EYES IN THE SKY: THE DOMESTIC USE OF UNMANNED AERIAL SYSTEMS

HEARING

BEFORE THE

SUBCOMMITTEE ON CRIME, TERRORISM, HOMELAND SECURITY, AND INVESTIGATIONS

OF THE

COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

ONE HUNDRED THIRTEENTH CONGRESS

FIRST SESSION

MAY 17, 2013

Serial No. 113–40

Printed for the use of the Committee on the Judiciary

Available via the World Wide Web: http://judiciary.house.gov

U.S. GOVERNMENT PRINTING OFFICE

80–977 PDF WASHINGTON : 2013

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON THE JUDICIARY

BOB GOODLATTE, Virginia, *Chairman*

F. JAMES SENSENBRENNER, JR., Wisconsin
HOWARD COBLE, North Carolina
LAMAR SMITH, Texas
STEVE CHABOT, Ohio
SPENCER BACHUS, Alabama
DARRELL E. ISSA, California
J. RANDY FORBES, Virginia
STEVE KING, Iowa
TRENT FRANKS, Arizona
LOUIE GOHMERT, Texas
JIM JORDAN, Ohio
TED POE, Texas
JASON CHAFFETZ, Utah
TOM MARINO, Pennsylvania
TREY GOWDY, South Carolina
MARK AMODEI, Nevada
RAÚL LABRADOR, Idaho
BLAKE FARENTHOLD, Texas
GEORGE HOLDING, North Carolina
DOUG COLLINS, Georgia
RON DeSANTIS, Florida
[Vacant]

JOHN CONYERS, JR., Michigan
JERROLD NADLER, New York
ROBERT C. "BOBBY" SCOTT, Virginia
MELVIN L. WATT, North Carolina
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
STEVE COHEN, Tennessee
HENRY C. "HANK" JOHNSON, JR., Georgia
PEDRO R. PIERLUISI, Puerto Rico
JUDY CHU, California
TED DEUTCH, Florida
LUIS V. GUTIERREZ, Illinois
KAREN BASS, California
CEDRIC RICHMOND, Louisiana
SUZAN DelBENE, Washington
JOE GARCIA, Florida
HAKEEM JEFFRIES, New York

SHELLEY HUSBAND, *Chief of Staff & General Counsel*
PERRY APELBAUM, *Minority Staff Director & Chief Counsel*

SUBCOMMITTEE ON CRIME, TERRORISM, HOMELAND SECURITY, AND INVESTIGATIONS

F. JAMES SENSENBRENNER, JR., Wisconsin, *Chairman*
LOUIE GOHMERT, Texas, *Vice-Chairman*

HOWARD COBLE, North Carolina
SPENCER BACHUS, Alabama
J. RANDY FORBES, Virginia
TRENT FRANKS, Arizona
JASON CHAFFETZ, Utah
TREY GOWDY, South Carolina
RAÚL LABRADOR, Idaho

ROBERT C. "BOBBY" SCOTT, Virginia
PEDRO R. PIERLUISI, Puerto Rico
JUDY CHU, California
LUIS V. GUTIERREZ, Illinois
KAREN BASS, California
CEDRIC RICHMOND, Louisiana

CAROLINE LYNCH, *Chief Counsel*
BOBBY VASSAR, *Minority Counsel*

CONTENTS

MAY 17, 2013

Page

OPENING STATEMENTS

The Honorable F. James Sensenbrenner, Jr., a Representative in Congress from the State of Wisconsin, and Chairman, Subcommittee on Crime, Terrorism, Homeland Security, and Investigations 1
The Honorable Robert C. "Bobby" Scott, a Representative in Congress from the State of Virginia, and Ranking Member, Subcommittee on Crime, Terrorism, Homeland Security, and Investigations 2

WITNESSES

John Villasenor, Nonresident Senior Fellow, The Brookings Institution
Oral Testimony 4
Prepared Statement 6
Gregory S. McNeal, Associate Professor of Law, Pepperdine University School of Law
Oral Testimony 19
Prepared Statement 21
Tracey Maclin, Professor of Law, Boston University School of Law
Oral Testimony 32
Prepared Statement 34
Christopher R. Calabrese, Legislative Counsel, American Civil Liberties Union (ACLU)
Oral Testimony 38
Prepared Statement 40

LETTERS, STATEMENTS, ETC., SUBMITTED FOR THE HEARING

Prepared Statement of the Honorable F. James Sensenbrenner, Jr., a Representative in Congress from the State of Wisconsin, and Chairman, Subcommittee on Crime, Terrorism, Homeland Security, and Investigations 1
Prepared Statement of the Honorable Robert C. "Bobby" Scott, a Representative in Congress from the State of Virginia, and Ranking Member, Subcommittee on Crime, Terrorism, Homeland Security, and Investigations 3
Prepared Statement of the Honorable Bob Goodlatte, a Representative in Congress from the State of Virginia, and Chairman, Committee on the Judiciary 52

EYES IN THE SKY: THE DOMESTIC USE OF UNMANNED AERIAL SYSTEMS

FRIDAY, MAY 17, 2013

HOUSE OF REPRESENTATIVES

SUBCOMMITTEE ON CRIME, TERRORISM, HOMELAND SECURITY, AND INVESTIGATIONS

COMMITTEE ON THE JUDICIARY

Washington, DC.

The Subcommittee met, pursuant to call, at 9 a.m., in room 2141, Rayburn House Office Building, the Honorable F. James Sensenbrenner, Jr. (Chairman of the Subcommittee) presiding.

Present: Representatives Sensenbrenner, Goodlatte, Gohmert, Coble, Franks, Chaffetz, Gowdy, Poe, Conyers, Scott, Chu, Bass, Richmond, and Jackson Lee.

Staff Present: (Majority) Sam Ramer, Counsel; Allison Halataei, Parliamentarian & General Counsel; Alicia Church, Clerk; and (Minority) Joe Graupenspurger, Counsel.

Mr. SENSENBRENNER. The Subcommittee on Crime, Terrorism, Homeland Security, and Investigations will come to order. Today we are having a hearing called, "Eyes in the Sky: The Domestic Use of Unmanned Aerial Systems," and this is dealing with the use of these systems within the United States. There are a lot of privacy and civil liberties concerns that are raised in there.

We are supposed to have votes about 10:00, and to try to get the hearing over with prior to the time we have votes because I do not think many Members will come back, I am going to ask, first, unanimous consent that the Chair be authorized to declare recesses when there are votes on the floor and, secondly, ask unanimous consent that all Members' opening statements be placed in the record, including mine and the Ranking Member's, and at this time, I will yield to the Ranking Member, Mr. Scott, to say whatever he wants to say.

[The prepared statement of Mr. Sensenbrenner follows:]

Prepared Statement of the Honorable F. James Sensenbrenner, Jr., a Representative in Congress from the State of Wisconsin, and Chairman, Subcommittee on Crime, Terrorism, Homeland Security, and Investigations

Welcome to the Subcommittee on Crime, Terrorism, Homeland Security and Investigations' hearing, "Eyes in the Sky: the Domestic Use of Unmanned Aerial Systems." Today we will explore the use of unmanned aircraft within the United States. We will discuss the possible uses and capabilities of such unmanned aircraft, and we will learn about the effect such use may have on the privacy of Americans. We

will also discuss the constitutional issues that may arise when the government uses unmanned aircraft for law enforcement and public safety purposes.

The United States remains at the forefront of technological progress. Every day we hear of some advancement in communications or computer technology that promises vast improvements in our daily lives. We have become a much more interconnected and informed population than we were just 10 years ago.

Within the last few years, high powered computers and data networks have been combined with aircraft, allowing them to be piloted remotely. Now, we are witnessing a boom in unmanned aerial systems, or UAS. Small, maneuverable UAS promise benefits in many fields that used to rely on manned aircraft. Law enforcement and public safety are increasingly becoming the most prevalent uses for UAS.

Unmanned aircraft can now be flown for longer times and for longer distances than ever before. Improved technology enables ground operators to both control UAS and to receive images and data from the aircraft. UAS are safer and less expensive to operate. It is now possible to purchase a UAS helicopter from a hobby store for a few hundred dollars and pilot it remotely from your smart phone or computer tablet.

The ability to fly a small, unmanned aircraft with cameras and sensors can also profoundly affect privacy and civil liberties in this country. No longer restricted to the high cost and short flight time of manned flight, UAS can hover outside a home or office. Using face recognition software and fast computer chips, a UAS may soon be able to recognize someone and follow them down the street. These new surveillance capabilities, in the hands of the police, may be intrusive to our concepts of individual liberty.

That is why I have cosponsored the "Preserving American Privacy Act of 2013," a bill sponsored by Representative Ted Poe of Texas and Representative Zoe Lofgren of California.

As UAS becomes more prevalent in our lives, we need to look at the 4th amendment and privacy implications of technology that enables prolonged remote flight. It has been well-settled in Supreme Court cases that the "reasonable expectation of privacy" applies to the home and surrounding cartilage. In contrast, generally speaking, a person that walks down the street no longer enjoys that expectation of privacy. This is commonly referred to as the open fields doctrine.

The distinction between one's home and curtilage versus the open fields is an important legal concept for understanding how the 4th amendment is applied to our daily lives.

UAS capabilities may affect how we decide the extent of the curtilage, along with the position of fences and walls. This is a subject that has great relevance today. This past March, in the case of Florida v. Jardines, the Supreme Court ruled that a police dog sniffing for marijuana at the front door of a house qualifies as a search under the 4th amendment. Justice Scalia, in that opinion, wrote about the importance of the curtilage, saying that the curtilage is "part of the home itself for 4th amendment purposes."

UAS may affect the debate where curtilage ends and the 'open fields' start. Any technology carried by a UAS that will magnify or enhance human senses could affect privacy concerns under the 4th amendment.

Every advancement in crime fighting technology, from wiretaps to DNA, has resulted in courts carving out the constitutional limits within which the police operate. With us today are several experts in UAS and constitutional law, and we will discuss the implications for this new technology and the constitution. We will discuss the directions in which constitutional legal theory is likely to go, and what the implications are for this promising, and potent new technology.

I look forward to hearing more about this issue and thank all of our witnesses for participating in today's hearing.

Mr. SCOTT. Thank you, Mr. Chairman.

I am pleased that we are examining these important topics and look forward to working with my colleagues on the Committee to update our laws to conform our expectation of privacy to emerging technology and ask that the rest of my statement be placed in the record.

Mr. SENSENBRENNER. Without objection.

[The prepared statement of Mr. Scott follows:]

Prepared Statement of the Honorable Robert C. "Bobby" Scott, a Representative in Congress from the State of Virginia, and Ranking Member, Subcommittee on Crime, Terrorism, Homeland Security, and Investigations

Good morning. Today the Subcommittee continues its focus on issues relating to evolving technology and privacy by discussing the use of drones by domestic law enforcement agencies.

As with the prior issues we've discussed with concerning email privacy and cell phone location privacy, advances in technology are outpacing our privacy laws.

I am pleased that we are examining these important topics and look forward to working with my colleagues on the Committee to update our laws where necessary.

The subject of drones is one of these areas that requires our attention. With expected action by the FAA to allow for the increased use of drones in U.S. airspace, drones will assist our society in many ways. Remote observation through the use of such drones has a wide variety of potential applications in the United States, such as helping to find lost children, identifying hot spots in forest fires, monitoring the health of crops, recording atmospheric data, and identifying traffic congestion.

Equipped with sophisticated cameras and sensing devices, drones will also greatly assist law enforcement with surveillance. Used appropriately, drones can help make us safer—but we must set clear rules establishing how the government may use drones for collecting information for law enforcement purposes.

We do not know how the courts would rule on the constitutionality of the warrantless use of drones by law enforcement, but the Supreme Court has allowed the warrantless use of aerial surveillance in some circumstances by aircraft with onboard pilots.

In those cases, the warrantless surveillance that was allowed involved the use of aircraft over fixed locations to detect and observe violations of the law. However, those cases did not involve the wide range of situations in which drones could be used by law enforcement, such as tracking individuals for long periods of time.

We should take note that Supreme Court justices are beginning to express concern about the degree and extent that new and emerging technologies impact privacy. The decision last year in *U.S. v. Jones* demonstrates that we are at a crossroad with respect to privacy and these new technologies.

While the *Jones* case generated a narrow ruling by Justice Scalia concerning a GPS tracking device, the concurring opinions of Justice Sotomayor and Justice Alito are relevant to the issue we are discussing today. Both of those justices expressed concern about the use of rapidly developing technology to track our movements.

Justice Alito cited the ability of the government, using new technology, to engage in long-term monitoring of an individual without the usual, practical constraints on law enforcement, such as resources and need for multiple personnel. He stated that, "In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative."

I note that my home state of Virginia recently adopted legislation providing for a 2-year moratorium on drone use by law enforcement, with some exceptions.

As we discuss the use of drones by law enforcement today, I believe we should take heed of Justice Alito's concerns and begin examining ways for Congress to legislatively address privacy concerns presented by the use of drones for law enforcement purposes.

Thank you.

Mr. SENSENBRENNER. We have a very distinguished panel today. I will begin by swearing in our witnesses before introducing them. If you would, please all rise.

[Witnesses sworn.]

Mr. SENSENBRENNER. I will be very brief in the opening introductions.

