**Before the**
**NATIONAL TELECOMMUNICATIONS**
**AND INFORMATION ADMINISTRATION**
**Washington DC, 20230**

| | | |
|---|---|---|
| In the Matter of | ) | |
| | ) | |
| Privacy, Transparency, and | ) | Docket No. 150224183-5183-01 |
| Accountability Regarding Commercial | ) | |
| And Private Use of Unmanned Aircraft | ) | |
| Systems | ) | |

**COMMENTS OF ASSISTANT PROFESSOR MARGOT E. KAMINSKI, AMIE STEPANOVICH, & NABIHA SYED[1]**

We welcome the opportunity for public participation provided by NTIA's Request for Public Comment on privacy, transparency, and accountability issues regarding commercial and private use of unmanned aircraft systems ("UAS," colloquially known as drones). We applaud the NTIA's dedication to providing an open and transparent forum for multistakeholder engagement on these important issues.

**Who we are.** We write in our individual capacities as attorneys who have each been meaningfully involved in public policy conversations about private and commercial drone use. Margot E. Kaminski, an Assistant Professor at The Ohio State University Moritz College of Law, has published on private drone use, privacy concerns, and newsgathering in both the academic and popular press.[2] Amie Stepanovich, who currently works as U.S. Policy Manager at Access (an international human rights organization that defends and extends the digital rights of users at risk around the world), has testified on UAS privacy implications before the Senate Judiciary Committee, and the Subcommittee on Oversight, Investigations, and Management of the House Committee on Homeland Security.[3] Nabiha Syed, a media attorney known for her work on innovative newsgathering technologies, is a founder of Drone University, an online educational platform for people interested in learning more about the social, technological, and

[1] Many thanks to Joyce Gray, Joshua Monroe, and Alia Sisson for valuable research assistance. The views expressed
[2] *See* Margot Kaminski, "Drone Federalism: Civilian Drones and the Things They Carry," 4 Calif. L. Rev. 57 (2013), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2257080; Margot Kaminski, "Up in the Air," Slate (Nov. 25, 2014), *available at* http://www.slate.com/articles/technology/future_tense/2014/11/faa_s_attempts_to_regulate_drones_could_have_first_amendment_problems.html; Margot Kaminski, "Rules of the Sky," Slate (Feb. 25, 2015), *available at* http://www.slate.com/articles/technology/future_tense/2015/02/faa_small_commercial_drone_rules_don_t_adequately_address_privacy_concerns.html; Margot Kaminski, "Drone Law," NPR (Feb. 21, 2014) *available at* http://www.onthemedia.org/story/drone-law/.
[3] *See* Staff Biography *available at* https://www.accessnow.org/about/staff ; see also Testimony and Statement of Amie Stepanovich before the U.S. Senate Judiciary Committee, Hearing on "The Future of Drones in America: Law Enforcement and Privacy Considerations," *available at* https://epic.org/privacy/testimony/EPIC-Drone-Testimony-3-13-Stepanovich.pdf; Testimony and Statement of Amie Stepanovich before the Subcommittee on Oversight, Investigations, and Management of the U.S. House of Representatives, Committee on Homeland Security, *available at* https://epic.org/privacy/testimony/EPIC-Drone-Testimony-7-12.pdf.

policy issues surrounding the proliferation of drones.[4]

While UAS raise fascinating issues across a wide variety of legal areas, we have limited our comments to **a subset of the questions** posed by the NTIA in its March 5, 2015 RFC, and paraphrased below. We look forward to continuing to be involved in future conversations about issues that have not yet been addressed here.

**As a general matter**, we strive to bring two things to the NTIA's attention.

- First, we are concerned that framing privacy and innovation as in direct tension with each other will deprioritize privacy, and does not accurately reflect the inherently value-laden nature of technological development.
- Second, we wish to flag for the NTIA that drone use will raise important concerns about free speech and newsgathering by UAS users, and we consequently encourage the formation of an additional working group on newsgathering applications of UAS.

