FOR DRONE OPERATORS, PRIVACY IS KEY FOR SMOOTH TAKEOFF AND LANDING

Jonathan Frankle*

CITE AS: 1 GEO. L. TECH. REV. 125 (2016)

https://perma.cc/22QT-64LV

INTRODUCTION

In a few short years, our skies will be far more crowded. Existing avian occupants will have to share the space above our heads with a new, man-made species of flying machines carrying packages, cameras, and pizzas:[1] Unmanned Aircraft Systems (UAS), a.k.a., drones.

On neighborhood streets, Amazon Prime Air[2] will use a fleet of small drones to deliver orders in under half an hour, making these flying couriers as commonplace as UPS trucks. Emergency personnel have already begun deploying drones to enhance their search and rescue capabilities,[3] while law enforcement is doing the same to both extend the reach of border patrols[4] and

---

* Staff technologist at the Center on Privacy & Technology at Georgetown Law. He has a B.S.E. and M.S.E. in computer science from Princeton.

[1] Frank Rosario, *Pizzeria owner uses drone to deliver pie in test flight*, N.Y. POST (Nov. 7, 2014, 3:25 AM), http://nypost.com/2014/11/07/pizzeria-owner-uses-drone-to-deliver-pie-in-test-flight/.

[2] AMAZON, https://www.amazon.com/b?node=8037720011 (last visited Nov. 13, 2016).

[3] Matt McFarland, *Drone operators assist search and rescue efforts after devastating floods in Texas*, WASH. POST (May 29, 2015), https://www.washingtonpost.com/news/innovations/wp/2015/05/29/drone-operators-assist-search-and-rescue-efforts-after-devastating-floods-in-texas/.

[4] William Booth, *More Predator drones fly U.S.-Mexico border*, WASH. POST (Dec. 21, 2011), https://www.washingtonpost.com/world/more-predator-drones-fly-us-mexico-border/2011/12/01/gIQANSZz8O_story.html.

keep officers out of harm's way.[5] Drones are even being produced as entertainment products to enhance the consumer's visual experiences.[6] The future is full of promising possibilities as more and more entrepreneurs, hobbyists, and first responders become able to fly.

From a privacy perspective, however, these tiny airborne cameras and microphones could stretch the boundaries of digital surveillance into the physical world. Today, corporations compete using web trackers to monitor our every movement online.[7] Tomorrow, drones could make it possible to do the same in person. How will you know what a drone is really up to when it flies past your window or over your child's school? Policymakers and companies need to convincingly answer this question if they want to earn citizens' trust.

Right now, some proposals ask drone operators to publish information about where they plan to fly and what data (like pictures and video) they plan to collect.[8] This is a good start, but it only solves half the problem—we would not know whether an operator actually kept her promises. What did the drone actually do in practice? Ideally, any citizen should be able to answer this question with just a few clicks.

THE CURRENT REGULATORY LANDSCAPE

Privacy and civil liberties advocates, companies, and government officials are already working to develop ways to ensure that we retain our "reasonable expectation of privacy" once these robot copters take flight.

In December 2015, the Center for Democracy & Technology (CDT) proposed comprehensive voluntary best practices for private use of drones.[9] A few months ago, the National Telecommunications and Information Administration (NTIA) concluded its multistakeholder process on drones.[10]

---

[5] Brian Bennett, *Police employ Predator drone spy planes on home front*, L.A. TIMES (Dec. 10, 2011), http://articles.latimes.com/2011/dec/10/nation/la-na-drone-arrest-20111211.

[6] GOPRO, https://shop.gopro.com/karma (last visited Nov. 13, 2016).

[7] *Online Behavioral Tracking*, ELEC. FRONTIER FOUND. (Sept. 29, 2016, 2:24 PM), https://www.eff.org/issues/online-behavioral-tracking.

[8] Press Release, Sen. Markey and Rep. Welch Introduce Legislation to Ensure Transparency, Privacy for Drone Use (Mar. 3, 2015), http://www.markey.senate.gov/news/press-releases/sen-markey-and-rep-welch-introduce-legislation-to-ensure-transparency-privacy-for-drone-use.

[9] *Model Privacy Best Practices for Unmanned Aircraft*, THE CTR. FOR DEMOCRACY & TECH. (Dec. 16, 2015), https://cdt.org/insight/model-privacy-best-practices-for-unmanned-aircraft/.

[10] *Multistakeholder Process: Unmanned Aircraft Systems*, NAT'L TELECOMM. & INFO. ADMIN (June 21, 2016), https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-unmanned-aircraft-systems.

This process produced a consensus document of drone best practices,[11] and many of CDT's December 2015 recommendations are reflected in the NTIA best practices.[12] This resource should help drone operators use their aircraft in responsible, privacy-respecting ways.

Among other things, the recommendations emphasize transparency and accountability to help people view this nascent technology with excitement rather than fear. For example, the best practices document asks companies to publish how they expect to use their drones—flight purposes ("to deliver pizzas"), flight plans ("along Main Street from the pizza shop to customers' houses"), intended data collection and use ("a camera recording to make sure customers actually received the pizza"), and contact information.