Our first witness is Mr. John Villasenor, who is a nonresident scholar, senior fellow in the governance studies for the Center of Technology and Center For Technology Innovation at Brookings. He is a professor of electrical engineering and public policy at UCLA and a member of the World Economic Forum's Global Agenda Council on the Intellectual Property System.

Mr. McNeal is a professor at Pepperdine University School of Law, and he previously served as the assistant director of the Institute for Global Security and co-directed a transitional counterterrorism program for the Justice Department.

Mr. Tracey Maclin is a professor at Boston University School of Law. He has served as counsel of record for the ACLU in issues addressing Fourth Amendment issues.

Mr. Calabrese is the legislative counsel for privacy-related issues in the ACLU's Washington legislative office. Prior to that he served as the project counsel on the ACLU Technology and Liberty Project.

And with that, I will say that, without objection, all of the witnesses' full statements will be placed into the record.

Each of you will have 5 minutes to summarize your full statement. We have a timer in front of you. I think you are all familiar with the green, yellow, and red lights.

And Mr. Villasenor, you are first.

TESTIMONY OF JOHN VILLASENOR, NONRESIDENT SENIOR FELLOW, THE BROOKINGS INSTITUTION

Mr. VILLASENOR. Good morning, Chairman Sensenbrenner, Ranking Member Scott, and Members of the Subcommittee. Thank you very much for the opportunity to testify today on the important topic of privacy and unmanned aircraft systems or UAS. I am a nonresident senior fellow in governance studies in the Center for Technology and Innovation at the Brookings Institution. I am also a professor at UCLA, where I hold appointments in both the electrical engineering department and the department of public policy.

The views I am expressing here are my own and do not necessarily represent those of the Brookings Institution or the University of California.

When discussing unmanned aircraft privacy, it is helpful to keep in mind the incredible variety of platforms made possible by this rapidly developing technology. Some unmanned aircraft, such as the Global Hawk, used by the U.S. military, are as large and nearly as fast as business jets. Some can stay aloft for very long periods of time. In the summer of 2010, a solar-powered airplane with a wingspan of about 74 feet but weighing only slightly over 110 pounds stayed aloft for over 2 continuous weeks over Arizona. Boeing is under contract with DARPA to develop the SolarEagle, which will be able to stay aloft in the stratosphere for 5 continuous years.

Some unmanned aircraft are amazingly small. The Nano Hummingbird, developed by California-based AeroVironment, weighs only two-thirds of an ounce, including an onboard video camera. A few weeks ago a team of Harvard researchers reported the successful flight of the RoboBee, a robotic insect powered by electricity delivered through a thin wire attached to an external power source. The RoboBee weighs less than one three-hundredth of an ounce.

Unmanned aircraft can be employed in an endless variety of civilian applications, the overwhelming majority of them beneficial. They can help rescuers identify people in need of assistance following a natural disaster. They can provide vital overhead imagery to police officers attempting to defuse a hostage standoff. In agriculture, they can be used for crop spraying. Scientific applications

include air quality assessment, wildlife tracking, and measuring the internal dynamics of violent storms.

Unmanned aircraft will provide a significant important new tool for news gathering as well. And they will generate significant economic benefits, both by creating jobs in unmanned aircraft design and production and by spurring advances in robotics that will apply well beyond aviation in fields ranging from manufacturing to surgery.

However, like any technology, unmanned aircraft can also be misused. In particular, there are legitimate and important privacy concerns. For unmanned aircraft operated by nongovernment entities, privacy involves contention between First Amendment freedoms and common law and statutory privacy protections. The First Amendment privilege to gather information is extensive, but it is not unbounded, and it ends when it crosses into an invasion of privacy.

With respect to government-operated unmanned aircraft systems, the Fourth Amendment is of course central to the privacy question. While the Supreme Court has never explicitly considered warrantless observations using unmanned aircraft, a careful examination of Supreme Court jurisprudence suggests that the Fourth Amendment will provide a stronger measure of protection against government unmanned aircraft privacy abuses than is widely appreciated.

The Fourth Amendment has served us well since its ratification in 1791, and there is no reason to suspect it will be unable to do so in a world where unmanned aircraft are widely used.

This does not mean that there is no need for additional statutory unmanned aircraft privacy protections. In fact, it makes eminent sense to consider appropriately balanced legislation. However, when considering new laws for unmanned aircraft privacy, it is important to recognize the inherent difficulty of predicting the future of any rapidly changing technology. Legislative initiatives in the mid-1990's to heavily regulate the Internet in the name of privacy would likely have impeded its growth while also failing to address the more complex privacy issues that arose in the subsequent decade with the advent of social networking and location-based wireless services.

When considering new laws for unmanned aircraft privacy, it is also important to recognize the power of existing legal frameworks. Those frameworks can play a vital role in preserving privacy in the face of a lengthening list of technologies that might be misused to violate it. Some of the best privacy protection may, in fact, lie not in statutory text drafted with a keen eye on the latest innovations in unmanned aircraft technology but instead in constitutional text drafted over 200 years ago.

Thank you again for the opportunity to testify on this important topic.

[The prepared statement of Mr. Villasenor follows:]

Governance Studies
at BROOKINGS

May 17, 201

Written Testimony of John Villasenor

Nonresident Senior Fellow
The Brookings Institution

and

Professor of Electrical Engineering and Public Policy
University of California, Los Angeles

before the

House Committee on the Judiciary

Subcommittee on Crime, Terrorism,
Homeland Security, and Investigations

"Eyes in the Sky: The Domestic Use
of Unmanned Aerial Systems"

May 17, 2013

John Villasenor is a nonresident senior fellow in Governance Studies and the Center for Technology Innovation at The Brookings Institution, and a professor of electrical engineering and public policy at UCLA.

Good morning Chairman Sensenbrenner, Ranking Member Scott, and Members of the Subcommittee. Thank you very much for the opportunity to testify today on the important topic of privacy and unmanned aircraft systems (UAS).[1]

I am a nonresident senior fellow in Governance Studies and the Center for Technology Innovation at the Brookings Institution. I am also a professor at UCLA, where I hold appointments in the Electrical Engineering Department and the Department of Public Policy. The views I am expressing here are my own, and do not necessarily represent those of the Brookings Institution or the University of California. Portions of my testimony today are adapted from a law review article I recently published in the *Harvard Journal of Law and Public Policy*.[2]

UAS, often referred to as "drones," can be employed in an endless variety of civilian applications, the overwhelming majority of them beneficial. However, like any technology, UAS can also be misused. The most common concern regarding domestic UAS relates to their potential impact on privacy. This is a legitimate concern. Existing laws and jurisprudence provide an important foundation, but they also leave many questions unanswered.

For non-government operators, determining when UAS use violates privacy involves the tension between First Amendment freedoms and common law and statutory privacy protections. With respect to government-operated UAS, the Fourth Amendment is of course central to the privacy question. While the Supreme Court has never explicitly considered warrantless observations using UAS, a careful examination of Supreme Court privacy jurisprudence suggests that the Constitution will provide a much stronger measure of protection against government UAS privacy abuses than is widely appreciated. The Fourth Amendment has served us well since its ratification in 1791, and there is no reason to suspect it will be unable to do so in a world where unmanned aircraft are widely used.

This does not mean that there is no need for additional statutory UAS privacy protections. However, when drafting new laws it is critical to adopt a balanced approach that recognizes the inherent difficulty of predicting the future of any rapidly changing technology. Although unmanned aircraft pose real and increasingly well-recognized privacy concerns, they also offer real and much less widely understood benefits. A dialog conducted with full awareness of this balance will be much more likely to lead to positive policy outcomes.

[1] The acronym "UAS" is also sometimes expanded to "unmanned aerial systems."
[2] John Villasenor, *Observations From Above: Unmanned Aircraft Systems and Privacy*, 36 HARV. J.L. & PUB. POL'Y 457 (2013).

Unmanned Aircraft Systems

While much of the public and legislative interest in UAS is recent, unmanned flight has a long history. In fact, early research in unmanned aviation laid some of the critical groundwork that was later used by pioneers in manned aviation,[3] including the Wright brothers, who achieved sustained manned heavier-than-air flight in 1903. Unmanned flight received significant attention throughout most of the twentieth century, particularly in the military aviation and model aircraft communities.

The dramatic growth over the last decade in worldwide UAS use is due to a confluence of multiple factors. Continued improvements in electronics have made it possible to equip even very small UAS platforms with sophisticated on-board computational systems for tasks such as image processing and GPS-based navigation. Thanks to advances in digital imaging systems and wireless communications, high resolution images and video acquired by an unmanned aircraft can be transmitted in real time to an observer fifty feet—or 5,000 miles—away. Innovations in airframe design and flight control methods are making it possible to design smaller and more agile UAS.

Unmanned aircraft will dominate the future of aviation as thoroughly as manned aircraft have dominated its past. In the U.S. military, which now has thousands of unmanned aircraft systems, that transition is well underway. Civilian UAS use in the United States is also set to grow rapidly following the enactment of the FAA Modernization and Reform Act of 2012,[4] which provides for the integration of UAS into the national airspace by late 2015.[5]

Unmanned aircraft come in an incredible variety of shapes and sizes. Some, such as the Global Hawk used by the U.S. military, are as large and nearly as fast as business jets.[6] Others are small enough to fit in a backpack or even the palm of a hand. The video-capable Nano Hummingbird, developed by California-based AeroVironment, weighs only two-thirds of an ounce.[7] In May 2013, a team of Harvard researchers reported the successful flight of the RoboBee, a robotic insect weighing less than one three-hundredth of an ounce, and powered by electricity delivered through a thin wire attached to an external power source.[8] In the summer

[3] Bill Hannan, *History in Models, Models in History*, MODEL AVIATION, Dec. 1986, at 78, 79–81.
[4] Pub. L. No. 112-95, 126 Stat. 11 (2012).
[5] *Id.* §§ 331–336, 126 Stat. at 72–78.
[6] *RQ-4 Global Hawk Factsheet*, THE OFFICIAL WEB SITE OF THE U.S. AIR FORCE, http://www.af.mil/information/factsheets/factsheet.asp?id=13225 (last visited May 4, 2013).
[7] Press Release, AeroVironment Inc., AeroVironment Develops World's First Fully Operational Life-Size Hummingbird-Like Unmanned Aircraft for DARPA, Feb. 17, 2011, *available at* http://www.avinc.com/resources/press_release/aerovironment_develops_worlds_first_fully_operational_life-size_hummingbird
[8] Press Release, Wyss Institute for Biologically Inspired Engineering at Harvard University, Robotic insects make first controlled flight, May 2, 2013, *available at* http://wyss.harvard.edu/viewpressrelease/110/.

of 2010, a solar-powered Qinetiq Zephyr weighing slightly over 110 pounds despite having a wingspan of about 74 feet stayed aloft for over two continuous weeks over Arizona.[9]

The potential applications of UAS are just as varied. UAS can help rescuers identify people in need of assistance following a natural disaster and provide vital overhead imagery to police officers attempting to defuse a hostage standoff. In the commercial world, UAS will be employed for tasks as diverse as surveying, crop spraying, and traffic monitoring. Scientific applications include air quality assessment, wildlife tracking, and measuring the internal dynamics of violent storms. UAS will also generate a number of economic benefits, both by creating jobs in unmanned aircraft design and production and by spurring advances in robotics that will apply well beyond aviation, in fields ranging from manufacturing to surgery.

It is also undeniable that UAS can be used in ways that violate privacy. For privacy from government UAS, the Fourth Amendment provides the key constitutional foundation.

Supreme Court Fourth Amendment Jurisprudence

The Fourth Amendment, which provides the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures," has been a cornerstone of privacy from government intrusion for over two centuries. While the Supreme Court has never ruled specifically on when UAS use constitutes a Fourth Amendment search, there is a long list of relevant precedents. Among these are two cases from the 1980s that addressed warrantless observations of the curtilage of a home from manned government aircraft.[10]

The first of these cases, *California v. Ciraolo*,[11] started with a September 1982 tip to police in Santa Clara, California regarding backyard marijuana cultivation. After finding the yard surrounded by high fencing obscuring the view from the street, the police obtained a small airplane and flew over the residence at 1,000 feet. The officers on the airplane observed and photographed what they concluded to be marijuana plants growing in the backyard. This evidence was used to obtain a search warrant to seize the plants.

---

[9] Andrew Chuter, *Solar UAV Lands After Record 2 Weeks Aloft*, DEFENSENEWS, July 23, 2010, http://www.defensenews.com/article/20100723/DEFSECT01/7230304/Solar-UAV-Lands-After-Record-2-Weeks-Aloft.

[10] There was also a case, *Dow Chem. Co. v. United States*, 476 U.S. 227 (1986), that considered aerial photography using a mapping camera of the open areas of an industrial facility. The Supreme Court ruled that the open areas were more akin to an "open field" than to the curtilage of a home, and as a result, were "open to the view and observation of persons in aircraft lawfully in the public airspace unmediately above or sufficiently near the area for the reach of cameras." *Id.* at 239.

[11] 476 U.S. 207 (1986).