**Question 2. Would it be helpful to form three working groups: on privacy, transparency, and accountability? Should the groups work in serial or parallel?**

We encourage the NTIA to form separate working groups dedicated to privacy, transparency, and accountability—and to form a fourth group dedicated to newsgathering. While these issues are interconnected, they are not precisely the same, and levers that positively affect one goal may negatively affect another.

In our view, the groups will work most effectively in parallel. If the groups work in serial, we worry that the NTIA will miss important opportunities for engagement on overlapping issues across the groups. We encourage the NTIA to structure occasions for the various working groups to collaborate on proposals, effectively allowing each group to vigorously represent any conflicting positions and interests. We believe this will be more fruitful than a serial process where subsequent working groups are constrained by what has already been decided.

We further strongly encourage the NTIA to establish a fourth working group dedicated to newsgathering. UAS will serve as an important technology of public accountability, but newsgathering uses will also raise privacy concerns. The First Amendment and freedom of expression interests are critical to any conversation about UAS privacy concerns. None of the other three proposed working groups would have these concerns at their core, and it would be remiss for the NTIA to omit any of those considerations here.

**Question 3. Would it be helpful to distinguish between micro, small, and large UAS platforms? Do smaller or larger platforms raise different issues for privacy, transparency,**

[4] *See* Non-Residential Fellow Biography of Nabiha Syed at Stanford Center for Internet and Society, *available at* http://cyberlaw.stanford.edu/about/people/nabiha-syed; *see also* Drone U, a*available at* http://droneu.org/about and http://www.slate.com/authors.nabiha_syed.html; Nabiha Syed, "Journo-Drones: A Flight Over the Legal Landscape," 33 Communications Lawyer 3 (June 2014), *available at* http://www.lskslaw.com/documents/CL_Jun14_v30n4_SyedBerry.pdf; Nabiha Syed on "Fast Forward with Jo Ling Kent," Fox Business Network (April 15, 2015), *available at* http://radio.foxnews.com/2015/04/15/drones-the-weaponized-web-and-a-look-inside-the-bush-white-house.

**and accountability?**[5]

It will be helpful to distinguish between UAS platforms by size for conversations about privacy, transparency, and accountability. Both UAS size and flight capabilities could affect how visible a UAS platform is, and thus what notice of recording a surveillance subject might receive. The size of a UAS platform may also impact the type of surveillance technology it could carry.

Notice is a crucial aspect of the U.S. approach to privacy governance. A larger UAS may be capable of sustained flight at a higher altitude, rendering it less visible; conversely, a smaller UAS may be capable of quietly and surreptitiously entering or focusing on spaces usually considered to be private, or tracking individual people over time.

The size of a UAS platform will also affect whether it is capable of supporting particular types of surveillance technologies. Heavier UAS platforms will be equipped to carry heavier camera mounts, which allow them to carry heavier cameras. Heavier UAS platforms may also be capable of different movement capabilities, such as more stable hovering, or have longer battery life, raising different kinds of concerns over targeted tracking over time.

Other countries have seen fit to regulate UAS platforms by size and by use purpose. For example, Canada distinguishes between drones under 35 kg flown for recreation purposes; drones between 25 kgs and 35 kgs used for commercial purposes; drones under 25 kgs flown for commercial purposes; and drones under 2 kgs flown for commercial purposes.[6] Interestingly, transparency about flight location and purpose also varies by size: drones used for commercial purposes between 2.1 kg to 25 kg require submission of where and why a drone is being used, while drones used for commercial purposes that weigh less than 2 kgs do not need to conform to these reporting requirements.[7] The United Kingdom and New Zealand both also distinguish between UAS by weight.

While the primary motivation for regulating UAS by size may be concerns over differing safety issues, the trend suggests two things. First, the Federal Aviation Administration (FAA) may similarly decide for safety reasons to regulate UAS by size; any contemplation of best practices for privacy policies must be prepared to react to this choice. Second, smaller UAS may merit a lighter regulatory touch in general, for fear of interfering with adoption of the technology.

