Protecting Against the Threat of Persistent Surveillance by Unmanned Aircraft Systems

Comments by New America's Open Technology Institute on *Privacy, Transparency, and Accountability Regarding Commercial and Private Use of Unmanned Aircraft Systems* in response to NTIA's Request for Comments [Docket No. 150224183–5183–01; RIN: 0660–XC016]

20 April 2015

To Members of the National Telecommunications and Information Administration:

The NTIA request for comment asks: "Which commercial and private uses of UAS raise the most pressing privacy challenges?" One clear answer is the use of UAS to engage in persistent surveillance of individuals or a mass of individuals over time and across space in a manner that was previously impossible or prohibitively expensive. A single UAS that is airborne for a long period of time, or multiple UAS used in sequence over a long period of time, can enable surveillance of an individual or even many individuals in a manner that – as per the Supreme Court's decision in *U.S. v. Jones* – violates their reasonable expectation of privacy. The development of reasonable and voluntary limits on private UAS use that respect this expectation of privacy against prolonged tracking of one's movements should be a primary goal of the NTIA's multistakeholder process on UAS-related issues of privacy, accountability and transparency.

I. UAS technology enables persistent and mass surveillance that poses a unique threat to privacy.

At present, prolonged surveillance of a particular person or geographic area using UAS is not cheap. Small, inexpensive UAS do not have the endurance necessary for such persistent surveillance. However, as UAS design advances, sensor packages are further miniaturized, and batteries improve, this will change and persistent surveillance will be within the reach of many private actors. Though UAS have only become commercially available and in widespread use in recent years, already the price of an unmanned aircraft is sharply falling. At the same time, the quality of UAS audio and video recording quality is rising. As prices fall, private surveillance using UAS – including *persistent* surveillance – will be a growing threat. The cost of any surveillance technology limits access to that technology, such that price is effectively a form of non-legal regulation that limits use to only those few who can afford it.[1] However, as the price to build and equip UAS with high-quality recording devices decreases, the regulating factor of cost will disappear. The result is that UAS capable of persistent surveillance will become available, accessible, and affordable to significantly more commercial and private actors than can afford the technology today.

[1] Kevin S. Bankston & Ashkan Soltani, *Tiny Constables and the Cost of Surveillance: Making Cents Out of* United States v. Jones, 123 YALE L.J. ONLINE 335, 337 (2014), http://yalelawjournal.org/2014/1/9/bankston-soltani.html; *See also* LARRY LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (V. 2.0) 123-25 (2006) (describing economic markets as one constraint on behavior; specifically, "markets constrain through the price that they exact," while the remaining constraints - law, social norms, and architecture - regulate behavior in other ways).

The technology that exemplifies the privacy challenge posed by persistent UAS surveillance, while currently expensive, is remarkably capable and advanced. For example, a UAS equipped with high-resolution cameras (such as the Gorgon Stare, which can take high-resolution images of an entire city twice per second[2]), can track all vehicles in a metropolitan area. Further, these high-resolution cameras can come equipped with impressive magnification and visual enhancement capabilities. For example, one drone currently on the market is equipped with a zoom lens that the manufacturers claim can identify a face or a license plate from 1,000 feet away and can read a serial number from a 100-foot distance.[3] Visual magnification can reveal information that is "effectively invisible to observers in public space"[4] but is clear and obvious to the drone operator and anyone with whom the operator chooses to share the information. Surveillance at this level of detail, over a long period of time and covering a large geographical area, would essentially enable the comprehensive monitoring of an individual's public movements, or the mass surveillance of the public movements of an entire population.

