and the procedures TCP recommends for establishing the UAS test sites in a way that protects the constitutional rights and values at issue. These recommendations also cover the appropriate uses of collected information and regulations for private entity to government information sharing. Finally, this comment includes recommendations for the use of UAS's at the border, and how the FAA should incorporate privacy rules even for use in these areas.

TCP is chiefly concerned with the regulations covering government use of UAS's in domestic airspace, as those uses directly implicate Americans' constitutional rights, including rights under the First and Fourth Amendments. As described in detail in TCP's video surveillance report, the rights to privacy, anonymity, free speech, and assembly among others,[2] are all threatened by the pervasive use of powerful electronic surveillance technologies. As technology is developing much more quickly than the law, it is important that the FAA take this opportunity to create regulations to ensure that government implementation of new technologies does not erode privacy protections in the digital age. In addition, TCP recognizes that commercial and private use of UAS's raise similar privacy concerns and urges that the recommendations below should be applied to commercial and private use of UAS's to the extent applicable. TCP's recommendations include reporting requirements, development of publicly available privacy policies, limits to what and where surveillance drones can record, clear guidelines for threshold requirements for different kinds of information compilation, use restrictions, and data safeguards.

Protection of Constitutional Rights and Interests

Not all UAS uses implicate constitutional rights and interests. For example, using UAS's to deploy sensors to monitor environmental conditions raises no constitutional red flags. On the other hand, UAS's are now capable of carrying cameras with gigapixel photo technology, infrared cameras, sound and motion detectors, and other devices that can be used to monitor people and their activities; it is this type of UAS application that raises constitutional concerns. The FAA regulations should provide a framework to make sure that the impact on privacy rights is minimal for all cases in which law enforcement agencies use UAS's to monitor people or their activities. The technology available to conduct electronic surveillance is developing much more rapidly than the law governing application of these new tools. It is critical that the legal rules recognize the impact of these technologies, and incorporate sufficient safeguards to protect constitutional rights in the digital age.

In *Katz v. United States*, the Harlan concurrence developed the Court's modern Fourth Amendment test for when privacy rights are implicated: (1) that a person "have exhibited an

[2] *TCP Guidelines* Report at 8-9.

actual (subjective) expectation of privacy" and, (2) that the "expectation be one that society is prepared to recognize as 'reasonable.'"[3] In *Katz*,[4] the Court determined that an unconstitutional Fourth Amendment search occurred when the police department tapped a public telephone booth, without a warrant, to eavesdrop on a series of conversations. For decades following *Katz*, the widely accepted doctrine was that individuals had no reasonable expectation of privacy when they were in public spaces.[5] However, recent cases have shown that the Supreme Court is starting to recognize that powerful new surveillance technologies may change the traditional analysis.[6]

In the past dozen years, the Supreme Court has begun to acknowledge the power of modern technology and the effect that such tools can have on traditional Fourth Amendment analysis. In *Kyllo v. United States*, the Court held that when law enforcement officers rely upon technology that is not used by the general public to gather information that, without the use of such technology, could not be obtained without a search warrant, a search has occurred and a warrant is required.[7] *Kyllo* involved heat sensing technology that could effectively search inside a home, the zone historically subject to the most stringent Fourth Amendment protection.

Last year, in *United States v. Jones*,[8] the Court extended this recognition of the intrusive power of electronic surveillance tools in a case involving the use of public roads. The Court held that attaching a GPS device to a car and using it to monitor and track the movement of the vehicle constantly for a full month, constituted a Fourth Amendment search even though the car only traveled on public roads. Although the Court majority decided the case on relatively narrow grounds, the two concurrences in *Jones*, covering a total of five Justices, show that a majority of Justices have begun to recognize the intrusiveness of more and more powerful electronic surveillance technologies and how continuous use of such technologies over extensive periods of time can compromise a reasonable expectation of privacy.[9] Justice Alito noted the threat of continuous monitoring technology in his concurrence, stating "the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy."[10] Justice Sotomayor went even further in her concurrence, declaring that even short term monitoring may require "particular attention"[11] because "GPS monitoring generates a precise, comprehensive

[3] *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J. concurring).
[4] *Katz*, 389 U.S. at 353.
[5] *See, e.g.*, Cal. v. Ciraolo, 476 U.S. 207 (1986) (stating that what a person exposes to the public is not subject to Fourth Amendment protection when there is no physical intrusion).
[6] *See, e.g., Kyllo v. United States*, 533 U.S. 27 (2001); *United States v. Jones* 132 S. Ct. 945 (2012).
[7] *Kyllo*, 533 U.S. at 34-35.
[8] *Jones*, 132 S. Ct. at 949.
[9] *Id.* at 954 (Sotomayor, J., concurring) (agreeing with Justice Alito's concurrence and recognizing that "where electronic or other novel modes of surveillance that do not depend upon a physical invasion on property" a long period of electronic monitoring impinges on a reasonable expectation of privacy even without a physical trespass); *Id.* at 958 (Alito, J., concurring).
[10] *Id.* at 964 (Alito, J., concurring).
[11] *Id.* at 954 (Sotomayor, J., concurring).