**Question 4. What existing best practices or codes of conduct could serve as bases for stakeholders' work?**

Several groups and organizations, from both the government and the private sector, have sought to identify principles or practices for drone use, many of which address privacy alongside other subjects, such as notice, use limitations, and attachment of other types of equipment and sensors.

---

[5] Thanks to Joshua Monroe for his valuable research assistance in answering this question.

[6] Transport Canada Guide to Flying an Unmanned Aircraft, *available at* http://www.tc.gc.ca/media/documents/ca-standards/Infographic_Permission_to_fly_a_UAV_Web_English.pdf (last accessed April 20, 2015).

[7] Transport Canada Exemption Submission Form, *available at* http://www.tc.gc.ca/eng/civilaviation/standards/general-recavi-uav-2265.htm?WT.mc_id=1zfhj#Form2 (last accessed April 20, 2015).

While these reports are educational on the positions of certain stakeholders, they should not be considered to be general best practices. In no case has a code of conduct been prepared that can be said to be representative of the different risks and needs of all stakeholders or of the public.

Included in the array of codes of conduct that have been published are:

- Recommended Guidelines for the Use of Unmanned Aircraft, International Association of Chiefs of Police (Aviation Committee);[8]
- sUAS Flight Safety Guide: Guidance for Safe, Responsible Flying, Academy of Model Aeronautics;[9]
- Micro Air Vehicle (MAV) Standard Operating Procedures, Miami-Dade Police Special Patrol Bureau / Aviation Unit;[10] and
- Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems.[11]

**Privacy**

**Question 5. Do some UAS-enabled commercial services raise unique or heightened privacy issues as compared to non-UAS platforms that provide the same services?[12]**

UAS platforms have been contemplated for use in a wide variety of commercial services. These services include: package delivery, agricultural use, and explicitly data-based services. For some of these services, UAS platforms clearly raise heightened privacy concerns. For example, drone use for data-gathering and subsequent data analysis provides new opportunities to physically track individuals while avoiding traditional physical and social hurdles, and will enable surveillance from a unique vantage point and at a lower cost than surveillance via manned aircraft. Uses of UAS to provide internet service also raises new and unique issues, including those related to net neutrality (particularly zero-rated services), permanence, and licensing and interconnection, and traffic monitoring. Where UAS could be used in special circumstances, such as disaster recovery, to amplify internet and phone service, these issues require special consideration. This is particularly important in the wake of revelations that wireless telecommunications companies were using "supercookies" to track users across different websites services.[13]

Drone use for agricultural purposes, however, or wildlife management, may not pose as significant concerns, if the primary purpose of the use is to monitor environmental conditions or

[8] International Association of Chiefs of Police, Recommended Guidelines for the Use of Unmanned Aerial Vehicles, *available at* http://www.theiacp.org/portals/0/pdfs/IACP_UAGuidelines.pdf (August 2012).
[9] Academy of Model Aeronautics sUAS Flight Safety Guide, *available at* http://suas.modelaircraft.org/ama/images/sUAS_Safety_Program_web.pdf (last accessed April 20, 2015).
[10] Miami-Date Police Department Draft Drone Standard Operating Procedures, *available at* https://www.eff.org/document/miami-dade-pd-draft-drone-standard-operating-procedures (last accessed April 20, 2015).
[11] Presidential Memorandum: Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights and Civil Liberties in Domestic Use of Unmanned Aerial Systems, *available at* https://www.whitehouse.gov/the-press-office/2015/02/15/presidential-memorandum-promoting-economic-competitiveness-while-safegua (April 15, 2015).
[12] Thanks to Alia Sisson for her valuable research assistance in answering this question.
[13] "Users Rally to Challenge Mobile Tracking," Access (Nov. 13, 2014) *available at* https://www.accessnow.org/blog/2014/11/13/users-rally-to-challenge-mobile-tracking-verizon

tend to crop needs in an unpopulated environment.