In a May 1986 decision, the Supreme Court noted that warrantless police observations of curtilage are not necessarily unconstitutional: "The Fourth Amendment protection of the home has never been extended to require law enforcement officers to shield their eyes when passing by a home on public thoroughfares."[12] Moreover, the Court noted, because the observations were made from "public navigable airspace . . . in a physically nonintrusive manner," the respondent's expectation of privacy from such aerial observations was not one "that society is prepared to honor."[13] The Court concluded that "[i]n an age where private and commercial flight in the public airways is routine, it is unreasonable for respondent to expect that his marijuana plants were constitutionally protected from being observed with the naked eye from an altitude of 1,000 feet."[14]

Just under three years after *Ciraolo*, the Supreme Court once again considered the constitutionality of aerial observations of a home's curtilage by law enforcement. Like *Ciraolo*, *Florida v. Riley*[15] arose from a tip involving marijuana cultivation behind a house. In *Riley*, the observations were made from a helicopter at 400 feet, enabling officers to see the plants through openings in the roof and sides of a greenhouse located behind a mobile home. A majority of the justices in *Riley* found the observations constitutional.[16]

The Court's 2001 *Kyllo v. United States*[17] decision, though it considered ground-based observations of a home, is also relevant to UAS privacy. In 1992, a government agent in a car used a thermal imaging device to measure the external temperature of the roof and outside wall of the home of a person suspected of growing marijuana. The roof and wall were found to be abnormally warm, and a search warrant was issued based in part on this information. Upon execution of the search warrant, marijuana plants were found. In a decision finding the use of the thermal imager unconstitutional, the Court held that when "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."[18]

The most recent Supreme Court ruling with significant implications for UAS privacy is *United States v. Jones*.[19] *Jones* considered the government's installation, without a valid warrant, of a GPS tracking device on a vehicle used by a suspect in a narcotics investigation. The Court's January 2012 decision was unanimous in

[12] *Ciraolo*, 476 U.S. at 213.
[13] *Id.* at 213–14.
[14] *Id.* at 215.
[15] 488 U.S. 445 (1989).
[16] The *Riley* decision comprised an opinion delivered by Justice White and joined by three other Justices and an opinion from Justice O'Connor concurring in the judgment. Thus, while there was no majority opinion, a majority of the Justices found the observations constitutional.
[17] 533 U.S. 27 (2001).
[18] *Id.* at 40.
[19] 132 S. Ct. 945 (2012).

finding the government's actions unconstitutional, but there was considerable divergence in the basis for that finding. The majority opinion, delivered by Justice Scalia, found a Fourth Amendment violation in the physical trespass that occurred during the placement of the GPS device on the vehicle. That intrusion, wrote Justice Scalia, "would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted."[20]

In an opinion concurring in the judgment, Justice Alito criticized "the Court's reliance on the law of trespass" to decide the case.[21] Instead, he wrote, the question is whether the "respondent's reasonable expectations of privacy were violated by the long-term monitoring" of his vehicle.[22] Because "law enforcement agents tracked every movement that respondent made in the vehicle he was driving" for four weeks—a level of monitoring that Justice Alito felt impinged on reasonable expectations of privacy—Justice Alito concluded that the tracking constituted a search.[23]

Justice Sotomayor, in addition to joining the majority, provided a separate concurring opinion arguing that "the trespassory test . . . reflects an irreducible constitutional minimum"[24] and agreeing with Justice Alito's view that the respondent's reasonable expectations of privacy were violated. Justice Sotomayor also expressed concern that the unchecked ability of the government to assemble "the sum of one's public movements" could enable it to obtain private information regarding political and religious beliefs.[25]

A "Level of Detail" Test for Constitutionality of UAS Images?

In *Ciraolo* and *Riley*, the aerial observations of the curtilage of a home were made with the naked eye, a fact specifically noted by the *Ciraolo* Court and in both of the *Riley* opinions that found the government's observations constitutional. Writing for the plurality in *Riley*, Justice White found no Fourth Amendment violation in part because "no intimate details connected with the use of the home or curtilage were observed."[26]

In combination, the opinions in *Ciraolo* and *Riley* imply a level of detail threshold beyond which government UAS observations could cross the line into a Fourth Amendment search and thus be unconstitutional without a warrant. This would pose no conflict with *Kyllo*, which stopped well short of *endorsing* the constitutionality of using technology in general public use. Under a "level of detail" standard, even

[20] *Id.* at 949.
[21] *Id.* at 962 (Alito, J., concurring).
[22] *Id.* at 958.
[23] *Id.* at 964.
[24] *Id.* at 955 (Sotomayor, J., concurring).
[25] *Id.* at 956.
[26] *Riley*, 488 U.S. at 452.

widely available UAS technology would lead to a Fourth Amendment violation if used by the government to capture intimate details of a home or its curtilage not normally discernable to a passer-by (or to a person flying over the house in a manned aircraft). By contrast, an image from a UAS camera flown at a very high altitude might raise no constitutional concerns if it reveals very few details.

Long-term UAS Surveillance of a Home or Curtilage

For logistical, regulatory, and financial reasons, law enforcement agencies will usually use small UAS. These platforms typically have flight durations measured in dozens of minutes. Thus, the overwhelming majority of law enforcement—and more generally, government—UAS will be incapable of conducting surveillance over a continuous period of days or weeks. But a full consideration of UAS privacy requires acknowledging that some unmanned aircraft do have long flight durations, and could potentially be used by the government to conduct extended surveillance of a home or its curtilage. Would this constitute a Fourth Amendment search?

Lower court rulings related to video cameras installed by the government on fixed structures such as utility poles to surveil private property in the course of criminal investigations are somewhat divergent, but generally recognize the higher expectation of privacy accorded the interior of a home and the fenced-in portion of curtilage.[27] In 1987, for example, the Fifth Circuit ruled on a case involving a government-installed video camera on a light pole overlooking a 10-foot fence at the border of a defendant's backyard. In finding this to be a Fourth Amendment search, the Fifth Circuit wrote that "[h]ere, unlike in *Ciraolo*, the government's intrusion is not minimal. It is not a one-time overhead flight or a glance over the fence by a passer-by."[28] The court concluded that the defendant's "expectation to be free from this type of video surveillance in his backyard is one that society is willing to recognize as reasonable."[29]

A similar line of reasoning should apply to surveillance conducted using unmanned aircraft. The expectation to be free from from extended video surveillance in the curtilage of a home is eminently reasonable, and no less so if the monitoring is performed using a camera mounted on an unmanned aircraft as opposed to on a utility pole. This suggests that the Fourth Amendment will offer strong protection against long-term UAS surveillance of areas of a home or curtilage that a resident has sought to maintain as private.

---

[27] See, e.g., *United States v. Cuevas-Sanchez*, 821 F.2d 248 (5th Cir. 1987) and *United States v. Jackson*, 213 F.3d 1269 (10th Cir. 2000).
[28] *Cuevas-Sanchez*, 821 F.2d at 251.
[29] *Id.*

Long-Term Location Tracking

Like multiple other technologies, unmanned aircraft could be used acquire images of pedestrian and vehicular traffic, and thus to potentially track people as they move about in public. In fact, the imaging technology to support this already exists. The DARPA-funded ARGUS-IS sensor merges data from an array of 368 imaging chips to form a single 1.8-gigapixel image. When used on an unmanned aircraft from a height of approximately 17,000 feet, ARGUS can take in a field of view covering many square miles while still retaining sufficient resolution to see six-inch objects on the ground.[30] Completely independently, Boeing is under contract with DARPA to develop the SolarEagle, a solar-powered UAS that will be able to stay aloft in the stratosphere for five continuous years.[31] Mounting an imaging sensor such as ARGUS on a UAS platform like the SolarEagle would create a system that could track all vehicle and pedestrian movements over many square miles on an extended basis.

The prospect that the government might someday be able to use unmanned aircraft to capture—and then use at will—this level of information about the movements of private individuals is sobering. It is therefore even more sobering that very similar tracking is *already* being conducted using the increasingly extensive networks of ground-level cameras and license plate readers deployed in many American cities. These systems collect information that, when aggregated, can track our travels just as thoroughly as a bank of cameras on a solar-powered unmanned aircraft turning slow circles in the stratosphere.

The existence of multiple technologies that can perform extended warrantless location tracking in no way diminishes the privacy concerns that would be raised when any one technology is used for this purpose. But the underlying constitutional question raised by location tracking by the government is not technology specific: Do we have a reasonable expectation of privacy from government monitoring of the *totality* of our public movements over extended periods? Most people would answer this question in the affirmative, and the opinions in *Jones* suggest that a majority of the Supreme Court Justices would answer affirmatively as well.

For the *Jones* majority, the physical trespass involved in attaching the tracking device was sufficient to find the government's actions unconstitutional. Justice Scalia's majority opinion noted that while the Court had previously found traditional visual surveillance using a large team of agents to be constitutional, extended location tracking using technologies such as GPS may be different: "It

---

[30] Ryan Gallagher, Could the Pentagon's 1.8 Gigapixel Drone Camera Be Used for Domestic Surveillance?, SLATE, Feb. 6, 2013, http://www.slate.com/blogs/future_tense/2013/02/06/argus_is_could_the_pentagon_s_1_8_gigapixel_drone_camera_be_used_for_domestic.html.

[31] Press Release, Boeing Co., Boeing Wins DARPA Vulture II Program (Sept. 15, 2010), *available at* http://boeing.mediaroom.com/index.php?s=43&item=1425.

may be that achieving the same result through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy, but the present case does not require us to answer that question."[32]

However, five of the Justices wrote or joined concurrences that went further. In a concurrence joined by three other Justices, Justice Alito expressed a view that extended warrantless electronic surveillance of public movements is unconstitutional, writing, "the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy."[33] In a separate concurrence, Justice Sotomayor noted her agreement with this statement.[34] Notably, Justice Alito's classification of the tracking as a search was a direct consequence of its extended length:

> In this case, for four weeks, law enforcement agents tracked every movement that respondent made in the vehicle he was driving. We need not identify with precision the point at which the tracking of this vehicle became a search, for the line was surely crossed before the 4-week mark.[35]

We will have to wait for a future case to know whether the Court itself would adopt such a view as the basis for finding a search unconstitutional. But in the aggregate, the *Jones* opinions indicate that the Fourth Amendment will indeed provide protection against extended warrantless location tracking using technologies such as GPS or unmanned aircraft.

Non-Government Unmanned Aircraft and Privacy

Private entities are not bound by Fourth Amendment restrictions that apply to the government, and have an affirmative First Amendment privilege to gather information. However, while that privilege is extensive, it is not unbounded, and can end when it crosses into an invasion of privacy. While most companies and individuals will endeavor to use unmanned aircraft responsibly, there will inevitably be some operators who observe less restraint. For example, it would be optimistic in the extreme to expect paparazzi to always operate UAS in a manner respectful of privacy considerations.

Invading an individual's privacy using a UAS could result in civil or criminal liability. Courts in most jurisdictions recognize two forms of common law invasion of privacy that could arise in connection with UAS: intrusion upon seclusion, and public disclosure of private facts. In addition, many states have civil or criminal statutes, or both, related to invasion of privacy. A person who is photographed in

[32] United States v. Jones, 132 S. Ct. 945, 954 (2012).
[33] *Id.* at 964 (Alito, J., concurring).
[34] *Id.* at 955 (Sotomayor, J., concurring).
[35] *Id.* at 964 (Alito, J., concurring).

his or her own home by a UAS hovering just outside an otherwise inaccessible window would thus have strong grounds for a valid cause of action.

Although privacy expectations are greatly reduced outside the home, use of an unmanned aircraft to capture images and other information in a public setting could sometimes constitute an invasion of privacy. A 1998 California Supreme Court ruling in *Shulman v. Group W Productions, Inc.*[36] regarding filming that occurred following a car accident is instructive in this regard. In *Shulman* the victims of the accident were subjected to video and audio recording (using a traditional news camera held by a camera operator on the ground, combined with audio from a microphone worn by the flight nurse from a helicopter rescue crew) without their consent for a television program. The California Supreme Court found that a woman injured in the accident "was entitled to a degree of privacy in her conversations with [the nurse] and other medical rescuers at the accident scene."[37] It was improper, the ruling stated, to conclude that the "plaintiffs had no reasonable expectation of privacy at the accident scene itself because the scene was within the sight and hearing of members of the public."[38] At the time of the rescue, the vehicle was located "in a ditch many yards from and below" a highway, rendering it "unlikely . . . that any passersby on the road could have heard" the conversation of the victim with the nurse and other rescuers.[39]

The *Shulman* ruling provides important guidance regarding newsgathering and UAS with respect to intrusion upon seclusion by drawing a distinction between the information about a newsworthy event available to passersby and the potentially greater amount of information available only to those intimately involved in the event itself. Under some circumstances, there will be no difference. If a crowd of people has gathered around an assault victim who is being treated by paramedics, the conversation between the victim and the paramedics may well be audible to all, and the victim's reasonable expectation of privacy correspondingly lower. But there will be many cases in which, as in *Shulman*, passersby have far from complete information about an unfolding event. Using an unmanned aircraft to fill in the gaps would carry a risk of crossing the line into intrusion.

There is an opportunity to strengthen state invasion of privacy statutes to add UAS to the list of recited technologies that could be used to violate privacy. For example, a bill currently pending in the California State Legislature would amend the California civil code statute relating to constructive invasion of privacy to identify a "device affixed to or contained within an unmanned aircraft system" as one of the visual or auditory enhancing devices that could be used to violate a plaintiff's

[36] *Shulman v. Group W Productions, Inc.*, 955 P.2d 469 (Cal. 1998).
[37] *Id.* at 491.
[38] *Id.*
[39] *Id.*

reasonable expectation of privacy.[40] The same bill would also amend the California penal code to explicitly provide that eavesdropping upon or recording a confidential communication using "a device affixed to or contained within" an unmanned aircraft is punishable by a fine or imprisonment.