The fact that the subjects of UAS surveillance may be wholly unaware as to the UAS' presence enhances the privacy threat. A number of privacy and technology scholars have documented the fact that UAS surveillance may provide no audible or visual notice to those being surveilled.[5] There are several characteristics that are unique to UAS and allow UAS to be piloted without little notice to those on the ground. First, UAS can be small: "small enough to fit in a duffel bag or satchel,"[6] for example. Second, UAS are capable of hovering and don't require constant horizontal or vertical movement, which could increase how noisy the aircraft is.[7] Third, UAS can be disguised to avoid drawing attention: for example, the aircraft can be designed to look like "birds sitting on a wire" or even like a dragonfly.[8] The fact that UAS can fly unnoticed makes these privacy threats distinct from other forms of state and private surveillance, such as CCTVs, which are often visible to the public.[9] As Margot Kaminski, assistant professor at the Moritz College of Law at The Ohio State University, has explained, because non-UAS surveillance technologies (such as CCTVs) are noticed – and noted – by members of the public, individuals can act accordingly and even choose to travel particular routes not subject to this surveillance.[10] Surveillance by UAS that do not announce their presence in some manner eliminates the public's agency to decide whether to be surveilled by private actors. Persistent surveillance of a significant geographic area by UAS, whether they announce their presence or not, similarly eliminates the public's agency since there is no travel route or travel time whereby the UAS monitoring can be evaded.

---

[2] Marina Malenic, *USAF declares Gorgon Stare follow-on operationally deployable*, IHS JANE'S 360, (July 2, 2014), http://www.janes.com/article/40290/usaf-declares-gorgon-stare-follow-on-operationally-deployable.
[3] Jason Koebler, *This Drone Zoom Lens can Identify Your Face from 1,000 Feet Away*, VICE: MOTHERBOARD (February 25, 2015, 3:30 PM), http://motherboard.vice.com/read/this-drone-zoom-lens-can-identify-your-face-from-1000-feet-away.
[4] Marc Jonathan Blitz, *The Fourth Amendment Future of Public Surveillance: Remote Recording and Other Searches in Public Space*, 63 AM. U. L. REV. 21, 47 (2013).
[5] *See, e.g.*, Margot E. Kaminski, *Drone Federalism: Civilian Drones and the Things They Carry,* 4 CAL. L. REV. CIRCUIT 57, 67 (2013); THERESA M. PAYTON & THEODORE CLAYPOOLE, PRIVACY IN THE AGE OF BIG DATA: RECOGNIZING THREATS, DEFENDING YOUR RIGHTS, AND PROTECTING YOUR FAMILY 120 (2014).
[6] Payton & Claypoole, *supra* note 5 at 120.
[7] Kaminski, *supra* note 5 at 67.
[8] *Id.*
[9] *Id.*
[10] *Id.*

One final aspect of the threat to privacy posed by persistent UAS surveillance is the fact that UAS-collected data could, with relative ease, be aggregated with other forms of information, allowing for those captured by the surveillance to be personally identified after (or even during) the surveillance.[11] By combining UAS-collected data with identifying information, such as a home or work address, a license plate number, or even a face, the fruits of persistent UAS surveillance can create an extended and intimately complete picture of your actions and associations over time. As Justice Sotomayor wrote in her 2012 concurring opinion in *U.S. v. Jones* (discussed at length in the next section), such comprehensive and extended monitoring of one's movements, even if only in public space, allows the surveiller to "ascertain, more or less at will, [the subject's] political and religious beliefs, sexual habits, and so on."[12]

Persistent mass surveillance of an entire neighborhood or city is not currently within the reach of private actors. However, assuming a steady decline in cost, it will be. The NTIA must consider this fact as it works to establish a multistakeholder engagement process to develop and communicate best practices for privacy, accountability, and transparency issues regarding commercial and private UAS use in the National Airspace System (NAS). This need is all the more apparent in light of recent caselaw indicating that prolonged surveillance of one's movements, even if limited to movements in public space, violate that individual's expectation of privacy.

II. Persistent and mass surveillance by private UAS operators violates individuals' reasonable expectations of privacy.

It has been settled law for nearly half a century that one has no reasonable expectation of privacy in information that is exposed to the public.[13] However, the Supreme Court's 2012 decision in *U.S. v. Jones* suggested that this simplistic rule may not hold true given 21st-century surveillance technologies when five of the Court's justices concluded that the tracking of a suspect's car over a period of four weeks using a secretly planted GPS device violated the suspect's reasonable expectation of privacy, *even though the car was visible to the public the entire time*.