**Question 6. Which commercial and private uses of UAS raise the most pressing privacy challenges?**

The use of UAS for commercial data-gathering and analysis about individuals poses the most pressing privacy challenges. Commercial UAS may be equipped with cameras or other sensors, such as GPS- or infrared- detecting, all of which are capable of collecting various amounts of data about individuals. Because of this, seemingly benign uses of UAS may collect far more information than one might otherwise expect or imagine.

Take, for example, UAS designed to deliver packages. A consumer can reasonably foresee that such a UAS would acquire and store her address, or any other location information volunteered to the delivery service. Should that same delivery UAS be equipped with a camera – for understandable reasons, such as avoiding collision – that perpetually stores the footage, the privacy considerations and their foreseeability change. It is one thing for a delivery UAS to know where you live, and another entirely for the delivery UAS to record and store data on what bathrobe you were wearing each time you open your door to collect a package. (Of course, any potential limitation on that type of visual collection of imagery, especially as visible from public thoroughfares, must also take into account First Amendment protections for recording what takes place in public.) And while layering on facial recognition technology could theoretically be valuable to the delivery service – recognizing the intended recipient before completing delivery could cut down on stolen or missing packages, for example – that too adds a level of privacy concern that is unforeseeable when considering delivery UAS in the abstract.

Accordingly, the most pressing privacy concerns associated with UAS are difficult to identify in advance, particularly by industry. What deserves scrutiny is the type of information is being collected, and how it is combined with other types of data, especially in combinations that are not obvious to the consumer who may be unwittingly volunteering that information with no ability to opt-out. Any use that acquires and stores locational data, especially when combined with visual recordings of individuals, is just one example of a particularly pressing privacy challenge.

Certainly, some privacy violations will fit neatly into existing torts, such as intrusion or public disclosure of private fact. But others will not – and may even be unforeseeable at this stage. A "data minimization" guiding principle may be helpful in that regard, encouraging commercial UAS operators to collect only that data which their services require and that they can reasonably keep secure.

**Question 7. What specific best practices would mitigate the most pressing privacy challenges while supporting innovation?**

Innovation and privacy are not in direct tension with each other. In fact, privacy may well be an innovative advantage, in an era with heightened privacy consciousness and with platforms (like drones) that stimulate both real and hyperbolic concerns. As commercial drones integrate into the airspace, consumers may gravitate towards those options that protect and guarantee their privacy.

To encourage those options, we should veer away from the false dichotomy of privacy versus innovation.

As for more concrete best practices, we suggest developments in three realms:

Notice of Use. Despite the presence of a publicly available and searchable database of licensed pilots, including the geographic area in which they are licensed, the FAA has declined to establish a central database of drone operators. Attribution of drone pilots raises interesting legal concerns, particularly when the drones are used for newsgathering or to document public gatherings as well as in more nefarious cases, such as drones used to stalk or harass. While the absence of a central database of operators may, in some instances, be a privacy-protective decision, is also means that people will not be aware of the identity of companies or other individuals operating drones within their area. Having an informed debate about the positive and negative implications of attribution, and technical, legal, and practical solutions to the questions raised by attribution (or lack thereof) would be broadly beneficial.

Notice of Data Collection. While notice is not alone sufficient to protect privacy concerns, it is a necessary first step. Notice must be comprehensive and meaningful, and not a formality. And notice may well ease adoption and acceptance of UAS in this transitional period: informing the public about UAS capability will encourage those who might otherwise be deterred, and influence those who would like to participate broadly in any related policy process. This type of informed debate is only possible with robust notice, including:

- Notice of what data is being collected and when;
- Notice of how it is stored;
- Notice of how data will be used, including repurposed, sold or otherwise transmitted;
- Notice of how data may be disposed, and whether there is any opt-out to collection;
- Notice of any data breach within a limited time period, if applicable state law regarding data breach does not apply.

This may be part of a required "privacy policy" featured prominently on a commercial platform's website.