Business Privacy

In 2011, a Texas man flew an unmanned aircraft over land near a Dallas-area meat packing plant and acquired images appearing to show environmental violations.[41] He contacted the Coast Guard, and in early 2012 the Texas Environmental Crimes Task Force served a search warrant on the company.[42] Once on the property, investigators found a pipe that "originate[d] in the back of the slaughterhouse" that appeared to be channeling pigs' blood into a nearby river and "[was] not linked to a waste water system."[43]

Though few would rush to defend a slaughterhouse that may be in violation of environmental codes, the ability of private citizens or groups to easily inspect for such violations via overflights raises complex issues. To the extent that overflights are lawfully conducted and reveal activities that may be endangering public health, they are obviously valuable. But what happens if a well-meaning but overzealous environmental group conducts daily flights over a large, fenced-in manufacturing facility and repeatedly reports "violations" to the government that turn out, after costly and time-consuming on-the-ground inspections, not to be violations after all? Does the company that owns the facility have grounds to ask a court to enjoin the environmental group from further overflights? What if the group posts pictures from its daily aerial surveillance missions on the Internet, and in doing so exposes information that the company regards as a trade secret? What if the group were to use an unmanned aircraft to examine the interior of buildings at the facility using an advanced thermal imager that, if in government hands and used to inspect a home, would be unconstitutional under *Kyllo*?

In many respects these questions involve issues that go well beyond unmanned aircraft. And in most cases, they will best be resolved through the courts as opposed to through new legislation aiming to solve a business UAS privacy problem of still-uncertain scope and nature.

---

[40] S. B. 15, 2013–2014 Legis., Reg. Sess. (Cal. 2013), *available at* http://www.leginfo.ca.gov/pub/13-14/bill/sen/sb_0001-0050/sb_15_bill_20130422_amended_sen_v97.htm.
[41] Meghan Keneally, *Drone plane spots a river of blood flowing from the back of a Dallas meat packing plant*, MAILONLINE, Jan. 24, 2012, http://www.dailymail.co.uk/news/article-2091159/A-drone-plane-spots-river-blood-flowing-Dallas-meat-packing-plant.html.
[42] *Id.*
[43] *Id.*

Conclusions

The Founders of this country certainly did not have unmanned aircraft in mind when drafting the Bill of Rights. But neither were they contemplating thermal imaging—a technology that the Fourth Amendment proved to be eminently capable of addressing hundreds of years later.

The Supreme Court's Fourth Amendment jurisprudence indicates that the government will indeed have some latitude in acquiring information using unmanned aircraft. But it also conveys the existence of important bounds. Use of an unmanned aircraft to resolve details of a home or its curtilage unavailable through naked-eye observations, or to conduct long-term observations of a home's curtilage, or to perform extended location tracking could be credibly challenged as unconstitutional without a warrant.

Of course, the only way to know with certainty how the Fourth Amendment will be interpreted with respect to unmanned aircraft observations is to wait for the courts—and ultimately, the Supreme Court—to rule. In the meantime, however, it would be a mistake to draft legislation driven by an assumption that the Fourth Amendment will offer *no* protection from UAS observations, no matter how invasive. A far better approach is to view privacy legislation for government UAS as complementary to a constitutionally protected right "to be secure . . . against unreasonable searches and seizures" that will still have force and meaning in a world in which unmanned aircraft are common.

There is also a legislative role—mostly at the state level—to provide enhanced privacy protection from UAS operated by non-government entities. State statutes relating to trespassing, invasion of privacy, harassment, and stalking should be examined and updated as appropriate to address potential privacy abuses using UAS.

When considering potential new statutory privacy protections, it is helpful to keep in mind what has occurred with the Internet and mobile telephones, two technologies that are associated with privacy threats that are in some respects much more significant than those that will arise from unmanned aircraft. Usage of both the Internet and mobile phones grew as fast as their underlying technologies enabled. As a result, the public and legislative dialog regarding how best to address the privacy issues they raise has been conducted with a strong appreciation of their benefits. By contrast, while the privacy concerns associated with domestic UAS are real and deserving of attention, they are getting significant focus long before the potential benefits of the technology are widely recognized.

If, in 1995, comprehensive legislation to protect Internet privacy had been enacted, it would have utterly failed to anticipate the complexities that arose after the turn of

the century with the growth of social networking and location-based wireless services. The Internet has proven useful and valuable in ways that were difficult to imagine over a decade and a half ago, and it has created privacy challenges that were equally difficult to imagine. Legislative initiatives in the mid-1990s to heavily regulate the Internet in the name of privacy would likely have impeded its growth while also failing to address the more complex privacy issues that arose years later.

This doesn't mean that there is no role for new privacy initiatives. But in developing these initiatives, it is important to recognize the near impossibility of predicting all of the ways that a rapidly developing technology can be used—for good or for ill—in future years. Some of the best privacy protection may in fact lie not in statutory text drafted with a keen eye on the latest innovations in unmanned aircraft technology, but instead in constitutional text drafted over two hundred years ago.

Thank you again for the opportunity to testify on this important topic.

Governance Studies
The Brookings Institution
1775 Massachusetts Ave., NW
Washington, DC 20036
Tel: 202.797.6090
Fax: 202.797.6144
www.brookings.edu/governance.aspx

The views expressed in this piece are those of the author and should not be attributed to the staff, officers or trustees of the Brookings Institution.

Mr. SENSENBRENNER. Thanks very much.
Mr. McNeal.

TESTIMONY OF GREGORY S. McNEAL, ASSOCIATE PROFESSOR OF LAW, PEPPERDINE UNIVERSITY SCHOOL OF LAW

Mr. MCNEAL. Good morning, Mr. Chairman, Ranking Member Scott, Members of the Subcommittee. I am pleased to be here to testify on this important issue. I want to commend the Subcommittee for the approach that you are taking, too. This is a very difficult issue to legislate on, and the approach that the Committee is taking I think is really a wise one, beginning first, of course, with our Fourth Amendment precedents and then working our way down through various privacy considerations.

The looming prospect of expanded use of unmanned aerial vehicles, colloquially known as drones, has raised understandable concerns regarding privacy. Those concerns have led some to call for legislation mandating that nearly all uses of drones be prohibited unless the government has first obtained a warrant. Such an approach would exceed the requirements of the Fourth Amendment and lead in some cases to perverse results that in some instances would prohibit the use of information when gathered by a drone but would allow the same information to be admitted if gathered by nearly any other means.

Such a technology-centered approach to privacy I think misses the mark. If privacy is the public policy concern, then legislation should address the gathering and use of information in a technology-neutral fashion. This testimony outlines six key issues that Congress should remain cognizant of when drafting legislation.

First, Congress should reject calls for a blanket requirement that all drone use be accompanied by a warrant. Proposals that prohibit the use of drones for the collection of such evidence or information unless authorized by warrant are overbroad and in my view ill-advised. Such legislation treats the information from a drone differently than information gathered from a manned aircraft, differently than that gathered by a police officer in a patrol car or even an officer on foot patrol. Under current Fourth Amendment jurisprudence police are not required to shield their eyes from wrongdoing until they have a warrant. Why impose such a requirement on the collection of information by drones?

Second, Congress should reject broadly worded use restrictions that prohibit the use of any evidence gathered by drones in nearly any proceeding. Such restrictions exceed the parameters of the Fourth Amendment and, in some circumstances, may only serve to protect criminals while not deterring government wrongdoing.

Third, if Congress chooses to impose a warrant requirement, it should carefully consider codifying some exceptions to the warrant requirement. For example, it should codify—as the Supreme Court has noted, suppressing evidence has serious consequences for the truth seeking and law enforcement objectives of our criminal justice system and, as such, should present a high obstacle for those urging for its application. It should be our last resort, not our first impulse. As such, the measures for when we should apply the exclusionary rule should not be whether a drone was used but, rather, should be when the benefits of deterrence outweigh the costs.

Fourth, Congress should spend a substantial amount of time carefully defining terminology and specifying what places are entitled to privacy protection. What a layperson sees when they read the word "search," what a legislator means, and what a court may think the legislature meant are all different things. As such, when using terms like "search," "surveillance," "reasonable expectations," "curtilage," "private property," "public place" and other terms of art that we as lawyers are familiar with, Congress should specify what the terms mean. This definitional task will be the most important part of the legislative drafting process as the terminology will drive what actions are allowable and what places are entitled to privacy protection.

Congress should consider adopting an entirely new set of definitions where necessary and be prepared to reject the existing terminology which may be confusing or overprotective or underprotective.

Fifth, Congress may want to consider crafting simple surveillance legislation rather than very detailed drone-based legislation. Some of the ways that Congress might want to look at this would be to craft a sliding scale for surveillance that looks at the duration for which surveillance might be conducted rather than looking at the platform from which the surveillance is launched, from which the surveillance takes place.

Sixth, Congress should consider adopting transparency and accountability measures, perhaps in lieu of a warrant requirement or suppression rules. Transparency and accountably measures may be more effective than suppression rules or warrants for controlling and deterring wrongful government surveillance. To hold law enforcement accountable, Congress should mandate that the use of all drones or unmanned systems be published on a regular basis, perhaps quarterly, on the Web site of the agency operating the system. These usage logs should detail who operated the system, when it was operated, where it was operated, perhaps even including GPS coordinates, and what the law enforcement purpose for the operation was. Congress may even mandate that manufacturers of unmanned systems make their systems equipped with software that allows for the easy export of flight logs that contain this information. Such logs will allow privacy advocates and concerned citizens to closely monitor how drones are being used and enables the political process as a mechanism to check government action rather than relying on the courts.

The emergence of unmanned aerial vehicles in domestic skies raises understandable privacy concerns that require careful and sometimes creative legislation. Rather than pursuing a drone-specific approach or a warrant-based approach, Congress should consider surveillance legislation aimed at making the use of these systems more transparent and empowering the people to hold government accountable. Thank you.

[The prepared statement of Mr. McNeal follows:]

"Eyes in the Sky: The Domestic Use of Unmanned Aerial Systems"

Testimony by Gregory S. McNeal
Associate Professor of Law
Pepperdine University School of Law

Before the

United States House of Representatives
Committee on the Judiciary
Subcommittee on Crime, Terrorism, Homeland Security and Investigations
May 17, 2013

PEPPERDINE UNIVERSITY
School of Law

The looming prospect of expanded use of unmanned aerial vehicles, colloquially known as drones, has raised understandable concerns regarding privacy. Those concerns have led some to call for legislation mandating that nearly all uses of drones be prohibited unless the government has first obtained a warrant. Such an approach would exceed the requirements of the Fourth Amendment and lead to perverse results that in some instances would prohibit the use of information when gathered by a drone, but would allow the same information to be admitted if gathered by nearly any other means. Such a technology centric approach to privacy misses the mark --- if privacy is the public policy concern, then legislation should address the gathering and use of information in a technology neutral fashion. This testimony outlines six key issues that Congress should remain cognizant of when drafting legislation.

1) CONGRESS SHOULD REJECT CALLS FOR A BLANKET REQUIREMENT THAT ALL DRONE USE BE ACCOMPANIED BY A WARRANT: Proposals that prohibit the use of drones for the collection of evidence or information unless authorized by a warrant are overbroad and ill-advised.[1] Such legislation treats the information from a drone differently than information gathered from a manned aircraft, differently than that gathered by a police officer in a patrol car, or even from an officer on foot patrol. Under current Fourth Amendment jurisprudence, police are not required to shield their eyes from wrongdoing until they have a warrant, why impose such a requirement on the collection of information by drones?

For example, imagine a police officer was on patrol in her patrol car. While driving she witnesses the car in front of her strike a pedestrian and speed off. Until witnessing the crime she did not have probable cause, or even reasonable suspicion to believe the vehicle in front of her would be involved in a crime. Let's further assume that her dash camera recorded the entire incident. That video may be used as evidence against the driver in a subsequent criminal proceeding, but under broadly worded proposals mandating a warrant for drone usage, the same piece of evidence if gathered by a drone would be inadmissible in court. Why?

Consider another example. Police receive an anonymous tip that someone is growing marijuana in their backyard. A police officer attempts to view the backyard from the ground but his view is blocked by a 10 foot tall fence. The officer next decides to fly a commercially available remote controlled helicopter[2] over the backyard and from a vantage point that does not violate FAA regulations observes marijuana plants growing in the yard. This observation would be unlawful under proposals that require a warrant for observations from a drone. However, these facts are nearly identical to the facts in the Supreme Court's 1986 *California v. Ciraolo*[3] decision which upheld aerial surveillance. The only difference is that in *Ciraolo*, the officer flew over the backyard in an airplane, rather than using a drone.

Notably, the fact that Ciraolo had erected a 10 foot fence to manifest his "intent and desire" to maintain privacy did not necessarily demonstrate a reasonable expectation of privacy as the court noted that the fence "might not shield these plants from the eyes of a citizen or a policeman perched on the top of a truck..." Thus, according to the Supreme Court, not only would observation of the marijuana plants from the air (as described above) be lawful, observation from the top of a police truck over the fence would be lawful, and by extension, observation of the marijuana plants by

[1] For example, the "Preserving Freedom from Unwarranted Surveillance Act of 2012."
[2] Perhaps a Parrot A.R. drone from the local mall's Brookstone store.
[3] 476 U.S. 207 (1986).

police from the third floor of a neighboring home would also be lawful. But under proposals requiring a warrant for observations by a drone, this evidence would be inadmissible.

