Memorandum

TO: Congressman Ed Markey, Congressional Bipartisan Privacy Caucus

FROM:

RE: Oversight methods for domestic UAV use

Date: May 24, 2012

Background

Until recently, almost all domestic use of unmanned aerial vehicles (UAVs) was prohibited by the Federal Aviation Administration (FAA). At the behest of Congress however, the FAA has begun to take incremental steps to allow the widespread use of UAVs throughout the United States. In the first rulemaking since it was asked to ease regulations, the FAA has allowed public safety departments to use UAVs up to 25 pounds without going through a special permitting process. Within days of the announcement, the FAA received over 60 applications for permission to operate the vehicles in domestic airspace.[1] While the FAA is starting small, the variety of today's UAVs runs the gamut: from nearly undetectable bird-size miniatures to airliner-size behemoths, and from ones that can stay aloft for only minutes to blimps and solar-powered machines that will remain in the air for months or years.[2]

Demand for the services that UAVs provide will only increase, and the expense of operating them will only decrease. The desire for UAVs is not limited to police and fire

[1] Levin, Alan. "Drones up to 25 pounds allowed for US Safety agencies." *Bloomberg News,* May 14, 2012. *http*://www.bloomberg.com/news/2012-05-14/drones-up-to-25-pounds-allowed-for-u-s-safety-agencies.html

[2] Villasenor, John. "The Drone Threat to National Security." *Scientific American*, November 11, 2011.

departments, but extends to universities, commercial entities, and even individuals. The ability of UAVs to provide real-time information from the air is an extremely useful asset that should, in many cases, be encouraged. However, as the use of UAVs begins to climb, so will concerns over privacy. The capability to provide detailed, extensive, and even intrusive surveillance on private citizens requires a thoughtful approach to protecting the privacy that many Americans come to expect.

While the FAA is responsible for maintaining the physical safety of the nation's airspace, no agency is currently tasked with any kind of oversight particularly pertaining to privacy from aerial surveillance. This lack of protection is cause for concern as more and more entities begin to acquire UAVs. This memo presents three recommendations for oversight mechanisms to approach this problem. It considers tasking the FAA with the additional responsibility, allowing the courts to set limits, and finally encouraging state legislatures to handle regulation.

Assign UAV Oversight Responsibility to the FAA

Historically, the primary task of the FAA has been to ensure the safety of airspace, air passengers, and the greater public. As such, its rules and regulations usually govern topics like the reliability of aircraft or the management of air traffic. However, the agency's mandate includes "protecting individuals…on the ground."[3] The ACLU argues that the courts have broadly interpreted this mandate.[4] Tasking the FAA with the role of protecting Americans from inappropriate surveillance would be a significant departure

[3] Stanley, Jay and Catherine Crump. "Protecting Privacy from Aerial Surveillance: Recommendations for Government Use of Drone Aircraft." ACLU, December 2011.
[4] 49 U.S.C. § 40103(b)(2)(B) (2006); City of Burbank v. Lockheed Air Terminal, Inc., 411 U.S. 624, 626-27 (1973)

from its previous activities, but it may fall under this mandated responsibility. There are also a number of reasons it may be well suited for the role.

The FAA has the greatest amount of experience in the realm of airspace regulation. Drawing on this experience, the FAA would be the most capable organization at immediately recognizing the challenges of UAV regulation. Technologically speaking, the FAA is the most well equipped federal agency for monitoring domestic airspace, although there are concerns about how effective this monitoring would be with small UAVs.[5] In addition, housing UAV control within the FAA reduces the complication of coordination between separate entities that would occur if two agencies were both regulating airspace. Importantly, tasking the FAA with this responsibility is politically feasible. If the Congressional Bipartisan Privacy Caucus can convince the Obama administration of its necessity, it could be achieved through Executive Order. Alternatively, a mandate could be added to the FAA's authorization, but that would take significantly longer as the agency is not due for reauthorization until 2015.[6]

The greatest disadvantage of tasking privacy issues to the FAA is the agency's lack of experience in privacy. In an agency accustomed to monitoring safety, it is possible that the FAA would ensure that UAVs will not crash into front doors, but would not know how to stop them from peering into back windows. The FAA is also criticized for viewing airlines as customers, and therefore not punishing them as harshly as they may deserve for violations.[7] It is possible that similar criticisms will surface about organizations that use or

---

[5] Villasenor, John. "The Drone Threat to National Security." *Scientific American*, November 11, 2011.
[6] United States. Cong. House. *FAA Modernization and Reform Act of 2012*. 112th Cong., 2nd sess. HR 658. Washington: GPO, 2012.
[7] "Southwest Faces Big Penalty on Plane Cracks." Associated Press. March 7, 2008.

manufacture UAVs exerting undue influence over the agency. However, it is unclear if UAVs could become a revenue source for the agency like civil aviation is, so this type of business-customer relationship may not arise.