Data Security. Whether the data is sensory, locational, image-based, or something else entirely, commercial UAS operators must understand the value of keeping it secure. At least one of the working groups should come up with guidelines for effective controls against hacking, hijacking, or theft of data. This obviously protects privacy and safety, but also enhances innovation through additional protection for trade secret or otherwise valuable data maintained by any commercial UAS operator. Clear data security guidelines are equally important in helping operators understand what is required of them, so they do not run afoul of FTC or state-based scrutiny for their practices.

**Transparency**
**Question 8. What information should UAS operators make public?[14]**

[14] Thanks to Joyce Gray for her valuable research assistance in answering this question.

As observed in the request for comments, transparent UAS operations can include the following requirements: identifying the entities that operate a particular UAS; identifying the purposes of UAS flights; and identifying the data practices associated with UAS operations.

Transparent UAS operations could go beyond these requirements. While we do not necessarily endorse all of the below, we wish to assist the NTIA in its review of transparency options.

Review of the draft Markey UAS bill and several state UAS laws reveal the following possible additional reporting requirements:

- Identification of the individuals or entities with the power to use the unmanned aircraft
- Contact information for lodging complaints or to request information
- Specific locations in which the UAS will operate
- The maximum period of time the UAS will be in flight
- The type of data to be collected; the scope; the purpose (including whether and how it might be sold, leased, or otherwise provided to third parties)
- Minimization procedures for data gathered that is unrelated to the specified use
- The data retention period
- When and how data will be destroyed
- A privacy impact statement describing the anticipated effect of UAS use on personal privacy
- Specific steps to be taken to minimize impact on privacy, such as encryption methods
- A process by which an individual may request and obtain personally identifiable data, including any reasons for denial of such a request and a process for challenging the denial
- A process by which an individual may challenge the accuracy of data, and if a challenge is successful, a way to have the data either erased or corrected
- Audit and oversight procedures for both UAS use and data use
- Publicly available, searchable database of UAS flights, including documentation of changes in flight time records
- Publicly available, searchable database of data security breaches
- Publicly available, searchable database of any nuisance complaints, searchable by individual UAS operator or owner

**Accountability**

**Question 14. Can audits, assessments, or reporting help promote accountability?**

We encourage commercial UAS operators to volunteer reports explaining their data collection processes to the public, as part of a push towards transparency and accountability overall. By way of example, some technology companies have started to provide annual transparency reports. Commercial UAS operators can and should join in that trend, not least of all because those efforts can help curry favor from consumers that might otherwise be wary of UAS technology.

Beyond voluntary reporting, some commercial UAS operators may be better suited to mandatory reporting, depending on size and the type of data collected. We acknowledge that a mandatory audit prompts a tension between burdening small companies and protecting privacy. That said, there are models for varying data security policies based on the size of company in other areas of U.S. data security law: for example, the Gramm-Leach-Bliley Act (GLBA), also known as the Financial Services Modernization Act of 1999, imposes requirements appropriate to the "size and complexity of" the institution and "nature and scope" of its activities, as well as the "sensitivity of any customer information at issue." In keeping with this contextual approach to audits and as a starting point, the NTIA may consider:

- Auditing only a statistically significant subset of small companies.
- Setting a minimum threshold of size and data collection capability below which a company will not be audited, unless a certain number of complaints are filed within any limited period of time.
- Auditing only for companies above a certain threshold.
- Auditing only a small amount of data provided by the company or user, depending on size. For example, small companies may be reviewed for operator credentials, policy statements, and logs for data transfer and resale.

This type of tiered auditing model may prevent overburdening smaller companies seeking to enter the market – though the NTIA should consider some observations from the current innovation landscape, which suggest that small companies frequently face volatility and often sell their data to larger companies when they disappear. Those larger companies may then accumulate data and bypass accountability if smaller companies escape audits entirely through a no-accountability or lax-accountability rule. In keeping with that possibility, we suggest the NTIA consider accountability and mergers if it considers a lesser auditing requirement for smaller companies. While complicated, we urge the NTIA to think critically about transparency and accountability for those commercial actors that will implicate considerable user data.

* * *

We thank the NTIA for this opportunity to comment. We look forward to engaging further on these and other issues.