What public policy goal is advanced by the suppression of evidence of a crime when documented by a drone when the same evidence if recorded by a dashcam, observed from an airplane, or viewed from a neighboring home would be admissible in court?

2) CONGRESS SHOULD REJECT BROADLY WORDED USE RESTRICTIONS: Congress should reject broadly worded use restrictions that prohibit the use of any evidence gathered by drones in nearly any proceeding. Such restrictions exceed the parameters of the Fourth Amendment and in some circumstances may only serve to protect criminals while not deterring governmental wrongdoing.

For example, the Alameda County, California Sheriff's Department recently proposed the use of small UASs for: crime scene documentation, EOD missions, HAZMAT response, search and rescue, public safety and life preservation missions, disaster response, fire prevention, and documentation of a felony when such documentation is premised upon probable cause.[4] Linda Lyle, a privacy advocate with the ACLU criticized the proposal, stating: "If the sheriff wants a drone for search and rescue then the policy should say he can only use it for search and rescue...Unfortunately under his policy he can deploy a drone for search and rescue, but then use the data for untold other purposes. That is a huge loophole, it's an exception that swallows the rule."[5] Her points mirror the ACLU's position in their December 2011 white paper where they state that drone use is acceptable so long as "the surveillance will not be used for secondary law enforcement purposes."[6] It is also similar to the language used in other proposals prohibiting the use of information gathered by a drone "as evidence against an individual in any trial, hearing or other proceeding...."

A simple hypothetical can help to illustrate the problem with this approach. Imagine that law enforcement uses a drone to search for a lost hiker in a national park. This is a search and rescue mission that fits within the public safety, emergency, or exigency exceptions in most proposals. However, imagine that during the course of the search the drone observed a man stabbing a woman to death in the park. That collection was entirely inadvertent, and as such suppressing the videotape of the stabbing would not serve to deter the police from using drones in the future as they were not searching for an unrelated stabbing crime, they were searching for a lost hiker. Yet, that evidence under the blanket use restrictions found in various proposals circulating in state legislatures, Congress, and under the ACLU's "secondary law enforcement purposes" standard would need to be suppressed.[7] Such suppression doesn't protect privacy (as inadvertent discovery can't be deterred); it merely protects a criminal who if observed from a helicopter, an airplane, or

---

[4] Alameda County Sheriff's Office, General Order 615 available at: http://nomby.files.wordpress.com/2013/02/small-unmanned-aircraft-system-general-order-6-15-draft.pdf

[5] Paul Detrick, "Cops with Drones: Alameda Co. CA Weighs Technology vs. Privacy" available at: http://reason.com/reasontv/2013/04/04/cops-with-drones-technology-vs-privacy

[6] "Protecting Privacy from Aerial Surveillance: Recommendations for Government Use of Drone Aircraft," American Civil Liberties Union, December 2011, p. 16.

[7] For example, the "Preserving American Privacy Act of 2013" in Section 3119c creates a general prohibition on the use of covered information as "evidence against an individual in any trial, hearing, or other proceeding..." While the Act provides a set of exceptions, including one for emergencies, the language of the emergency exception as currently drafted does not clearly specify that inadvertent discovery of information unrelated to the emergency justifying the drone usage would be admissible, and it's likely that defense counsel in such a case would seek to prohibit the admission of evidence in such a case by relying on the lack of a clearly specified exception.

from the ground would face evidence of his crime, but under some broadly worded drone focused privacy bills may be more difficult to prosecute.

What public policy goal is furthered by suppressing evidence of a crime merely because the evidence was gathered from a drone? If the discovery were genuinely inadvertent, there is little to no deterrent value that justifies suppressing the evidence.

3) IF CONGRESS CHOOSES TO IMPOSE A WARRANT REQUIREMENT, IT SHOULD CAREFULY CONSIDER CODIFYING EXCEPTIONS: If Congress seeks to impose a statutory warrant requirement on the use of drones, it should codify exceptions to the warrant requirement and exclusionary rule that the courts have developed through decades of jurisprudence.

As the Supreme Court has noted, suppressing evidence has serious consequences for the "truth-seeking and law enforcement objectives" of our criminal justice system, and as such should present "a high obstacle for those urging [for its] application"[8] it should be "our last resort, not our first impulse."[9] As such, the measure for when we should apply the exclusionary rule should not be whether a drone was used, but rather should be when "the benefits of deterrence...outweigh the costs."[10] Some exceptions and other procedural devices that Congress should consider codifying are:

- Rather than codify a blanket restriction on the use of any information gathered from a drone, Congress should codify a **standing requirement** that premises one's ability to raise a suppression challenge on whether the person raising the suppression claim was the purported target of drone surveillance. Thus, if law enforcement uses a drone to document illegal dumping of toxic waste by Co-conspirator #1, Co-conspirator #2's privacy rights were not violated and #2 should not have the ability to vicariously assert #1's privacy rights to protect himself from prosecution.
- Evidence gathered by drones should be admissible in proceedings short of trial such as grand jury proceedings,[11] preliminary hearings,[12] bail hearings,[13] and other **non-trial proceedings**.
- Evidence gathered by drones should be admissible for **impeachment purposes** as there is little deterrent value in keeping such impeachment evidence out of a trial (as law enforcement is unlikely to gather it solely for that purpose) and the use of evidence gathered by drones for such a limited purpose furthers the truth-seeking process and deters perjury. [14]

---

[8] *Pennsylvania Board of Probation and Parole v. Scott*, 524 U.S. 357, 364-365 (1998).
[9] *Hudson v. Michigan*, 547 U.S. 586, 591 (2006).
[10] *Herring v. United States*, 129 S. Ct. 695, 700 (2009).
[11] This is consistent with the Supreme Court's approach to Fourth Amendment violations per *United States v. Calandra*, 414 U.S. 338 (1974). (noting that allowing "a grand jury witness to invoke the exclusionary rule would unduly interfere with the effective and expeditious discharge of the grand jury's duties, and extending the rule to grand jury proceedings would achieve only a speculative and minimal advance in deterring police misconduct at the expense of substantially impeding the grand jury's role.").
[12] This is consistent with Congress' guidance in Federal Rule of Criminal Procedure 5.1(c) which states in relevant part "At the preliminary hearing, the defendant may cross-examine adverse witnesses and may introduce evidence but may not object to evidence on the ground that it was unlawfully acquired."
[13] *See* 18 U.S.C. 3142(f) noting the "rules concerning admissibility of evidence in criminal trials do not apply to the presentation and consideration of information at the hearing."
[14] *Contra James v. Illinois*, 493 U.S. 307 (1990).

- If Congress imposes a statutory warrant requirement on the use of drones, it should also codify directly, or by reference the body of jurisprudence associated with the so-called **good faith exception** as articulated in *United States v. Leon*[15] and *Massachusetts v. Sheppard*.[16] The good faith exception allows for the admission of evidence gathered pursuant to a defective warrant, unless, based on objective facts, "a reasonably well trained officer would have known the search was illegal despite the magistrate's authorization."
- Congress should make clear that the **independent source doctrine** as articulated in *Murray v. United States* applies equally to drone related surveillance.[17] The independent source doctrine allows for the admission of evidence, despite police illegality, if the evidence seized was not causally linked to the illegal police conduct.
- Congress should codify the **inevitable discovery rule** articulated in *Nix v. Williams*.[18] In the context of drone surveillance, the rule would operate to allow the admission of drone gathered evidence in a criminal trial if the prosecutor can prove (by a preponderance of the evidence) that the evidence would have ultimately or inevitably been discovered by lawful means.[19]
- Rather than suppress all fruit of drone surveillance, Congress should codify the **attenuation principles** articulated in *Nardone* and *Wong Sun*.[20] The Court in *Wong Sun* stated that when considering whether fruit of an unlawful search should be suppressed, a court must ask "whether, granting establishment of the primary illegality, the evidence to which instant objection is made has been come at by exploitation of that illegality or instead by means sufficiently distinguishable to be purged of the primary taint." Stated differently, at some point the fruit of the poisonous tree loses its potency. Factors Congress should consider codifying are passage of time between the illegal search and the acquisition of evidence, intervening events and a lack of foreseeability that the illegal drone surveillance would result in the gathering of evidence, and whether the initial illegal surveillance was a flagrant or deliberate violation rather than an accidental one.[21]

4) CONGRESS SHOULD SPEND A SUBSTANTIAL AMOUNT OF TIME CAREFULLY DEFINING TERMINOLOGY AND SPECIFYING WHAT PLACES ARE ENTITLED TO PRIVACY PROTECTION: What a layperson sees when they read the word search, what a legislator means, and what a court may think the legislature meant are all different things. As such, when using terms like search, surveillance, reasonable expectations, curtilage, private property, public place and other terms of art, Congress should specify what the terms mean. This definitional task will be the most important part of the legislative drafting process as the terminology will drive what actions are allowable and what places are entitled to privacy protection. Congress should consider adopting an entirely new set of definitions, and be prepared to reject existing terminology which may be confusing. A good example of a well thought out definitional

[15] 468 U.S. 897 (1984).
[16] 468 U.S. 981 (1984).
[17] 487 U.S. 533 (1988).
[18] 467 U.S. 431 (1984).
[19] Note, *Nix* was a Sixth Amendment case but courts have applied the fruits analysis to searches.
[20] *Nardone v. United States*, 308 U.S. 338 (1939) and *Wong Sun v. United States* 371 U.S. 471 (1963) respectively.
[21] *See, Brown v. Illinois*, 422 U.S. 590, 604 (1975).

approach is the proposed legislation offered by Professor Christopher Slobogin.[22] He uses the following terms:

- "Search: An effort by government to find or discern evidence of unlawful conduct. A targeted search seeks to obtain information about a specific person or circumscribed place. A general search seeks to obtain information about people or places that are not targets at the time of the search."
- "Public search: A search of a place, in the absence of explicit consent, focused on activities or persons, limited to what the natural senses of a person on a lawful public vantage point could discern at the time of the search.
- "Probable cause: An articulable belief that a search will more likely than not produce contraband, fruit of crime, or other significant evidence of wrongdoing..."
- "Reasonable suspicion: An articulable belief that a search will more likely than not lead to evidence of wrongdoing...."

5) CONGRESS MAY WANT TO CONSIDER CRAFTING SIMPLE SURVEILLANCE LEGISLATION, RATHER THAN VERY DETAILED DRONE LEGISLATION: In light of the various issues I've raised in my prior points, Congress may find it preferable to legislate with an eye towards controlling surveillance writ large, not just drone surveillance. To do this Congress should focus on controlling the duration of surveillance.

The duration of surveillance can be controlled by crafting legislation that places aggregate limits on how long law enforcement may surveil specific persons or places. Slobogin suggests a sliding scale, allowing for 20 minute searches at an officer's discretion, 20 minute to 48 hour searches with a court order and reasonable suspicion, and searches of longer than 48 hours when accompanied by a warrant and probable cause.[23] The specific amount of time Congress may settle on will depend on whether Congress wants to value privacy or law enforcement efficiency, but the point is that carefully crafting duration based rules for surveillance (whether by drone or otherwise) may be a wiser choice than the current drone focused approach that is riddled with blanket bans and exceptions. (To see the perils of a process riddled with exceptions, look at the recent bill passed by the Texas legislature which has no fewer than 22 exceptions for drone use with carve outs for agriculture interests, electrical companies, oil companies, real estate brokers and others).[24] Rather than crafting special exceptions, legislating with an eye towards creating rules based on clearly defined (albeit arbitrary) durational limits on surveillance creates legislation that is clearer and easier to follow.

6) CONGRESS SHOULD CONSIDER ADOPTING TRANSPARENCY AND ACCOUNTABILITY MEASURES, PERHAPS IN LIEU OF A WARRANT REQUIREMENT OR SUPPRESSION RULES: Transparency and accountability measures may be more effective than suppression rules or warrants for controlling and deterring wrongful government surveillance. To hold law enforcement accountable, Congress should mandate that the use of all drones be published on a regular basis (perhaps quarterly) on the website of the agency operating the system. These usage logs should detail who operated the system, when it was

[22] Christopher Slobogin, "Making the Most of *United States v. Jones* in a Surveillance Society: A Statutory Implementation of Mosaic Theory," Duke Journal of Constitutional Law & Public Policy (forthcoming) available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2098002 .
[23] Slobogin at 24.
[24] See HB 912, available at: http://www.legis.state.tx.us/BillLookup/History.aspx?LegSess=83R&Bill=HB912

operated, where it was operated (including GPS coordinates), and what the law enforcement purpose for the operation was. Congress may even mandate that manufacturers of unmanned systems come equipped with software that allows for the easy export of flight logs that contain this information. Such logs will allow privacy advocates and concerned citizens to closely monitor how drones are being used and enables the political process as a mechanism to hold operators accountable.

In circumstances where publishing usage logs may reveal information that is law enforcement sensitive (such as an ongoing investigation) the agency operating the drone may keep their usage logs confidential until the investigation is closed. The agency should be required to make the logs public within 30 days of the close of an investigation. To facilitate public accountability Congress should mandate that all logs be published in an open and machine readable format consistent with the President's Executive Order of May 9, 2013.

For evidence that this flight log approach works, one need only look across the Atlantic to the UK where many police departments publish their helicopter flight logs on their webpage --- in fact some even live Tweet their helicopter's activities. While there is no law within the United Kingdom that specifically requires police departments or law enforcement agencies to publish the flight logs of their helicopters, their version of the Freedom of Information Act appears to be the legislative authority prompting publication of police helicopter logs.

