Senate Committee on the Judiciary

Hearing on "The Future of Drones in America: Law Enforcement and Privacy Considerations"

Questions for the Record

From Ranking Member Charles E. Grassley

Questions for Amie Stepanovich:

(1) Fourth Amendment Considerations

At the hearing, I asked a number of questions about the application of the Fourth Amendment to the use of unmanned aerial vehicles by law enforcement. I appreciate the answers you provided, but would like to follow-up on a couple of those matters in light of the recent decision by the Supreme Court in *Florida v. Jardines*. In *Jardines*, the Court held, 5-4, that the use of a drug sniffing dog at the front door of a private residence where law enforcement suspect illegal drugs are being grown constitutes a search under the Fourth Amendment.

This decision was based upon the common law notion of trespass extending the Court's reasoning from the 2011 decision in *United States v. Jones*. The majority opinion authored by Justice Scalia reasoned that it was unnecessary to address whether the use of the dog sniff violated the individual's reasonable expectation of privacy, because the trespass onto private property implicated the Fourth Amendment regardless of whether the trespass invades an individual's reasonable expectation of privacy.

- **The use of trespass doctrine to examine the application of the Fourth Amendment to law enforcement activity has implications for the use of drones. Do you believe that the reasoning in both *Jones* and *Jardines* change any of the analysis for reviewing aerial surveillance by unmanned systems under the Fourth Amendment? If so, please describe. If not, why not?**

  In the recent cases of *United States v. Jones*, 132 S. Ct. 945 (2012), and *Florida v. Jardines*, 133 S. Ct. ____ (2013), the Court held that certain law enforcement behavior violated the Fourth Amendment. The majority opinions in both cases focused on the physical intrusion of law enforcement onto private property.

  In both cases, Justice Scalia wrote a majority opinion that made clear that the trespass test was a standard to provide baseline privacy protections, and was not intended to overrule or otherwise change *Katz's* "reasonable expectation of privacy" test. Justice Sotomayor agreed with Scalia in a concurrence in *Jones*, referring to the trespass standard as an "irreducible minimum" of Fourth Amendment protection. Justice Scalia set out a two-part test, first asking if the intrusion violated a constitutionally-protected area (such as the curtilage of the house), and, if so, whether the physical intrusion was unlicensed. In *Jardines*, Scalia noted, "in permitting, for example, visual observation of the home from

'public navigable airspace,' we were careful to note that it was done 'in a physically nonintrusive manner.'"

Drones carry surveillance technology that makes it unnecessary to cross personal property lines in order to obtain sensitive, personal information about an individual, family, group, or organization. Drones are capable of hovering in an area adjacent to the property for prolonged periods of time while collecting vast amounts of personal information. The majority holdings in *Jones* and *Jardines* do not change the test for determining whether the use of drone technology that has not trespassed on private property violates a "reasonable expectation of privacy." Justice Kagan's concurrence in *Jardines* wrote, "where . . . the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant." But the greater insight of Justice Kagan's concurrence, which was joined by Justice Ginsburg and Justice Sotomayor, is that privacy intrusions can raise concerns under both the trespass doctrine and the *Katz* reasonable expectation of privacy doctrine. This is particularly true, she observed, where the surveillance that takes place is of the home: it is both the trespass onto private property as well as the intrusion into private life that is significant.

The law should clarify in what circumstances a drone has physically invaded or "trespassed" into a constitutionally protected area. Congress could, for example, codify the current standard of up to 400 feet above private property as a minimum basis for a protected area. In addition, comprehensive legislation could preserve current expectations of privacy against increased surveillance, including unregulated data collection and storage.

- **Physical surveillance is difficult and expensive given manpower constraints. Drones can conduct surveillance for hours on end with low cost and little effort. Given the length of time drones can stay on a target, and the low burden on law enforcement, does that change the Fourth Amendment calculus? If so, please explain.**

Practical barriers to surveillance are being reduced by the development of new and inexpensive technologies. The affordability and ease of drone operations will enable increased surveillance unless statutory protections are enacted.