record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."[12]

Additionally, if government surveillance cameras monitor and record the movements and activities of individuals, this can chill First Amendment rights of expression and association. The threat of government monitoring may be enough to deter citizens from freely exercising these rights. Therefore the regulations governing the use of surveillance cameras and other devices on UAS's should be crafted to incorporate adequate safeguards to minimize this threat.

In order to minimize the possible infringement on constitutional rights, the scope of a planned UAS must first be explicitly defined and made public. The importance of the FAA's assertion in the notice that "privacy policies should be updated as necessary to remain operationally current and effective" should be highlighted, because a big challenge today is that Congress and state legislatures are still struggling to catch up with developing technology. [13] However, the specifications set forth in the notice's proposed privacy requirements numbers one, calling for public availability of privacy policies based on the Fair Information Practice Principles (FIPPs), [14] and two, requiring compliance with current federal and state laws, are helpful but not sufficient. While TCP applauds the inclusion of the FIPPs in the request for comments and the FAA's expressed desire to include reporting requirements for the UAS test site programs, simple compliance with current laws is not enough. The FAA needs to require privacy best practices that can be applied to current technology and can be advanced when necessary to encompass new technology.

As set forth in more detail below, to address the constitutional issues raised by the use of UAS's for government surveillance, the regulations of such test sites should limit the geographic scope that the UAS will cover and impose limits on exactly what kinds of locations and actions can be included in the surveillance area. Additionally, the regulations should impose limits on the use of footage from the UAS, following the FIPPs principle of use limitation. Finally, these regulations should also address the use of UAS surveillance technology at our national borders, recognizing that although the standards may be different, the Fourth Amendment still applies at the border.

---

[12] *Id.*

[13] *See, e.g., United States v. Jones* 132 S. Ct. 945, 964 (2012) (Alito, J. concurring)(stating that in the face of rapid technological advances privacy solutions should come from the legislature but recognizing that neither Congress nor most of the states have enacted statutes to regulate GPS tracking).

[14] Federal Trade Commission, Fair Information Practice Principles, available at http://www.ftc.gov/reports/privacy3/fairinfo.shtm.

Develop Limits on Locations and Activities Included in UAS Surveillance

There are several different purposes for which government entities may seek to rely upon UAS's to conduct surveillance. These include monitoring for public safety and surveillance for law enforcement purposes. As discussed in detail in TCP's Liberty and Security Committee's video surveillance report, the scope and capabilities of a surveillance program should be carefully designed to serve its intended purpose, to minimize the program's impact on constitutional rights.[15] For example, if UAS's are being used to monitor an area during a natural disaster to inform authorities about when and where they need to deploy rescue units, there may be no need to record or at least no need to retain footage once the natural disaster has ended.

The UAS rules should require that systems must be carefully designed to serve their intended government purposes and that they do not intrude unnecessarily on individuals' privacy. This should include limits on the geographic scope and capabilities of the surveillance to be conducted. For example, law enforcement officials may seek to rely upon UAS surveillance technology in an attempt to cut down crime rates, asserting that UAS's would have a lower overhead cost than having law enforcement officers physically patrolling the same areas. The rules should require that the geographic scope of such UAS surveillance be specifically tailored to minimize the imposition on privacy rights while still reasonably furthering the purposes of general crime reduction.[16] Limiting the locations and the kinds of activities that can be included within the scope of UAS surveillance follows the FIPPs minimization principle and will therefore help curtail any intrusion on privacy rights. Similarly, UAS surveillance should be limited so that cameras and other detection devices cannot look inside the windows of homes or into private, covered areas around the home.[17]

Additionally, as noted above, the public has a First Amendment protected right to participate in political expression or religious assembly, including the right to engage in such activities anonymously.[18] Safeguards should be put in place to limit the identification and recording of individuals during surveillance that encompasses these kinds of First Amendment protected activities.