Like the United States, there are a number of public watchdog groups in the United Kingdom that monitor police activity, including groups whose sole purpose is to monitor the activity (and related noise complaints) of police helicopters.[25] These groups, and their respective websites, act as a forum for noise and privacy complaints from various individuals across the Kingdom, and several of these groups organize and lobby Members of Parliament (MPs) to pass legislation restricting helicopter flyovers.[26] These groups, and the advocacy which they generate, appear to be largely responsible for the recent trend of many UK police departments publishing their helicopters' flight logs, or even creating Twitter accounts for their helicopters that publish real-time or delayed-time updates of the aircraft's activity.[27]

These helicopter Twitter accounts, which have become a growing trend amongst British police departments, have had an immediate and powerful effect on public relations in their respective jurisdictions. In Islington, the police department went from struggling to handle the overload of noise complaints relating to the department's use of its helicopter to receiving no complaints after the creation of its Helicopter Twitter feed.[28] The Twitter account gained over 7,000 followers after its first few weeks, and the public criticism of police helicopter activity ceased entirely. The officer

[25] See http://www.helicopter-noise.org.uk/; http://www.whatdotheyknow.com/request/issue_of_police_helicopter_fligh

[26] See http://www.parliament.uk/edm/2012-13/394 (proposed legislation to regulate/reduce the amount of noise pollution caused by nighttime police helicopter flyovers in London).

[27] Not all activity is published. The Cleveland (UK) Police Department's website indicates that: "This page is intended to provide basic information to the general public regarding the work of the police helicopter and will be updated on a daily basis. Weekend and public holiday updates will appear on the next working day. Please note that not all items are always listed due to operational sensitivity or ongoing investigation." http://www.cleveland.police.uk/news/helicopter-watch.aspx

[28] http://www.islingtongazette.co.uk/news/police_helicopter_twitter_account_stops_islington_complaints_1_1206725

second in command of the department reflected on the effectiveness—as well as future potential—of the Twitter feed by issuing this statement:

> Maybe that is all people wanted – just to know and understand what we were doing. We don't update people in real time, but my vision is that soon we will be able to let people know about an operation as soon as it is over. In some cases we could get them to help – imagine if an elderly person with Alzheimer's was missing in Islington, we could Tweet our followers to keep an eye out.

The Suffolk Police Department launched its Twitter feed with the hope of shedding some light on police practices. Roger Lewis, an observer with the Suffolk Police, described the department's intentions in the following way:

> We hope to use the Twitter feed to highlight the positive work being done by the Air Operations Unit and to keep members of the public informed as to why the helicopter has been deployed. We hope people will enjoy finding out more about the Unit and hopefully our tweets will give some explanation as to why we have been deployed and give some interesting insights into a very important policing tool.[29]

It is not difficult to see how the practice of disclosing non-sensitive flight logs through a public channel—such as a department web page or through Twitter—can be a useful tool in reassuring the public that law enforcement's helicopter does not represent Big Brother's eye in the sky, but rather embodies a part of the department's lawful policing practices. Just as a police helicopter high overhead can be ominous to those on the ground who are unaware of its purposes, the very idea of drones—of any kind—flying above American cities and towns might be foreboding to many lay persons. By requiring law enforcement to publish data or logs Congress can add a citizen centric political check that will help quell the fears of a society that is not yet certain how it should react to the increasing presence of drones over the skies of America.

CONCLUSION

The emergence of unmanned aerial vehicles in domestic skies raises understandable privacy concerns that require careful and sometimes creative solutions. However, we should reject alarmist calls that suggest we are on the verge of an Orwellian police state as we've heard these calls before and they did not come true.[30] In 1985, the ACLU argued in an amicus brief filed in *California v. Ciraolo* that police observation from an airplane was "invasive modern technology" and upholding the search of Ciraolo's yard would "alter society's very concept of privacy." Later, in 1988, the ACLU argued in *Florida v. Riley* that allowing police surveillance by helicopter was "Orwellian" and "would expose all Americans, their homes and effects, to highly intrusive snooping by government agents..." In a different context in 2004 (before the advent of the iPhone) police in Boston were going to use Blackberry phones to access public databases --- the equivalent of Googling. Privacy advocates decried the use of these handheld phones as "mass scrutiny of the lives and activities of innocent people," and "a violation of the core democratic principle that the government should not be permitted to violate a person's privacy, unless it has a reason to believe that he or she is involved in wrongdoing."[31] Reactionary claims such as these get the public's attention and are easy to make,

[29] http://helihub.com/2012/09/03/uks-suffolk-police-helicopter-unit-now-on-twitter/
[30] Interestingly, Orwell seems to be a favorite citation for the ACLU who has cited him nearly 70 times in briefs.
[31] See Gregory S. McNeal, "Can The 'Drone' Industry Compete With The Privacy Lobby?" available at: http://www.forbes.com/sites/gregorymcneal/2012/08/13/can-the-drone-industry-compete-with-the-privacy-lobby/

but have the predicted harms come true? Is the sky truly falling? We should be careful to not craft hasty legislation based on emotionally charged rhetoric. Outright bans on the use of drones and broadly worded warrant requirements that function as the equivalent of an outright ban do little to protect privacy or public safety and in some instances will only serve to protect criminal wrongdoing. Rather than pursuing a drone specific approach or a warrant based approach, Congress should consider surveillance legislation aimed at making the use of these systems more transparent and empowering the people to hold operators accountable.

ATTACHMENT

Forbes

North Carolina's Poorly Worded Drone Killing Privacy Bill

GREGORY S. MCNEAL

This article is available online at:
http://www.forbes.com/sites/gregorymcneal/2013/03/31/north-carolinas-poorly-worded-drone-killing-privacy-bill/

A bill introduced in the North Carolina General Assembly will practically ground all future drone use in the state if it is not rewritten. The bill proposes to "regulate the use of drones to conduct searches" and is already being praised by the ACLU of North Carolina as an "opportunity to place strong safeguards and regulations on the use of drones . . . ." The bill, however, doesn't regulate the use of drones so much as it buries their operation in ambiguities and contradictory constraints.

The so called "Preserving Privacy Act of 2013" would, barring a few narrow exceptions, make it unlawful for an individual or State agency "to use a drone for the purpose of gathering evidence . . . pertaining to criminal conduct." It takes an aerial axe to the long-established plain view doctrine, which allows law enforcement officers to seize evidence and contraband found when an officer observes that evidence and contraband from a lawful vantage point. The bill accomplishes this by making any information or data acquired from the warrantless use of a drone inadmissible in civil, criminal, or administrative proceedings unless the drone's use fell under a handful of narrow exceptions. Inadvertent discovery of a crime isn't listed as one of those exceptions. If this bill passes, evidence of a person stabbing someone to death, if inadvertently collected by a drone, would be inadmissible in any criminal or civil proceeding. The bill imposes restrictions that don't exist for ordinary law enforcement officers on the ground or flying overhead in manned aircraft. Society has never before asked the police to look the other way when they inadvertently observe criminal conduct from a lawful vantage point, but North Carolina's proposed law would force them to do just that.

While the bill (in Part C) allows for several exceptions to the limitation on drone usage, those exceptions are largely meaningless. For example, the second exception listed in the bill states that drones may be used to conduct a search within the "Search and Seizure by Consent" provision of the state's general statute. While, the state's general statute gives a law enforcement officer the authority to conduct a warrantless search and make seizures when individuals and property owners give their consent to search their persons, possessions, or property –it is difficult

to see how this would be implemented in an aerial context. Will police need to go door to door asking residents if they wouldn't mind a drone flying overhead? Why the special restrictions for drones but not for manned helicopters?

The Supreme Court has held time and time again that non-intrusive aerial surveillance over areas open to public view does not constitute a search prohibited by the Fourth Amendment (see *California v. Ciraolo, Florida v. Riley, Dow Chemical v. United States)*, so perhaps the drafters of the bill are more concerned about any aerial observation, not just those observations that would trigger Fourth Amendment scrutiny (i.e. would be a search). What, then, constitutes an unlawful observation for the purposes of this new law? Let's consider a scenario where a drone is launched in response to a 911 call, and is deployed to 1313 Mockingbird Lane, the site where the call originated. If a subject runs from 1313 Mockingbird Lane to 1315 Mockingbird Lane, does the drone need to go blind? Will police need to contact each person in the neighborhood to get their consent prior to observing their property? After all, the bill limits the scope of an undefined "search" to collection of "information or data only on the person or location subject to the search," and also requires that operators "avoid information or data collection on individuals, homes, or areas other than the subject of the search." The 911 scenario seems to fit within the bills prohibitions. Perhaps the bill's drafters were hoping that drones would have automated technology that blurs or redacts all other persons or properties other than the subject of the "search?" (That might be a good idea, but the bill doesn't take this path, rather it seems headed toward prohibition).

Another way in which the bill is a drone killer is in Part G, where the bill requires the destruction of any information collected in violation of the law within 24 hours of the information's collection. Juxtapose that provision against Part E which allows those who have been aggrieved under this new law to sue the violating agency or individual, and even provides for criminal punishment for improper collection activities. Careful readers will immediately note the dilemma: A drone operator could be prosecuted or sued for (1) collecting information in the first place, (2) destroying that information (because she is covering up evidence of a crime as well as discoverable evidence in a lawsuit), and (3) prosecuted for not destroying the information (as required by the law). If I'm a trial lawyer, I love the Catch 22 this provision creates. Actually, privacy advocates will find a lot to love in this bill in general. The document reeks of ambiguities and vagueness, and leaves a lot of room to argue that just about any use of a drone in any situation violates some portion or provision of the proposed law.

If preventing drones from ever being operated is the goal of the bill's sponsors, then this bill will do the trick. But if the drafters are serious about wanting to allow drone usage while still protecting privacy, this bill will require substantial rewriting.

Gregory S. McNeal is a professor specializing in law and public policy. You can follow him on Twitter @GregoryMcNeal.

Mr. SENSENBRENNER. Thank you very much.
Mr. Maclin.

TESTIMONY OF TRACEY MACLIN, PROFESSOR OF LAW, BOSTON UNIVERSITY SCHOOL OF LAW

Mr. MACLIN. Thank you, Mr. Chairman, Ranking Member Scott, and Members of the Committee for inviting me to testify about the Fourth Amendment issues surrounding the domestic issue—domestic use of drones by law enforcement officials. The constitutionality of drones for domestic law enforcement purposes raises several important questions that are not easily answered by the Supreme Court's current Fourth Amendment jurisprudence.

As you know, drones can be equipped with sophisticated cameras, thermal imaging devices, license plates readers, and laser radar systems. According to a recent paper by the Congressional Research Service, drones will soon be able to operate with facial recognition or soft biometric recognition equipment that can recognize and track individuals based on attributes, such as height, age, gender, skin color. Because of the advanced technology now available, comparing a drone to a traditional airplane or helicopter is like comparing a frisk from a police officer to a modern x-ray machine that can see beneath one's clothes and graphically depict one's physical features.

The Supreme Court's 1980 Supreme Court rulings that airplanes and helicopter surveillance do not implicate the Fourth Amendment were premised on naked eye observations and surveillance equipment that was readily available to the public. For example, in *California v. Ciraolo*, Chief Justice Burger's majority opinion distinguished concerns about future electronic developments from what he called, quote, simple visual observations from a public place that were challenged in Ciraolo. Moreover, in each of these cases the court signaled that more intrusive and sophisticated police surveillance would raise different and very, and more difficult Fourth Amendment issues.

Thus, I agree with our previous speaker, John Villasenor that the Court's 1980 rulings do not control the use of drones that are capable of capturing much more detail unavailable to the human eye. Furthermore, it is important to recognize, even among the Justices of the current Court, that the definition of what constitutes a search and thus what triggers the Fourth Amendment is subject to change, and I would say is in a state of flux.

In the recent GPS case, *United States v. Jones*, five justices indicated a willingness to reassess traditional notions of privacy under the Court's Katz analysis. For example, Justice Sotomayor encouraged her colleagues to reconsider the Court's traditional analysis for even short-term monitoring of a person's public activities. And Justice Alito, although not going as far as Justice Sotomayor, indicated his willingness to consider the Court's current privacy jurisprudence. And I state from Justice Alito's concurrence and dissent, he said, quote, The use of longer-term GPS monitoring investigations of most criminal offenses impinges expectations of privacy. Now, what I read from that are five of the justices are saying that you have an expectation of privacy vis-a-vis long-term electronic monitoring when you are in the public. Well, if you have got that

expectation of privacy, at least in the eyes of five of the Justices when you are in the public, when you are on the public streets, you certainly ought to have that same level of expectation of privacy when you are on your own property, notwithstanding the fact that a drone may or may not be in navigable air space.

A final point I think the Committee should consider is the following: When considering whether drone surveillance constitutes a search under the Fourth Amendment, I would urge the Committee to avoid resolving this question with litmus tests or, as Mr. McNeal pointed out, legal terms of art. The expectation of privacy tests out of Katz is a vague subjective test. Most of the Justices have acknowledged that, even Justice Harlan, who of course is responsible for the expectation of privacy tests, disavowed that test in the *United States v. White* decision, which was a 1971 decision. Often judges when deciding Fourth Amendment cases will simply say all the Fourth Amendment requires is reasonableness, and they will judge the case accordingly. In these cases, the courts typically apply what amounts to a rational basis test, simply deciding whether or not the government activity was rationally related to a legitimate governmental interest.