In *United States v. Jones*, the Supreme Court unanimously found that the warrantless attachment and use of a GPS device to a suspect's car for the purpose of monitoring the suspect's movements for a one-month period was a violation of the Fourth Amendment.

The majority opinion in *Jones* rested on a physical trespass rationale. However, a group of four Justices joined Justice Alito's concurring opinion holding that the long-term GPS monitoring also violated a reasonable expectation of privacy. Justice Sotomayor joined the majority opinion, but also wrote in concurrence to note that she agreed with Justice Alito's reasonable expectation of privacy analysis. These concurring opinions created shadow majority in the Jones decision. Justice Alito's opinion held that "the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy," and even

though he does not indicate precisely where the line between "short-term" and "long-term" monitoring lies, "the line was surely crossed before the 4-week mark."

Justice Sotomayor agreed with Justice Alito's conclusion that "at the very least, 'longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.'" Justice Sotomayor noted, "cases involving even short-term monitoring . . . require particular attention" because the "Government can store such records and efficiently mine them for information years into the future." Justice Sotomayor focused on aspects of GPS tracking that also apply to drone technology, namely that it "is cheap . . . proceeds surreptitiously, [and] it evades the ordinary checks that constrain abusive law enforcement practices: 'limited police resources and community hostility.'" Generally, the Court's analysis suggests that in the absence of a legal standard enacted by Congress, drone surveillance will proliferate over time.

- **Does the addition of technology, such as facial recognition, biometric recognition, and thermal imaging equipment, affect whether there is a reasonable expectation of privacy under the Fourth Amendment? If so, please explain.**

Drones already carry infrared cameras, heat sensors, GPS, sensors that detect movement, and automated license plate readers. In the near future, government and corporate actors may attempt to outfit drones with facial recognition technology, Stingray cell-site simulators, and electronic frisking scanners.

The use of this technology to conduct surveillance of activities within the home (e.g. thermal imaging) should trigger Fourth Amendment protections. In *Kyllo v. United States*, 533 U.S. 72 (2001), and, more recently, in Justice Kagan's concurring opinion in *Florida v. Jardines*, the Court indicated that "where [a] device is not in general public use, training it on a home violates our minimal expectation of privacy." Absent Congressional action to preserve current expectations of privacy, the availability and proliferation of surveillance technology may degrade the current standards of privacy protection against surveillance in and around the home.

The curtilage, or the area directly surrounding the home, enjoys special Fourth Amendment protections similar to the home itself *United States v. Hester*, 365 U.S. 57 (1924). In *Florida v. Jardines*, the Court held that the curtilage "is part of the home itself for Fourth Amendment purposes." However, the Court has previous allowed warrantless law enforcement surveillance of the curtilage from the vantage point of a fixed-wing manned aircraft flying over the home within the public airspace. *Florida v. Riley*, 488 U.S. 445 (1989), *see also California v. Ciraolo*, 476 U.S. 207 (1986). By contrast, at least one Circuit Court has held that long-term fixed-camera surveillance of curtilage violated the Fourth Amendment *United States v. Anderson-Bagshaw*, 2012 WL 6600331 (2012). Courts will continue to struggle with the question of when surveillance of the curtilage using advanced technology constitutes a Fourth Amendment search.

As Justice Sotomayor's concurring opinion in *Jones* explained, extended surveillance, such as that made possible by advanced technologies, can generate "a wealth of data" about a person and reveal intimate details of their life that would not otherwise be public. Because of this risk to privacy, Congress should set defined limits on the warrantless use of these technologies, even in public spaces.

(2) First Amendment Considerations

The use of drones by private entities, such as the news media, to gather information on individuals and organizations is fast becoming a reality. Government regulation of private drone use is likely to be a new battleground under First Amendment. Even now, states legislators are proposing new laws to severely curtail the use of drones by private persons and entities. For example, a new bill proposed in California would prevent people or entities not affiliated with the government from using unmanned aircraft "for the purpose of surveillance of another person without that person's consent.

The First Amendment protects the freedom of the press, subject to reasonable restrictions. Drone technology could potentially offer the press a powerful tool in terms of surveillance.