In two concurrences in *Jones*, five justices explained that GPS – a "21st century surveillance technique" – had changed the playing field with respect to privacy in public places.[14] New technologies, such as GPS and UAS, enable prolonged surveillance that was previously impossible or unaffordable for the vast majority of state and private actors. Prior to

[11] RICHARD M. THOMPSON II, CONG. RESEARCH SERV., R43965 DOMESTIC DRONES AND PRIVACY: A PRIMER 9 (2015).
[12] United States v. Jones, 132 S. Ct. 945, 955-56 (2012) (Sotomayor, J., concurring); *See also* California v. Greenwood, 486 U.S. 35, 50-51 (1988) (Brennan, J., dissenting) (Explaining that "[a] single bag of trash testifies eloquently to the eating, reading, and recreational habits of the person who produced it.").
[13] *See* United States v. Karo, 468 U.S. 705, 730 (1984) ("If personal property is in the plain view of the public, the possession of the property is in no sense 'private' and hence is unprotected."); United States v. Knotts, 460 U.S. 276, 281 (1983) ("A person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."); Katz v. United States, 389 U.S. 347, 351 (1967) ("What a person knowingly exposes to the public...is not a subject of Fourth Amendment protection," which turns on a reasonable expectation of privacy).
[14] *Jones* at 956 (Sotomayor, J., concurring); *Jones* at 957 (Alito, J., concurring).

the advent of those technologies, we reasonably expected to be free from such prolonged surveillance, and *Jones* stands for the proposition that we should be able to maintain that expectation despite the march of technology. Justice Sotomayor, concurring, pointed to the GPS monitor's "relatively low cost" and its ability to gather "a substantial quantum of intimate information about any person" as critical factors in considering whether prolonged GPS tracking violated a reasonable expectation of privacy.[15] In a separate concurrence, Justice Alito pointedly drew a distinction between modern and "pre-computer age" surveillance.[16] He said that the persistent surveillance at issue in *Jones* would have been previously impossible without "a large team of agents, multiple vehicles, and perhaps aerial assistance.[17] Because such surveillance was incredibly expensive, one could reasonably expect that it would not occur.

The reasoning of the *Jones* concurrences turned on how a once impossible-to-access and impossible-to-afford surveillance technology is now within reach, thanks to a radical drop in cost, as Justice Sotomayor explained noted in her concurrence.[18] In other words, the five concurring justices in *Jones* adopted a "cost-focused structural privacy rights approach," in which the low cost of the surveillance technology compared to the previously high cost of doing such prolonged surveillance absent the new technology was central to the conclusion that the surveillance violated a reasonable expectation of privacy.[19] The logic of *Jones* applies to UAS as well. UAS, like the GPS at issue in *Jones*, are an example of a technology that is rapidly dropping in cost, thus making the technology more widely available. Also like the GPS in *Jones*, UAS can be equipped to enable surveillance of movements over prolonged periods of time that would have been previously impossible. Yet unlike the single GPS device at issue in *Jones* and further heightening the privacy concern, UAS could enable *Jones*-like prolonged location tracking of *any and every person* over a wide geographic area.

The major takeaway from *Jones* – that persistent surveillance, even if only of one's public movements, can violate a reasonable expectation of privacy – has clear implications for UAS, which could similarly violate the privacy of countless individuals. And although *Jones* was a Fourth Amendment decision focused on surveillance by government actors, the conclusions from *Jones* are still relevant in the context of private actors. Many U.S. privacy laws, which protect against violations by private actors, aim to protect a reasonable expectation of privacy, or something closely equivalent.[20] The reasonable expectation of privacy standard has its roots in a concurrence by Justice John Marshall Harlan in *Katz v. United States*, which considered whether FBI eavesdropping on a public payphone booth was an unreasonable search under the Fourth