This degree of deference to police intrusions, I suggest, is at odds with the central meaning of the Fourth Amendment. The Fourth Amendment was not asserted in the Bill of Rights so that judges could defer to governmental intrusions on privacy. Rather, we know, the amendment was put in the Bill of Rights so that the government could control.

Sorry, Mr. Chairman.

[The prepared statement of Mr. Maclin follows:]

Boston University School of Law

765 Commonwealth Avenue
Boston, Massachusetts 02215
T 617-353-4688 F 617-353-3077
tmaclin@bu.edu

Tracey Maclin
Professor of Law

BOSTON UNIVERSITY

House Judiciary Subcommittee on Crime, Terrorism, Homeland Security and Investigations
May 15, 2013

Written Statement of Tracey Maclin
Professor of Law
Boston University School of Law

Thank you Chairman Sensenbrenner, ranking Member Scott, and members of the Committee for inviting me to testify about the Fourth Amendment issues surrounding the domestic use of drones by law enforcement officials.

My name is Tracey Maclin. I am a law professor at Boston University School of Law. I have taught Constitutional Law and Criminal Procedure since 1985. My opening comments will be brief.

The constitutionality of drones for domestic law enforcement purposes raises several questions that are not easily answered by the Supreme Court's current jurisprudence.

Drones can be equipped with sophisticated cameras, thermal imaging devices, license plate readers and laser radar systems. According to a recent paper by the Congressional Research Service, soon drones will be able to operate with facial recognition or soft biometric recognition

equipment that can "recognize and track individuals based on attributes such as height, age, gender, and skin color."

Because of the advanced technology now available, comparing a drone to a traditional airplane for Fourth Amendment purposes is similar to comparing a frisk conducted by a security guard to a modern x-ray machine that can see beneath one's clothing utilized at some airports.

The 1980s Supreme Court rulings that airplane and helicopter surveillance did not implicate the Fourth Amendment were premised on naked-eye searches and surveillance equipment that was readily available to the public. For example, in *California v. Ciraolo*, Chief Justice Burger's majority opinion distinguished concerns about future electronic developments from "***simple visual observations from a public place***" that were challenged in *Ciraolo*.

Moreover, in each of those cases, the Court signaled that more intrusive and sophisticated police surveillance would raise different and more difficult Fourth Amendment issues. Thus, I agree with the view of John Villasenor that the Court's 1980's rulings do not control the use of drones that are capable of capturing much more detail unavailable to the human eye.

Furthermore, it is important to recognize, even among the Justices of the Roberts' Court, the definition of what constitutes a "search" under the Fourth Amendment is subject to change.

In the recent GPS case, *United States v. Jones*, five Justices indicated a willingness to reassess traditional notions of privacy regarding long-term electronic monitoring of a person's movements in public. Justice

Sotomayor, for example, encouraged her colleagues to reconsider the Court's traditional analysis for even short-term monitoring of a person's public activities. And Justice Alito, although not going as far as Justice Sotomayor in his willingness to reconsider the Court's privacy jurisprudence, did state: "The use of longer term GPS monitoring investigations of most offenses impinges on expectations of privacy."

A final point: When considering whether drone surveillance constitutes a search under the Fourth Amendment, I encourage the Committee to avoid resolving this question with a simplistic litmus test or legal term of art.

When deciding search and seizure cases, often judges will rule that the central point of the Fourth Amendment is "reasonableness." In the typical case, this "reasonableness" model is the equivalent of a rational basis test for judging a statute, or governmental conduct that implicates non-fundamental rights. In these ordinary cases, judges uphold police intrusions because the intrusion rationally serves legitimate state interests.

This degree of deference to police intrusions is at odds with the central purpose of the Fourth Amendment, which is distrust of discretionary police power. The Fourth Amendment was not inserted in the Bill of Rights so that judges could defer to government intrusions of privacy; rather the amendment was designed to control such intrusions. The colonists who battled the British did not trust or defer to the judgments of British customs officials. They wanted the discretionary power of customs officers restrained.

Objections to warrantless drone surveillance do not stem from a view that law enforcement officers are bad people. Instead, objections are raised against this form of police authority because "power is a heady thing, and history shows that the police acting on their own cannot be trusted." This distrust of discretionary police power is the central meaning of the Fourth Amendment.

Thank you for the opportunity to speak today. I look forward to your questions.

Mr. SENSENBRENNER. Thank you very much, Mr. Maclin.

Mr. Calabrese.

TESTIMONY OF CHRISTOPHER R. CALABRESE, LEGISLATIVE COUNSEL, AMERICAN CIVIL LIBERTIES UNION (ACLU)

Mr. CALABRESE. Thank you, Chairman Sensenbrenner, Ranking Member Scott, Members of the Committee, thank you for inviting me to testify today. The ACLU believes that the widespread domestic use of unmanned aerial systems, also known as drones, raises significant new privacy issues which cannot be adequately addressed by existing law.

Drones share some characteristics with manned aerial surveillance, such as planes and helicopters, but the privacy invasion they represent is substantially greater in both scope and volume.

Manned aircraft are expensive to purchase, operate, and maintain. This expense has always imposed a natural limit on the government's aerial surveillance capability.

Drones' low cost and flexibility erode that natural limit. Small, hovering platforms can explore hidden spaces or peer in windows, and large static blimps enable continuous, long-term monitoring, all for much less than the cost of a plane or helicopter.

Ongoing improvements in computing technology exacerbate these privacy issues. High-powered night vision cameras and see-through imaging provide more and better detail. Imagine technology similar to the naked body scanners at the airports attached to a drone. Through technologies like face recognition, improved analytics, and wireless Internet, it is possible to track specific individuals with multiple drones. Uses could extend all the way from high-tech, long-term surveillance to traffic enforcement.

While drones certainly have beneficial uses for search-and-rescue missions, firefighting, dangerous police tactical operations, these technological realities point to significant possible harms if left unchecked. With the use of video cameras, we have seen ongoing problems with voyeurism and racial profiling by operators. If there is a persistent danger of monitoring, it creates the real danger that people will change how they act in public, whether at a protest rally or just sunning themselves in their backyard.

Drones must be integrated into the Federal air space by 2015. While the use of this technology is poised to explode, current law has not yet caught up to this new technology. As Professor Maclin has noted, the Supreme Court has authorized aerial surveillance and photography of private property. The Court may eventually extend Fourth Amendment protections to ongoing and unlimited automated tracking, but no cases have yet been decided around drone use.

Federal privacy protections are spotty and State statutory protections are in their infancy.

As the entity that regulates the skies, the Federal Government is in the best position to create rules for the use of drones by law enforcement. The ACLU recommends that these rules be based on four key principles: First, no mass surveillance. No one should be spied upon by the government unless the government believes that person has committed a crime. Drone use over private property should only happen with a search warrant based on probable

cause, the same standard used to search someone's house or business. It may be permissible to monitor individuals in public at a lower standard, perhaps reasonable suspicion, but the key is to prevent mass suspicion-less searches of the general population, including for intelligence gathering. In order to prevent this pretextual use of drones, exceptions to this rule should be limited to emergencies connected to life and safety or narrowly drawn administrative exceptions.

Second, information collected from drones for one purpose, to combat a fire or perform a search and rescue, should not be used for another purpose, such as general law enforcement. Information collected by drones should also be kept securely and destroyed promptly once it is no longer needed.

Third, drones should not carry weapons. Weapons developed on the battlefield in Iraq and Afghanistan have no place in the United States. There is a consensus forming on this issue. In fact, the Heritage Foundation and the International Association of Chiefs of Police both support sharp limits on weaponized drones.

Finally, oversight is crucial. Communities, not just law enforcement, must play a central role in whether to purchase a drone. Like any new technology, drone use must be monitored to make sure it's a wise investment that works. Drones should only be used if subject to a powerful framework that regulates their use in order to avoid abuse and invasions of privacy. The ACLU believes that some Members of the Committee have already taken great strides to find this balance, with H.R. 637, the Preserving Americans Privacy Act. We support this bipartisan legislation from Mr. Poe and urge the Committee to make marking it up a priority. Thank you.

[The prepared statement of Mr. Calabrese follows:]

STATEMENT OF
CHRISTOPHER R. CALABRESE, LEGISLATIVE COUNSEL

AMERICAN CIVIL LIBERTIES UNION
WASHINGTON LEGISLATIVE OFFICE

on

"Eyes in the Sky: The Domestic Use of Unmanned Aerial Systems before the House Judiciary Committee, Subcommittee on Crime, Terrorism, Homeland Security, and Investigations

May 17, 2013

Good morning Chairman Sensenbrenner, Ranking Member Scott, and Members of the Committee. Thank you for the opportunity to testify on behalf of the American Civil Liberties Union (ACLU) its more than half a million members, countless additional activists and supporters, and fifty-three affiliates nationwide, about the privacy and civil liberties implications of the domestic use of unmanned surveillance vehicles, also known as drones, and recommendations for new protections for use of this technology.

I. Introduction

Unmanned aircraft carrying cameras raise the prospect of a significant new avenue for the surveillance of American life. Many Americans are familiar with these aircraft, commonly called drones, because of their use overseas in places like Afghanistan and Yemen. But drones are coming to America. Recently passed legislation requires the Federal Aviation Administration to "develop a comprehensive plan to safely accelerate the integration of civil unmanned aircraft systems into the national airspace system."[1] This new legislation has dramatically accelerated the deployment of drones and pushed this issue to the forefront. Meanwhile, the technology is quickly becoming cheaper and more powerful, interest in deploying drones among police departments is increasing, and our privacy laws are not strong enough to ensure that the new technology will be used responsibly and consistently with constitutional values. In short, the specter of routine aerial surveillance in American life is on the near horizon — a development that would profoundly change the character of public life in the United States.

We need a system of rules to ensure that Americans can enjoy the benefits of this technology without bringing our country a large step closer to a "surveillance society" in which every move is monitored, tracked, recorded, and scrutinized by the authorities. This statement outlines a set of protections that would safeguard Americans' privacy in the coming world of drones.

Aerial surveillance from manned aircraft has been with us for decades. One of the first aircraft the Wright brothers built was a surveillance aircraft, and it was sold to the U.S. Army. Many common uses of drone aircraft—search and rescue, fighting wildfires, dangerous tactical police operations—are beneficial. In the 1980s the Supreme Court ruled that the Fourth Amendment does not categorically prohibit the government from carrying out warrantless aerial surveillance of private property.

But manned aircraft are expensive to purchase, operate and maintain, and this expense has always imposed a natural limit on the government's aerial surveillance capability. Now that surveillance can be carried out by unmanned aircraft, this natural limit is eroding. The prospect of cheap, small, portable flying video surveillance machines threatens to eradicate existing practical limits on aerial monitoring and allow for pervasive surveillance, police fishing expeditions, and abusive use of these tools in a way that could eventually eliminate the privacy Americans have traditionally enjoyed in their movements and activities. In order to prevent this harmful and invasive outcome, Congress must act.

---

[1] FAA Modernization and Reform Act of 2012, P.L. 112-95, §332, 126 Stat.11, 73. For privacy controls the ACLU recommends the FAA implement as part of its regulatory process please see: http://www.aclu.org/technology-and-liberty/aclu-comment-faa-unmanned-aircraft-system-test-site-program

II. The Technology

There are hundreds of different types of Unmanned Aerial Vehicles (UAVs), as drones are formally known.[2] They can be as large as commercial aircraft or as small as hummingbirds, and include human remotely guided aircraft as well as autonomous, self-guided vehicles. They include:

- **Large fixed-wing aircraft.** The largest UAVs currently in use, such as the Israeli-made Eitan, are about the size of a Boeing 737 jetliner. The Eitan's wingspan is 86 feet, and it can stay aloft for 20 hours and reach an altitude of 40,000 feet.[3] The Predator B drone, which has been used extensively on overseas battlefields as well as on the U.S.-Mexico border, has a wingspan of 66 feet, and it can stay aloft for over 30 hours and reach an altitude of 50,000 feet.[4] In Pakistan and Afghanistan, the U.S. military and CIA deploy Predators and Reapers armed with surveillance capability as well as missiles capable of destroying a moving vehicle from thousands of feet in the air.[5]

- **Small fixed-wing aircraft.** Smaller fixed-wing aircraft are the current favorite for domestic deployment. The Houston police department, for example, recently tested the ScanEagle, made by Boeing subsidiary Insitu.[6] The ScanEagle is 4 ½ feet long with a wingspan of 10 feet, and it can climb to 19,500 feet and stay aloft for more than 24 hours.[7]

- **Backpack craft.** Another class of craft is designed to be carried and operated by a single person. The hand-launched AeroVironment Raven, for example, weighs 4 pounds, has a wingspan of 4.5 feet and a length of 3 feet, can fly up to 14,000 feet and stay aloft for up to 110 minutes. Similar-sized products include a three-foot helicopter called the Draganflyer X6, a one-foot-long, one-pound fixed-wing craft called the AeroVironment Wasp, and a fan-propelled craft called the Honeywell T-Hawk that can "hover and stare." Individual hobbyists have also built a number of drones in this size range.[8]

---

[2] See Wikipedia, "List of unmanned aerial vehicles," at http://en.wikipedia.org/wiki/List_of_unmanned_aerial_vehicles.

