U.S. Department of Commerce
National Telecommunications and Information Administration
Docket No. 150224183-5183-01, RIN 0660-XC016
Privacy, Transparency, and Accountability Regarding
Commercial and Private Use of Unmanned Aircraft Systems

Public Comments from Jill Bronfman
Program Director of the Privacy and Technology Project
Adjunct Professor of Law, Data Privacy
Institute for Innovation Law
University of California Hastings College of the Law
April 20, 2015

These comments are provided in support of the National Telecommunications and Information Association, U.S. Department of Commerce ("NTIA")'s detailed proposal to obtain information about the issues surrounding privacy, transparency, and accountability for the commercial and private use of unmanned aircraft systems ("UAS" or "drones"). As an academic who has researched in this area[1], I believe that the proposed requests for information are necessary to consider at this time and appropriately tailored to balance privacy and safety concerns.

The Federal Aviation Agency (FAA) has begun regulating the use of UAS devices, but "[t]he current rules concerning drone use are geared solely towards safety."[2] Privacy issues remain unsettled by the FAA. Therefore, a bill was proposed last year to establish rules, and explicitly, "provide assurances"[3] that privacy would be maintained at least at the current levels of reasonable expectations of consumers. It has not yet been enacted. Nevertheless, there are some business and legal models, discussed herein, that provide a starting point for creating standards to maintain a reasonable expectation of privacy in the skies just above us.

At a high level, privacy, transparency, and accountability should be considered together, however, when the time comes for implementation, a separate workshop could be convened on standards for accountability and enforcement of proposed rules. Cost-benefit analysis should be considered in imposing each method of enforcement.

---

[1] Prior UAS research was presented at the National Association of Broadcasters and Broadcast Educators' Conference (NAB/BEA) in April 2014, and will be presented at International Association of Privacy Professionals (IAPP) conference May 2015. Also, paper on Internet of Things (IoT) home surveillance and monitoring to be discussed at the University of California, Berkeley Privacy Law Scholars Conference (PLSC) June 2015.

[2] *EPIC appeals to court for FAA drone privacy rules*, CIO, March 31, 2015, http://www.cio.com/article/2904693/epic-appeals-to-court-for-faa-drone-privacy-rules.html, retrieved April 1, 2015.

[3] "Unmanned Aircraft Systems Privacy Act of 2014," ("Act") Staff Working Draft, September 18, 2014, 113th Congress, 2D Session. The proposed Act suggests provisions for a privacy policy requirement for UAS operators, and confers authority upon the Federal Trade Commission to review such privacy policies.

I. Privacy: A Transactional Analysis

Historically, the legal principle of a "reasonable expectation of privacy" has been threaded through several cases[4] and analyses of the law therein. The Fourth Amendment to the U.S. Constitution has a long and storied history as a basis for claims of privacy violation, but it is insufficient as a stand-alone basis for privacy against the onslaught of a new technology that creates an expanded platform for accessing private information. In the United States, privacy law has maintained a balance, usually weighed on a case-by-case basis, between individual expectations of privacy and First Amendment considerations[5] protecting rights of free speech and assembly. These considerations should not be lost in the future application of the Constitution to new technologies. To reformulate a reasonable expectation of privacy in the current scenario, we need to look not only forward but up.

At this point, we need to redefine legal privacy parameters and physical space perimeters to include aerial space. To leave this space unregulated is to invite commerce in without safeguards for individual privacy. Detriments to individual privacy include unpermitted use of images of private individuals, private spaces, and private ideas. Detriments to business development include unlicensed use of copyrighted ideas, trade secrets, and other intellectual property. Finally, and not least, there is the possibility, and near probability, of threats to the overall sense of security in their physical persons that U.S. citizens generally enjoy as a benefit of living in a free society.

UAS use has the potential to accelerate a nascent blurring of the legal definitions of public and private spaces.[6] The notion of personal air traffic control means the ability of any individual or business to have sufficient information on the geographic parameters of where drone usage is permissible as well as understandable context to expect when drones will be used in or near the home, work, or public environs.

Despite the touted benefits of UAS operations for business and public benefit,[7] the use of UAS in the United States has been limited, at least legally, to certain industries and

[4] The U.S. Supreme Court stated that "a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection…. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." Katz v. U.S. 389 U.S. 347 (1967), et. al.

[5] Sec. 103. Constitutional Considerations. "Unmanned Aircraft Systems Privacy Act of 2014," ("Act") Staff Working Draft, September 18, 2014, 113th Congress, 2D Session.