Allow the Courts to Establish Proper UAV Limits

The courts are traditionally the defenders of privacy against threats like unconstitutional police surveillance. However, the question of UAV surveillance has not been directly tackled, and it is unclear exactly how the courts would interpret relevant precedents. Privacy advocates are encouraged by cases like Kyllo v. United States (2001), in which the Supreme Court found that the use of a thermal imaging camera on Kyllo's home violated his Fourth Amendment rights. Since thermal imaging technology is not in general public use, the imagery it produces is not considered public view.[8] However, the Supreme Court found no such violation when police flew over another suspect's home and observed his marijuana plants through two missing roof panels, holding that the plants were in public view, albeit from the air.[9] It is unclear if the use of a UAV for surveillance without a warrant would fall under the former category of technology not in common public use, or in the latter designation of within the public view. Furthermore, the public use doctrine may erode as UAVs become more common among hobbyists and the public.

Although it is unclear how the courts will react, there are significant advantages to allowing courts to decide the matter. They are the authority on constitutional issues, which ultimately the debate over privacy boils down to. They have the capability of taking in

[8] Villasenor, John. Lecture: "Digital Privacy". April 19, 2012.
[9] Stanley, Jay and Catherine Crump. "Protecting Privacy from Aerial Surveillance: Recommendations for Government Use of Drone Aircraft." ACLU, December 2011.

both legislative intent and relevant precedents, and therefore have a significantly larger view of the issue than a regulatory body would. In addition, allowing the courts to decide the issue is the easiest path politically, as it requires no action by any legislative or executive body.

However, there are also disadvantages to leaving the issue up to the courts. Courts are reactive bodies. They can only rule on cases brought to them. That means that significant intrusions of privacy may become commonplace before a case even makes its way before a judge. Moreover, courts can only rule on laws that already exist. In the U.S. there is no Federal law that explicitly guarantees a right to privacy, and it is unclear if there is the political will to create one. Whether or not there should be a law is outside of the authority of the court, and they are not in the habit of making decisions based on the normative desires of the public. Because of this, even intrusions that most Americans would think is a clear violation of privacy may not be struck down because of a lack of legal framework on the issue.

Encourage States to Implement Regulations

UAVs may be better regulated by the states because they have a better understanding of resident needs and preferences. An urban state like New Jersey might not find the intrusion of UAVs any different than surveillance cameras already in common use, and will highly value the cheap and accurate traffic reports they can provide. Other less dense states might find surveillance intrusive, and Great Plains states might find aerial footage not much more useful than a high tower.

The main advantage of letting states regulate the issue is this ability to tailor regulations to suit these preferences. In addition, states can encourage the particular services they want from UAVs by easing regulations on UAVs that perform those duties. An example might be expedited permitting for wildfire-spotting UAVs in California. Furthermore, states are able to respond to concerns more effectively than either the courts or a Federal agency. If a particular incident of privacy violation infuriates the public, states are usually much faster at legislating remedies than Federal-level lawmakers.

However, state-level regulation also has significant drawbacks. As mentioned above, having two agencies in charge of airborne vehicles may lead to wasteful redundancy and coordination problems. A state agency regulating UAVs might find the FAA restricting its authority, and jurisdictional issues are bound to arise. States hoping to cultivate the nascent UAV industry might cater to companies by offering extremely lax regulations, essentially selling off their residents' privacy. Finally, privacy may come to be considered an essential civil right if a privacy movement takes hold. If different states have inconsistent privacy laws, this may require the intervention of the courts in states that are not adequately protecting their citizens, which would create additional burden on the court system.

Recommendation: Assign UAV Oversight Responsibility to the FAA

The FAA has the most relevant experience, the most complete technology, and the closest authority to the issue out of any Federal agency. Moreover, whether they intended to or not, by restricting the use of UAVs in domestic airspace the FAA essentially tasked itself with the responsibility, as government and industry organizations are already looking

to them for the go-ahead on UAV projects. It is recommended that the Congressional Bipartisan Privacy Caucus pursue a strategy that will:

- Expand the FAA's mandate, either through Executive Order or reauthorizing legislation, to include responsibility over UAVs to ensure the privacy of people on the ground
- Provide additional funding upon reauthorization for the FAA specifically for UAV regulation
- Instruct the FAA to create a department, staffed with the appropriate privacy advocates and legal counsel, to properly handle privacy issues
- Expand the FAA's rulemaking authority to include UAVs, specifically providing for the authority to:
    - Require safety, monitoring, and tracking systems be installed
    - Restrict the ability to collect and maintain surveillance footage of any kind
    - Overrule local, state, and Federal departments in relation to the use of UAVs in domestic airspace
- Instruct the FAA to compile a report on the types of UAVs it can effectively monitor with existing ground-based radar and research solutions for monitoring those it cannot[10]
    - Incorporate technology for monitoring UAVs into the agency's Next Generation Air Transportation System (NextGen)[11]

By providing a strong framework for the duties of the FAA, the Privacy Caucus can ensure that there is an agency held responsible for these issues. As UAVs in the U.S. become more pervasive, it is essential that this framework be created to prevent privacy violations before they happen, not in reaction to them. A strong posture on privacy rights by the caucus will ensure that UAVs are properly regulated from the start.

---

[10] Villasenor, John. "The Drone Threat to National Security." *Scientific American*, November 11, 2011.

[11] NextGen is changing aviation monitoring from ground-based radar systems to advanced satellite-based systems that will have additional functionality. http://www.faa.gov/nextgen/