- **Does the First Amendment prohibit Congress from restricting use of drone technology by the press?**

Drones do not enjoy more Constitutional protection than other technologies or methods for newsgathering or documentation. As with all forms of expression, content-based restrictions on drones would be unconstitutional under the First Amendment. Laws such as the Video Voyeurism Protection Act and state paparazzi laws are currently in force that restrict image collection in certain, limited situations.

- **What reasonable restrictions could Congress consider placing on the use of drone technology by the press?**

Over private property, laws could define the parameters under which a drone would commit a trespass, violate a reasonable expectation of privacy, or intrude upon an individual's right of enjoyment of his or her property. Non-content based restrictions on the use of drones may be permissible. For example, Congress could clarify the current standard by defining individual property ownership of the airspace up to 400 feet and codify current expectations of privacy against increased surveillance.

However, even non-content based restrictions on the use of drones by individuals should be carefully considered. Drones may be powerful tools for journalism in many instances. For instance, in holding public officials accountable in the performance of their official duties or reporting on weather-related events, such as hurricanes or earthquakes.

- **With regard to commercial applications, we have heard concerns about the increased use of private data collected by companies for advertising or other business purposes. What restrictions and limitations on private data collection by corporations exist?**

There is not a comprehensive privacy law in the United States to restrict the collection or use of personal information by commercial entities. A patchwork of sector-specific laws include protections for privacy, such as the Gramm-Leach-Bliley Act and the Fair Credit Reporting Act. In addition, the Federal Trade Commission investigates "unlawful or deceptive" trade practices by industry, including those involving corporate privacy practices.

The Electronic Communications Privacy Act ("ECPA") restricts the interception of wire, oral, or electronic communications. In 2012, the U.S. Department of Justice refused to file charges against Google, Inc. after the company had intercepted Wi-Fi data with Wi-Fi receivers concealed in the Company's Street View vehicles. Following independent investigations, Google conceded that it gathered MAC addresses (the unique device ID for Wi-Fi hotposts) and network SSIDs (the user-assigned network ID name) that it stored along with location information for private wireless networks. Google also admits that it intercepted and stored Wi-Fi transmission data, which included email passwords and email content. Congress should clarify that such practices are impermissible.

- **What recourse would private citizens have if they feel that their privacy rights have been violated by the press, or by other private citizens or companies utilizing drones?**

Absent Congressional action to create private right of action, individuals have limited recourse available to them against a private citizen or company who operates a drone in a way to violates their privacy or civil liberties. While some relief may be available under the U.S. common law for torts or pursuant to state laws, these protections are inconsistent and insufficient to address the unique aspects of surveillance made possible by drones. When the drone operator can be identified, a criminal action may be maintained in some states in the more egregious circumstances, such as stalking. This, however, also becomes an issue since drones may be operated in a manner to make identification of the operator difficult, and there are currently no public licensing requirements.

(3) Regulation of Unmanned Aerial Vehicles by the Federal Aviation Administration (FAA)

The Federal Aviation Administration (FAA) is currently the lead federal agency in approving the use of drones in the public airspace. Law enforcement agencies, civilian agencies, and individuals must apply with the FAA for a permit to authorize domestic drones.

- **In your opinion, is the FAA the best agency for authorizing the domestic use of drones? If not, what additional agencies should be involved?**

The FAA is required to "promote safe flight of civil aircraft." The FAA Modernization and Reform Act requires the FAA to, within a certain amount of time, "develop a comprehensive plan" to implement drones into civil commerce. Before May 14, 2012 the FAA must "simply the process" by which government entities operate drones in the national airspace. This authority places the FAA into the best position to assess many of the privacy problems associated with the highly intrusive nature of drone aircraft, and the ability of operators to gain access to private areas and to track individuals over large distances.

In addition, to the extent that the Department of Homeland Security, as well as other agencies that choose to operate drones, are responsible for greater aerial surveillance of individuals within the United States, we believe that the Agency should also develop appropriate regulations to safeguard privacy. Congress should require all agencies choosing to own and operate drones to promulgate, subject to the public notice and comment provisions of the Administrative Procedure Act (5 U.S.C. § 553), rules and standards for the protection of individual privacy and civil liberties.