[6] California clarifed this demarcation by adding UAS operation to the definition of trespass in SB-142 Civil law: unmanned aerial vehicles, which would amend the Civil Code to add Section 1708.83, which includes, "A person knowingly enters onto the land of another person pursuant to subdivision (a) of Section 1708.8 if he or she operates an unmanned aerial vehicle below the navigable airspace…" http://leginfo.legislature.ca.gov/faces/billTextClient.xhtml, retrieved April 2, 2015.

[7] "[UAS systems] may play a transformative role in fields as diverse as urban infrastructure management, farming, public safety, coastal security, military training, search and rescue and disaster response." Presidential Memorandum: Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems, The White

certain circumstances. Outside of the U.S., UAS businesses and the use of UAS to support business have expanded in the EU and Japan.[8] Where permitted, drone usage has been expedient for package delivery services and camera work for real estate, film, and video game production for previously inaccessible angles and locations.

In situations where drone use is becoming common, there are lower barriers to entry for businesses, in that UAS (in particular, small drone plus attached camera) present small businesses and even consumers with wallet-friendly startup costs. Further, environmental monitoring made possible by remote sensors and UAS surveys offer society-wide benefits in areas affected by drought and other extreme weather conditions in need of accurate forecasting for planning purposes. Allocation of scarce state and federal disaster funds can be optimized when more accurate on the spot information becomes available from these sensors at a lower cost than those associated with personnel, helicopters and traditional aircraft, and larger camera and sensor equipment.

The NTIA in its Request for Public Comment has the ability to gather information on the means to effectuate change in the regulation of these devices that, while seeming to shift the status quo, actually maintains the current reasonable expectation of privacy principles of law as applied to new technologies, and supports a business environment. The following section describes how existing models of notice can be used to effectuate transparency for the use of a new technology.

II. Transparency: Seeing New Technology Through Existing Legal Models

As a fundamental matter, privacy is supported by effectively communicated notice and transparency about the purpose of data collection and use. Best Practices for notice and transparency would incorporate a balancing of public access to complete information with individual rights to protect a subsection of that information that relates to individual privacy. In order to effectuate transparency for UAS usage to the public, U.S. regulation should address the actions of users, developers/designers, and owners of UAS devices. Privacy protective Best Practices for UAS Operation would stand on a platform of existing models of disclosure of information that have worked successfully to provide effective notice to consumers and affected business entities while supporting innovative delivery of goods and services. Several examples of such models are suggested below:

House, Office of the Press Secretary, February 15, 2015, retrieved March 26, 2015, from https://www.whitehouse.gov/the-press-office/2015/02/15/presidential-memorandum-promoting-economic-competitiveness-while-safegua.

[8] "In the EU there are 2,495 operators of drones weighing less than 150kg (330 pounds), the EASA [European Aviation Safety Agency] believes that number to be the largest amongst worldwide operations where just 2,342 operators are flying in the rest of the world combined (with 2,000 of those sanctioned operations taking place in Japan)." http://www.forbes.com/sites/gregorymcneal/2015/03/23/european-drone-regulations-are-about-to-get-smarter-and-more-permissive/, retrieved March 31, 2015.

•Online Service Maps: UAS users could be required to post online service maps similar to wireless coverage maps shared online by wireless telecommunications providers. At least at the onset, a "dog park" model of drone usage indicating where drones affirmatively are allowed could provide certainty for users and the public about where drone usage could be expected.

• Posted Notices: In the European Union, citizens and visitors have become accustomed to posted public notices indicating that surveillance cameras are in use in the vicinity. The United Kingdom has recently expanded its guidelines for video camera capture of private information to UAS technology.[9]

• Markings: Similar to airplane markings, UAS devices should be marked to indicate ownership and contact information, particularly if they reach beyond the ability of the operator to recall them in case of lost battery or other communication malfunction. UAS devices could at minimum indicate, "If lost, please return to…" for the smallest devices, and larger devices could indicate the purpose of the device or its current mission, including commercial or private, non-military purpose. Markings can be interpreted to include not only affixed text markings but also sound and/or light signaling beacons indicating a drone is present, or, in some cases, lost. The alerts would be visible to those in the drone's line of sight and/or to the larger group of citizens in the nearby area by text message alert.