This gesture is a great step in the right direction, but how do we know whether a drone operator actually followed these recommendations? Which, if any, sensors were *actually* activated in flight, and over whose back yard? When it comes to deploying a brand new technology with such invasive potential, trust is not enough. We need verification.

Unfortunately, the FAA rule requiring drone registration since December 21, 2015 does not solve this surveillance issue.[13] Instead, it requires owners of only small drones to pay a small fee and provide this name, physical address, and e-mail address.[14] It does not address the other verification issues that would likely be more troubling to the public at large.

Drone operators should consider adopting an approach that combines **auditing** with **access**. Although some might bristle at additional requirements for fear they could limit the growth of this emerging technology, these requirements may actually help spur the development of the technology. In exchange for recordkeeping and inspection, drone operators could get more flexibility in the flight plans they publish upfront. This framework would give companies greater room to experiment and adjust their proposed purposes as necessary, affording this technology the freedom to reach its full potential.

---

[11] *Voluntary Best Practices for UAS Privacy, Transparency, and Accountability*, NAT'L TELECOMM. & INFO. ADMIN (May 18, 2016), https://www.ntia.doc.gov/files/ntia/publications/uas_privacy_best_practices_6-21-16.pdf.

[12] *Privacy and Civil Liberties Protections at Heart of NTIA Best Practices for Drones*, THE CTR. FOR DEMOCRACY & TECH. (May 18, 2016), https://cdt.org/press/privacy-and-civil-liberties-protections-at-heart-of-ntia-best-practices-for-drones/.

[13] *FAA Requires Drone Registration but Again Fails to Limit Drone Surveillance*, EPIC (Dec. 14, 2015), https://epic.org/2015/12/faa-requires-drone-registratio.html.

[14] *Id.*

AUDITING

Drone manufacturers should consider harnessing equipment that already exists to audit the flight activity of each drone in a way that builds privacy into the technology itself. For example, drones can be fitted with "black boxes" similar to those already found in cars and airplanes. These devices could record basic telemetry about the drone over the course of its lifetime, including its altitude, GPS coordinates, and physical positioning at certain time intervals. They could also record sensor metadata such as when a camera was activated and where it was pointed.

Individuals armed with this information could infer possible privacy violations (for example, when a drone passes over private property at a low attitude with its camera activated and pointed at a certain angle) without burdening companies with technologically onerous requirements. The mere act of being watched would encourage operators to alter their behavior in accordance with privacy expectations. Beyond privacy, this information would be vital for safety—drones will certainly suffer the occasional mechanical failure or operator mistake, and reliable flight data would help investigators sort out and learn from these incidents just as they do car and plane accidents today.

ACCESS

In order to ensure that these records truly hold operators accountable, someone needs to monitor the data. The ideal examiners are private citizens, who are best equipped to investigate the drones they personally see flying over their heads. To make this possible, flight data should be public—accessible to anyone with an internet connection.

However, such access could have unintended consequences. Reporting data in real time could grant too little privacy to operators, discouraging drone usage or revealing trade secrets. It might even create more privacy damage than it prevents (tracking drones from a sensitive healthcare company to a neighbor's house) or lead to unsafe situations (following a package delivery drone with the intent to steal its contents).

These side effects could be mitigated by obscuring the data enough to protect privacy without undermining its value for auditing. Instead of reporting in real time, for example, drone operators could release their data in a "timely" fashion—perhaps delaying publication by a few hours. They could also announce data for a time frame or geographic area rather than an exact moment or location.

Alternatively, operators could offer transparency by request. When someone sees an Amazon drone zip by, for example, she could contact the company's drone department to ask for more information.

Imagine a world in which a cooperative network of volunteers and local governments keeps track of drone movements over wide areas and submits this information to a centralized, online database as a free public service. This forum could be provided by the FAA or even as a voluntary industry service to consumers—a testament of good-faith drone operations that preserve individual privacy to the greatest extent possible.

CITIZEN TRUST IS ESSENTIAL

These mechanisms for accountability and transparency are not intended to punish drone operators before the technology even gets off the ground. To the contrary, building and maintaining citizen trust will be critical to this technology's success.

Many people are justifiably concerned about the prospect of hundreds, perhaps thousands, of drones buzzing around in formerly quiet airspace, peering into open windows, and even threatening citizens with weapons and other safety concerns.[15]

The right strategy is not to dismiss these fears as misguided. It is to make a concerted effort to assuage these concerns from the beginning, through transparency and accountability. This will result in strong yet adaptable privacy practices that will allow this promising technology to realize its full potential.

[15] Georgia Wells, *GoPro Recalls New Karma Drone*, THE WALL ST. J. (Nov. 8, 2016, 9:32 PM), http://www.wsj.com/articles/gopro-recalls-new-karma-drone-1478658769 (discussing the drones loss of power during flight); *See* Melanie Bates, *The FAA released rules for the operation of commercial drones*, FUTURE OF PRIVACY F. (June 21, 2016), https://fpf.org/2016/06/21/faa-released-rules-operation-drones-commercial-purposes/ (citing a Robohub article discussing the fact that operators will no longer be required to hold a manned aircraft pilot's license. This loosening of restrictions means that less qualified people will be piloting drones).