



May 31, 2013

Mr. Robert Davis  
Cadwalader, Wickersham & Taft LLP  
700 6th Street, NW, Suite 300,  
Washington, DC 20001

Lt. Gov. Mead Treadwell  
The Aerospace States Association  
107 S. West Street, Suite 510  
Alexandria, VA 22314

Dear Mr. Davis and Lieutenant Governor Treadwell,

Thank you for the invitation to participate in the Aerospace States Association's efforts to draft model privacy legislation to regulate unmanned aerial systems (UAS).

EFF is a non-profit organization that has worked for more than 20 years to protect civil liberties, privacy, consumer interests, and innovation in new technologies. Our organization has, for the last few years, been extensively involved in privacy and civil liberties issues raised by unmanned aircraft (UA),<sup>1</sup> commonly referred to as drones. This work has included consulting with state and federal legislators on legislation that would place appropriate limits on law enforcement's abilities to use drones for surveillance; commenting on government and private use of drones on EFF's website, in the press, and in other public fora; and obtaining, reporting on and making accessible to the public drone authorization records received from the FAA pursuant to the Freedom of Information Act.<sup>2</sup>

Legislation regulating drone use to protect privacy must, at a minimum, address three main points:

1. Law enforcement use of drones requires a warrant;
2. Commercial drone use must be subject to privacy protections and reporting requirements;
3. Regulations on private and media use of drones must strike an appropriate balance between the First Amendment and privacy.

### **Law Enforcement Drone Use Requires a Warrant**

UAS have the potential to fundamentally change the nature of policing in the United States. The technological advances in surveillance provided by drones may provide important benefits to law enforcement. For example, drones could be employed in dangerous situations to avoid risk of harm to an officer or to search in areas challenging to traverse. Drones will also make aerial surveillance much less costly for cash-strapped law enforcement agencies.

---

<sup>1</sup> For links to EFF's drone-related work, see *generally Drone Flights in the U.S.*, EFF.org, <https://www.eff.org/foia/faa-drone-authorizations>.

<sup>2</sup> See Jennifer Lynch, *Are Drones Watching You?*, EFF.org (Jan. 10, 2012) <https://www.eff.org/deeplinks/2012/01/drones-are-watching-you>.

However, these same advances will also present significant privacy and civil liberties risks. UAS are capable of highly advanced and near-constant surveillance through live-feed video cameras, thermal imaging, communications intercept capabilities, and backend software tools such as license plate recognition, GPS tracking, and facial recognition. They can amass large amounts of data on private citizens, which can then be linked to data collected by the government and private companies in other contexts. Without strong limitations on how this sophisticated technology can be used, we risk a society where we may all be subject to government surveillance at any time.

For this reason, any legislation regulating law enforcement UAS use must require that officers obtain a warrant based on probable cause before using the UAS for criminal investigations. Such a warrant must have limitations on duration and content recorded, much like a wiretap order does today,<sup>3</sup> and must apply whether the drone flies over private or public space.<sup>4</sup> The warrant requirement must also apply when law enforcement seeks access to data gathered by a drone that is owned or flown by a separate entity, whether that entity is a private party, commercial entity or another public agency.<sup>5</sup>

The warrant requirement can only be subject to limited exceptions for emergency situations such as imminent threats to life or of great bodily harm and only where a warrant could have been obtained but for the time constraints of the situation. And legislation establishing a warrant requirement must have a meaningful enforcement mechanism that allows persons subject to drone surveillance to move to suppress the evidence in any case brought against them.

### **Commercial Drone Use Must Be Subject to Privacy Protections and Reporting Requirements**

Congress has mandated that by 2015, the skies will be open to commercial drone flights.<sup>6</sup> In fact, the FAA has predicted that, in addition to the hundreds of drones currently used domestically by the military and law enforcement, there will be roughly 10,000 commercial drones flying in the US skies in just five years.<sup>7</sup> In reality, many small drone operators are already flying UAVs for

---

<sup>3</sup> See, e.g., *Berger v. New York*, 388 U.S. 41 (1967) (describing particularity requirements for wiretap warrants). In *Berger*, the Supreme Court indicated that the Fourth Amendment triggers heightened scrutiny when surveillance is undertaken as “a series or a continuous surveillance” rather than as “one limited intrusion.” See *id.* at 57. Therefore, a statute that regulates “a series or a continuous surveillance” must include special privacy protections or risk invalidity under the Fourth Amendment. See *id.* at 56.