• Tracking: United Parcel Service (UPS) provides tracking of packages via website or mobile application, a model that could be used for operators and interested parties to track movement of UAS via Radio Frequency Identification (RFID) and/or Global Positioning Systems (GPS). Such tracking could indicate position, flight path, and destination. UAS operators could issue alerts akin to "Amber Alerts"[10] for lost drones to engage the public in locating, capturing, and safely returning missing devices. Tracking UAS could be a collaborative exercise, including data from operators as well as members of the public.[11] There may be some problems when developers or

[9] In addition to previously required signage for cameras, the UK notes that for UAS, "You will need to come up with innovative ways of providing this information. For example, this could involve wearing highly visible clothing identifying yourself as the UAS operator, placing signage in the area you are operating UAS explaining its use and having a privacy notice on a website that you can direct people to, or some other form of privacy notice, so they can access further information." *In the picture: A data protection code of practice for surveillance cameras and personal information, issued by the Information Commissioner's Office* (ICO), Version 1, 15/10/14, https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf, retrieved April 2, 2015.

[10] "As of January 1, 2013, AMBER Alerts™ will now be automatically sent through the Wireless Emergency Alerts (WEA) program to millions of cell phone users." http://www.amberalert.gov, retrieved April 14, 2015.

[11] Air traffic apps have included customer-sourced data, and could be a model for collecting UAS traffic data, even if the technology used is different. "On the leading edge of flight tracking tech is ADS-B, which relies partly on sensors operated by commercial and government entities, and partly on rooftop and window receivers run by thousands of flight tracking enthusiasts across the globe. Think of them as the bird watchers of the aviation age… By 2020, the FAA will require every plane flying in most U.S. airspace to be equipped with ADS-B transponders as part of a decade-old project called NextGen to upgrade air traffic control." However, UAS application may require an analogous technology as "below

designers of UAS devices create tracking-resistant devices or cloak the devices to block tracking but law enforcement has had experience with "Silk Road"[12] perpetrators in the Internet context, and will be aware of such capabilities in the mobile and UAS device market as well.

• Warranties & Warnings: Traditional legal warranties could be crafted to cover what the UAS could reasonably be expected to do, including range of flight, both distance and elevation; proper use of accessories and add-ons, including privacy limitations for camera still and video capture; and appropriate parameters for use in certain scenarios- home use, workplace environment use, and use in public spaces. Listed warnings on the packaging of devices, or accessible via website, would describe the potential legal and privacy hazards for violations of privacy protective regulation promulgated as a result of this proceeding.

• Do Not Call: Similar to do not call registries, consumers and businesses might be permitted to register with their local agency in advance to create a Do Not Flyover space above their dwellings or place of business, citing privacy concerns.

III. Accountability and Training: Best Practices Interpreted and Implemented

A. Training

Training is the cornerstone of enforcement of any type of regulations. The course content of these "Drivers' Ed" classes for drone manufacturers, owners, and operators should include the final regulations resulting from this proceeding, and a reasonable amount of explanation of the consequences of violating the rules. Course content may also include industry-based and government-origin source materials that provide further guidance beyond the mandatory rules.

At some point, the rules will languish if they are not adequately publicized, explained, and targeted to the audience in possession of the technology. Training should be tailored to the type of drone operation, including size of the device, range of the device, and purpose for which it will be used. Guidelines may also include checklists for privacy protective operation, and additional considerations for use among children on playgrounds, the elderly or disabled in special living properties, and near secure military facilities.

B. Licensing and Certification of Owner/Operators

Licensing of UAS owners and operators, both business and individual, has potential for privacy protections as well as safe operation. After completing training, targeted

---

30,000 feet… ADS-B coverage may not work." http://www.fastcompany.com/3044490/how-flight-tracking-apps-work, retrieved April 14, 2015.

[12] See http://www.wired.com/2015/01/silk-road-trial-undercover-dhs-fbi-trap-ross-ulbricht/, retrieved April 14, 2015.

as described above to the type of device and planned operation, post-training testing and licensing would be similarly segmented. Consumer use for camera or communications purposes could be licensed by completing a simple online test and agreement post-purchase. Larger scale devices with multiple purposes, for example, for a delivery or Internet business, would be subject to a more extensive training and testing program, yet still using online resources and certification. The interesting question in licensing is whether each company could, based on federal guidelines, develop "Do it Yourself" (DIY) training and licensing or whether it would be worth the time and other resources to develop a standardized federal license. There are grandfathering issues as well, for UAS in current operation.

C. Transparency and Reporting

Transparency, in the sense of disclosing the uses and possible abuses of UAS devices with regard to data collection, and report of alleged abuses, is the last step in the construction of a viable privacy policy for UAS operation. Much of the transparency approaching the ideal would come from the Privacy Protective Best Practices for UAS Operation proposed above.

Reporting could be required from UAS Original Equipment Manufacturers ("OEMs"), from various supplemental equipment providers including cameras and accessories, and from consumer and business users. Reporting activities by the public would include complaints under the system of regulation and resolution of such complaints by a regulatory or judicial authority.