Detail Explicit Use Restrictions on Live Stream and Recorded UAS Footage

The UAS rules should also impose limits on how surveillance footage or other evidence from surveillance devices may be used, both in real time and in later review of compiled material.[19] The ability to create a database of the movements of identified individuals

[15] *TCP Guidelines* Report at 19-20.
[16] *TCP Guidelines* Report at 19.
[17] *TCP Guidelines* Report at 4.
[18] *TCP Guidelines* Report at 6.
[19] *TCP Guidelines* Report at 5.

undermines a reasonable expectation of privacy, as well as anonymity and freedom of association – rights protected by the First and Fourth Amendments.[20] When surveillance focuses on a specific individual, or when law enforcement seeks to compile evidence on a specific individual from databases created from UAS surveillance, these constitutional rights are implicated. While such tools should be available to investigate crimes, safeguards are needed to ensure that law enforcement officers establish the proper criminal predicate and avoid monitoring innocent individuals. For these reasons, law enforcement officials should be required to obtain a warrant based on probable cause before they are allowed to use a UAS surveillance live stream or recorded footage to continuously track an individual or compile information about a specific individual from UAS surveillance databases. Additionally, there should be use restrictions in place that prohibit the wide sharing of recorded surveillance footage beyond the scope of its original purpose.

In addition, although private UAS operators are not covered by constitutional requirements, in many instances private operators may seek to share data collected by UAS's with the government. In order to prevent circumvention of government surveillance and recording protocols, the same rules should apply when the government receives surveillance information from private or commercial UAS operators as when the government is the one collecting the information.

Include Guidelines for Use of UAS's in Maintaining Border Security

One of the government UAS uses that is already in operation is the Department of Homeland Security's program to rely on UAS's to conduct surveillance at the border. While this may be a valid and appropriate use of UAS's for surveillance, it is still critical to incorporate safeguards for Fourth Amendment rights. As the U.S. Court of Appeals for the Ninth Circuit recently recognized, even at the border "individual privacy rights are not abandoned."[21]

Addressing searches of electronic devices at the border, TCP's Liberty and Security Committee released a report in 2011 entitled *Suspicionless Border Searches of Electronic Devices: Legal and Privacy Concerns with The Department of Homeland Security's Policy*.[22] In the report, the committee explained how modern technology dramatically expands the scope and nature of information people may carry with them as they cross the border.[23] Therefore, the report urged that to preserve the historically narrow scope of the border search exception,

---

[20] *TCP Guidelines* Report at 27.
[21] *United States v. Cotterman*, 2013 U.S. App. LEXIS 4731, at *13 (quoting *United States v. Seljan*, 547 F.3d 993, 1000 (9th Cir. 2008).
[22] The Constitution Project's Liberty and Security Committee, *Suspicionless Border Searches of Electronic Devices: Legal and Privacy Concerns with The Department of Homeland Security's Policy* (2011) (hereinafter *TCP Border Searches* Report), available at http://www.constitutionproject.org/pdf/Border_Search_of_Electronic_Devices_0518_2011.pdf .
[23] *TCP Border Searches* Report at 2.

government agents should only be permitted to search the contents of electronic devices such as laptops if they have reasonable suspicion of criminal wrongdoing. Many of the concerns for safeguarding Fourth Amendment rights detailed in this report are applicable to the use of UAS surveillance in maintaining border security.

Last month, in *United States v. Cotterman*, the Ninth Circuit, sitting en banc, ruled that the government must have reasonable suspicion when conducting a forensic search of an electronic device like a laptop at the border.[24] This decision recognizes that while there is a reduced level of privacy protection at the border, this does not strip an individual of constitutionally protected right to privacy, and it "does not mean . . . that at the border 'anything goes.'"[25] Thus, although a different standard of Fourth Amendment protection applies to the areas immediately around our national borders,[26]even in border areas, indiscriminate searches and surveillance are not constitutional.[27] The FAA's UAS regulations should therefore ensure that there are appropriate safeguards in place to maintain Fourth Amendment protection at and around our national borders.

Conclusion

Again, TCP commends the FAA for issuing this request for comments regarding privacy protections to be incorporated into the UAS test site program. TCP urges that rules be adopted to safeguard constitutional rights to privacy, free speech, and assembly. In order to address these concerns, and minimize the actual impact on these rights, TCP recommends that the FAA regulations include: limits to the geographic scope that the UAS can cover and the activities that can be included in the UAS surveillance; explicit guidelines for the use of live stream and recorded footage, including a warrant requirement for law enforcement tracking of a specific individual; restrictions on sharing footage; and guidelines for the use of UAS surveillance at the nation's borders.

Respectfully submitted,

Sharon Bradford Franklin
Senior Counsel
The Constitution Project
1200 18th Street, NW
Suite 1000
Washington, DC 20036

[24] *Cotterman*, 2013 U.S. App. LEXIS 4731, at *17 (9th Cir. March 8, 2013).
[25] *Id.* at *13 (quoting *United States v. Seljan*, 547 F.3d 993, 1000 (9th Cir. 2008)).
[26] *United States v. Flores-Montano*, 541 U.S. 149, 154 (2004).
[27] *City of Indianapolis v. Edmond*, 531 U.S. 32 (2000).