<sup>4</sup> See, e.g., *U.S. v. Jones*, 132 S.Ct. 945 (2012) (Alito, J., concurring; Sotomayor, J. concurring) In *Jones*, which held law enforcement must get a warrant before affixing a GPS tracking device to a car, five justices took issue with the pervasive nature of surveillance possible with the device, even though the device tracked travel that occurred in public.

<sup>5</sup> Legislatures must also establish laws limiting the use of drones by non-law enforcement public agencies such as departments of forestry or agriculture. These should include requirements that images, footage or data pertaining to humans obtained by a public agency should not be disseminated outside the collecting agency and should not be used for purposes other than that for which it was collected. And all public agencies, including law enforcement, should be subject to annual reporting requirements to the public on any UAV purchases and how UAVs have been used.

<sup>6</sup> See FAA Modernization and Reform Act of 2012, Pub. L. 112–95.

<sup>7</sup> *FAA Aerospace Forecast Fiscal Years 2012-2032: Unmanned Aircraft Systems*, available at [http://www.faa.gov/about/office\\_org/headquarters\\_offices/apl/aviation\\_forecasts/aerospace\\_forecasts/2012-2032/media/Unmanned%20Aircraft%20Systems.pdf](http://www.faa.gov/about/office_org/headquarters_offices/apl/aviation_forecasts/aerospace_forecasts/2012-2032/media/Unmanned%20Aircraft%20Systems.pdf).

commercial purposes.<sup>8</sup>

For these reasons, it is critical that legislatures enact laws establishing privacy protections for commercial drone flights. These laws should set out standards that limit the collection, use, sharing, retention and disclosure of data gathered by UAVs. They should also include requirements that the commercial entity establish notice procedures on the type of data gathered by a UAV, how it's gathered and for what purpose, as well as the location the UAV is flown, how long data is retained, with whom it's shared, and how it's disclosed.<sup>9</sup>

### **Balancing the First Amendment and Privacy in Private and Media Use of Drones**

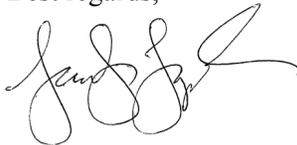
Regulations on private and media use of drones need to strike a balance between protecting privacy and not hampering First Amendment protected speech and associated activities.

As UAV use becomes more prevalent throughout society, private parties and the media will likely also want to fly UAVs for their own and for newsgathering purposes. Some of these activities might include using a UAV to report on a public figure, to monitor law enforcement activities at a political rally, or to record the aftermath of a natural disaster in an urban area. Each of these may impact privacy interests—of the public figure, of the police officer, or of the victims of the natural disaster—but also involve First Amendment-protected activities.<sup>10</sup> For this reason, any law designed to protect privacy must be sufficiently cabined to provide room for these activities. Acceptable limitations could include, for example, duration limits (such as limitations on how long a drone may be used to monitor a specific person), location limits (such as restrictions on monitoring of private spaces like a home or backyard) or could require a finding that the monitoring impinges on an objectively reasonable privacy interest, is highly offensive to a reasonable person, and causes emotional distress.

### **Conclusion**

EFF welcomes the ASA's efforts to craft model legislation to regulate public and private drone use. Please let me know if I can answer any questions or provide further information.

Best regards,



Jennifer Lynch  
Staff Attorney  
Electronic Frontier Foundation

---

<sup>8</sup> See, e.g., Chris Francescani, *From Hollywood to Kansas, Drones are Flying Under the Radar*, Reuters (Mar 3, 2013) <http://www.reuters.com/article/2013/03/03/us-usa-drones-domestic-idUSBRE92206M20130303>.

<sup>9</sup> See, e.g., Drone Aircraft Privacy and Transparency Act of 2013, H.R. 1262, 113th Cong. 1st Sess. (1st Sess. 2013) § 339 (b).

<sup>10</sup> For more information, see, e.g., Bill Kenworthy, *Photography & the First Amendment*, First Amendment Center (Jan. 1, 2012), <http://www.firstamendmentcenter.org/photography-the-first-amendment>; Alissa Dolan & Richard Thompson, *Integration of Drones into Domestic Airspace: Selected Legal Issues*, 17-19, Congressional Research Service (Apr. 4, 2013) available at <http://www.fas.org/sgp/crs/natsec/R42940.pdf>.