---

[15] *Jones* at 956 (Sotomayor, J., concurring).
[16] *Jones* at 956 (Sotomayor, J., concurring); *Jones* at 957 (Alito, J., concurring).
[17] *Jones* at 963 (Alito, J., concurring).
[18] *Jones* at 956 (Sotomayor, J., concurring).
[19] Bankston & Soltani, *supra* note 1 at 337.
[20] *See, e.g.*, Dietemann v. Time, Inc., 449 F.2d 245, 249 (9th Cir. 1971) ("We are convinced that California will 'approve the extension of the tort of invasion of privacy ... into spheres from which an ordinary man in plaintiff's position could reasonably expect that the particular defendant should be excluded.'"); Pearson v. Dodd, 410 F.2d 71, 704 (D.C. Cir. 1969) ("Just as the Fourth Amendment has expanded to protect citizens from government intrusions where intrusion in not reasonably expected, so should tort law protect citizens from other citizens.") (footnote omitted); *Fischer v. Hooper*, 143 N.H. 585, 590, 732 A.2d 396, 400 (1999) (pointing to the New Hampshire state wiretapping and eavesdropping statute, which "requires a reasonable expectation by the plaintiff that her communications will not be intercepted" in order for the plaintiff to recover damages.).

Amendment.[21] Since *Katz* was decided, the reasonable expectation of privacy standard has become a cornerstone of privacy law, its application extending beyond state actors to private actors. Today, the concept of a reasonable expectation of privacy can be found in Fourth Amendment jurisprudence, in state statutes aimed at private actors, and in federal and state caselaw interpreting privacy torts.[22] Therefore, the Fourth Amendment ruling in *Jones* can – and should – have implications for private UAS operators as well, and especially those that might engage in persistent surveillance of individuals over a prolonged period.

III. Conclusion: The NTIA process should establish best practices that will protect individuals' reasonable expectation of privacy against persistent and mass surveillance by private UAS operators.

The NTIA request for comment asks, "What specific best practices would mitigate the most pressing privacy challenges while supporting innovation?" Considering that under the reasoning of *Jones*, persistent UAS surveillance over a prolonged period and across a wide area will likely violate individuals' reasonable expectations of privacy, the NTIA should formulate best practices to prevent such surveillance. The first and most obvious best practice to consider would be reasonable limits on the duration of flights and on the number of flights during a particular period, as well as limits on the size of the geographic area over which the UAS flies, in order to avoid violation of any individual's reasonable expectation of privacy as per *Jones*. Additionally, the NTIA process should develop guidance for when UAS operators may and may not correlate UAS-derived data with other data such that those captured by UAS surveillance may be personally identified, in order to avoid the creation of dossiers that reveal specific individuals' public movements over a prolonged period of time, as did the GPS device in *Jones.*

The *Jones* decision helped articulate a vision of privacy for the 21st century, and we look forward to working with the NTIA to develop best practices that will apply that vision to the world of UAS.

For questions or additional information, please contact: Liz Woolery, Policy Analyst, New America's Open Technology Institute, lizwoolery@opentechinstitute.org

[21] Katz v. United States, 389 U.S. 347 (1967).

[22] *See, e.g.,* WIS. STAT. ANN. § 942.10 ("Whoever uses a drone, as defined in s. 175.55(1)(a), with the intent to photograph, record, or otherwise observe another individual in a place or location where the individual has a reasonable expectation of privacy is guilty of Class A misdemeanor."); CAL. CIV. CODE 1708.8(b) (banning capture of "any type of visual image, sound recording, or other physical impression of the plaintiff engaging in a personal or familial activity under circumstances in which the plaintiff had a reasonable expectation of privacy"); Video Voyeurism, 18 U.S.C. §1801(b)(5)(b) (2006); Electronic Privacy Communications Act, 18 U.S.C.A. § 2510 (2002); Nader v. Gen. Motors Corp., 25 N.Y.2d 560, 255 N.E.2d 765 (1970).