[3] "Israel unveils world's largest UAV," Homeland Security Newswire, Feb. 23, 2010, online at http://homelandsecuritynewswire.com/israel-unveils-worlds-largest-uav.

[4] See General Atomics web page on Predator B at http://www.ga-asi.com/products/aircraft/predator_b.php; R.P.G. Collinson, Introduction to Avionic Systems (2011), p. 495

[5] Yochi J. Dreazen, "From Pakistan, With Love: The technology used to monitor the skies over Waziristan is coming to your hometown," National Journal, March 13, 2011, online at http://www.nationaljournal.com/magazine/drones-may-be-coming-to-your-hometown-20110313.

[6] Stephen Dean, "Police line up to use drones on patrol after Houston secret test," Houston Examiner, Jan. 11, 2010, online at http://www.examiner.com/page-one-in-houston/police-line-up-to-use-drones-on-patrol-after-houston-secret-test.

[7] Insitu, ScanEagle brochure, online at http://www.insitu.com/documents/Insitu%20Website/Marketing%20Collateral/ScanEagle%20Folder%20Insert.pdf

[8] AeroVironment brochure, online at http://www.avinc.com/downloads/Raven_Domestic_1210.pdf; AeroVironment web page on the Wasp at http://www.avinc.com/uas/small_uas/wasp/; Carrie Kahn, "It's A Bird! It's A Plane! It's A Drone!" National Public Radio, March 14, 2011, online at http://www.npr.org/2011/03/14/134533552/its-a-bird-its-a-plane-its-a-drone; "Drones on the home front," Washington Post, Jan. 23, 2011, online at http://www.washingtonpost.com/wp-srv/special/nation/drone-gallery/

- **Hummingbirds.** A tiny drone called the Nano Hummingbird was developed for the Pentagon's Defense Advanced Research Projects Agency (DARPA) by AeroVironment. Intended for stealth surveillance, it can fly up to 11 miles per hour and can hover, fly sideways, backwards and forwards, for about 8 minutes. It has a wingspan of 6.5 inches and weighs only 19 grams—less than a single AA battery.[9]

- **Blimps.** Some blimps are envisioned as high-altitude craft, up to 300 feet in diameter, that would compete with satellites, while others would be low-altitude craft that would allow the police to monitor the streets. Supporters say they are more cost-effective than other craft due to their ability to stay aloft for extended periods.[10]

III. Drone Capabilities—Today and in the Future

The aircraft themselves are steadily improving and, as with so many technologies, that is likely to continue. They are becoming smaller. The military and law enforcement are keenly interested in developing small drones, which have the advantages of being versatile, cheap to buy and maintain, and in some cases so small and quiet that they will escape notice.[11] They are also becoming cheaper. The amazing continual decreases in the prices of electronics that have become normal in our time all but guarantee that the surveillance technologies attached to UAVs will become less expensive and yet more powerful—and with mass production, the aircraft that carry those electronics will become inexpensive enough for a police department to fill the skies over a town with them.

Drones are also becoming smarter. Artificial intelligence advances will likely help drones carry out spying missions. Korean researchers, for example, are working to teach robots how to hide from and sneak up upon a subject.[12] They also will have better staying power, with a greater ability to stay aloft for longer periods of time. Mechanisms for increasing time aloft could include solar power, or the use of blimps or gliders.[13]

---

[9] W.J. Hennigan, "It's a bird! It's a spy! It's both," Los Angeles Times, Feb. 17, 2011, online at http://articles.latimes.com/2011/feb/17/business/la-fi-hummingbird-drone-20110217.

[10] On high-altitude blimps see Elliott Minor, "Interest Growing in 'Security' Blimps," Associated Press, April 27, 2004, available online at http://www.rustysforum.com/cgi-bin/domains/com/rustysforum/frc_bb/ultimatebb.cgi?ubb=next_topic&f=1&t=000807&go=older; on low-altitude blimps see e.g. James Nelson, "Utah city may use blimp as anti-crime spy in the sky," Reuters, Jan. 16, 2011, online at http://www.reuters.com/article/2011/01/16/us-crime-blimp-utah-idUSTRE70F1DJ20110116.

[11] W.J. Hennigan, "It's a bird! It's a spy! It's both," Los Angeles Times, Feb. 17, 2011, online at http://articles.latimes.com/2011/feb/17/business/la-fi-hummingbird-drone-20110217.

[12] M. Ryan Calo, "Robots and Privacy," April 2010, online at http://ssrn.com/abstract=1599189.

[13] "Gliders Emerge As Surveillance UAVs," Aviation Week, June 8, 2010, online at http://www.aviationweek.com/aw/generic/story_generic.jsp?topicName=ila_2010&id=news/awx/2010/06/08/awx_06_08_2010_p0-232627.xml; James Nelson, "Utah city may use blimp as anti-crime spy in the sky," Reuters, Jan. 16, 2011, online at http://www.reuters.com/article/2011/01/16/us-crime-blimp-utah-idUSTRE70F1DJ20110116; Ned Smith, "Solar-powered UAV can stay aloft 5 years," TechNewsDaily, Sept. 22, 2010, online at http://www.msnbc.msn.com/id/39313306/ns/technology_and_science-tech_and_gadgets/t/solar-powered-uav-can-stay-aloft-years.

Although the primary uses of drones so far have been military, even on overseas battlefields their main use is surveillance. The larger drones can be fitted with weapons or other heavy payloads, but all of them can carry cameras and other imaging technologies that have developed amazing capabilities in recent years and are likely to become even more capable in the near future.

Except for possibly the very lightest craft, drones can carry the full range of advanced surveillance technologies that have been developed—and are likely to be developed—including:

- **High-power zoom lenses.** UAVs can carry increasingly powerful lenses that allow significant zooming, increasing the chance that individuals will come under scrutiny from faraway aircraft without knowing it. And the density of photo sensors is growing at an exponential pace (in line with Moore's law), allowing for higher and higher resolution photos to be taken for the same price camera.[14]

- **Night vision.** Infrared and ultraviolet imaging enable night vision by capturing light outside the spectrum visible to the human eye. Infrared imaging (also known as thermal imaging) shows heat emitted by an object, and so is especially suited for identifying humans and animals in the dark.[15] Ultraviolet (UV) imaging can detect some materials not visible in natural or infrared light, and can also be used to enhance detail; for instance, it can be used to image surface textures not apparent in visible light.[16] Moving forward, thermal imaging is likely to improve—for example becoming more sensitive and available at higher resolutions.

- **See-through imaging.** The military is developing radar technologies that can see through ceilings and walls and allow the tracking of human targets even when they are inside buildings.[17] A technology called Synthetic Aperture Radar, for example, can see through cloudy and dusty conditions and through foliage, and has the potential to penetrate the earth and walls.[18]

---

[14] Nathan Myhrvold, "Moore's Law Corollary: Pixel Power," New York Times, June 7, 2006, online at http://www.nytimes.com/2006/06/07/technology/circuits/07essay.html. Moore's law is the observation that the number of transistors that can be placed on an integrated circuit—and therefore broadly speaking the power of computers—doubles approximately every two years. It has held true for over 50 years.

[15] NASA Science Mission Directorate, "Infrared Energy," Mission: Science, 2010, online at http://missionscience.nasa.gov/ems/07_infraredwaves.html.

[16] Austin Richards, "Digital Reflected-Ultraviolet Imaging," Advanced Imaging, Apr. 2006, online at http://www.uvcorder.com/pdf/ADI0406%20Component%2018-20.pdf.

[17] See e.g., William Saletan, "Nowhere To Hide," Slate.com, Sept. 17, 2008, online at http://www.slate.com/articles/health_and_science/human_nature/2008/09/nowhere_to_hide.html Greg Miller and Julian E. Barnes, "Special drones pursue militias," Los Angeles Times, Sept. 12, 2008, online at http://articles.latimes.com/2008/sep/12/world/fg-pakistan12.

[18] "Ground Moving Target Indicator (GMTI) Radar Discrimination of Combatants versus Animals in Severe Clutter," DARPA, undated document (topic number SB082-019), online at http://www.dodsbir.net/sitis/archives_display_topic.asp?Bookmark=32303. Sandia National Laboratories, "Synthetic Aperture Radar Applications," undated, online at http://www.sandia.gov/radar/sarapps.html; Alicia Tejada, "MIT Develops New Radar Technology: Military Could See Through Walls," ABC News, Oct. 20, 2011, online at http://abcnews.go.com/Technology/radar-technology-mit-walls/story?id=14773871.

- **Video analytics.** This field seeks to apply artificial intelligence techniques not just to collect but also to "watch" video. The technology has been improving rapidly, and can recognize and respond to specific people, events, and objects.[19] One of the most significant uses would be to continually track individuals or vehicles as they move about, using face recognition or other bodily characteristics.[20] It might also be used to identify particular movement patterns as "suspicious," or to identify and flag changes in routines, buildings or grounds.[21] Computers performing these tasks have a distinct advantage over human observers, because as one observer summed it up, "machines do not blink or forget. They are tireless assistants."[22]

The PBS series NOVA, "Rise of the Drones," recently aired a segment detailing the capabilities of a powerful aerial surveillance system known as ARGUS-IS. This system, which is basically a super-high, 1.8 gigapixel resolution camera that can be mounted on a drone, demonstrates many of these capacities. The system is capable of high-resolution monitoring and recording of an entire city. To witness a demonstration of this capacity please see: http://www.youtube.com/watch?feature=player_embedded&v=13BahrdkMU8

IV. UAVs and Possible Harms

With the federal government likely to permit more widespread use of drones, and the technology likely to become ever more powerful, the question becomes: what role will drones play in American life? Based on current trends—technology development, law enforcement interest, political and industry pressure, and the lack of legal safeguards—it is clear that drones pose a looming threat to Americans' privacy. The reasons for concern reach across a number of different dimensions:

- **Mission creep.** Even where UAVs are being envisioned for search and rescue, fighting wildfires, and in dangerous tactical police operations, they are likely to be quickly embraced by law enforcement around the nation for other, more controversial purposes. The police in Ogden, Utah think that floating a surveillance blimp above their city "will be a deterrent to crime when it is out and about."[23] In Houston, police suggested that drones could possibly be used for writing traffic tickets.[24] The potential result is that they become commonplace in American life.

---

[19] Vigilant Video, online at http://www.vigilantvideo.com

[20] Noah Shachtman, "Army Tracking Plan: Drones That Never Forget a Face," *Wired.com*, Sept. 28, 2011, online at http://www.wired.com/dangerroom/2011/09/drones-never-forget-a-face/.

[21] On change detection, see Sandia National Laboratories, "Synthetic Aperture Radar Applications," undated, online at http://www.sandia.gov/radar/sarapps.html.

[22] Steve Lohr, "Computers That See You and Keep Watch Over You," *New York Times*, Jan. 1, 2011, online at http://www.nytimes.com/2011/01/02/science/02see.html.

[23] James Nelson, "Utah city may use blimp as anti-crime spy in the sky," Reuters, Jan. 16, 2011, online at http://www.reuters.com/article/2011/01/16/us-crime-blimp-utah-idUSTRE70F1DJ20110116.

[24] Stephen Dean, "Police line up to use drones on patrol after Houston secret test," Houston Examiner, Jan. 11, 2010, online at http://www.examiner.com/page-one-in-houston/police-line-up-to-use-drones-on-patrol-after-houston-secret-test.

- **Tracking.** The Justice Department currently claims the authority to monitor Americans' comings and goings using cell phone and GPS tracking devices—under uncertain legal standards. Fleets of UAVs, interconnected and augmented with analytics software, could enable the mass tracking of vehicles and pedestrians around a wide area.

- **New uses.** The use of drones could also be expanded from surveillance to actual intervention in law enforcement situations on the ground. Airborne technologies could be developed that could, for example, be used to control or dispel protesters (perhaps by deploying tear gas or other technologies), stop a fleeing vehicle, or even deploy weapons.[25]

In addition, drones raise many of the same issues that pervasive video surveillance brings in any context. For example:

- **Chilling effects.** What would be the effect on our public spaces, and our society as a whole, if everyone felt the keen eye of the government on their backs whenever they ventured outdoors? Psychologists have repeatedly found that people who are being observed tend to behave differently, and make different decisions, than when they are not being watched. This effect is so great that a recent study found that "merely hanging up posters of staring human eyes is enough to significantly change people's behavior."[26]

- **Voyeurism.** Video surveillance is susceptible to individual abuse, including voyeurism. In 2004, a couple making love on a dark nighttime rooftop balcony, where they had every reason to expect they enjoyed privacy, were filmed for nearly four minutes by a New York police helicopter using night vision. This is the kind of abuse that could become commonplace if drone technology enters widespread use. (Rather than apologize, NYPD officials flatly denied that this filming constituted an abuse, telling a television reporter, "this is what police in helicopters are supposed to do, check out people to make sure no one is … doing anything illegal").[27]

- **Discriminatory targeting.** The individuals operating surveillance systems bring to the job all their existing prejudices and biases. In Great Britain, camera operators have been found to focus disproportionately on people of color. According to a sociological study of how the systems were operated, "Black people were between one-and-a-half and two-

[25] Joseph Nevins, "Robocop: Drones at Home," Boston Review, January/February 2011, online at http://www.bostonreview.net/BR36.1/nevins.php.
[26] Sander van der Linden, "How the Illusion of Being Observed Can Make You a Better Person," Scientific American, May 3, 2011, online at http://www.scientificamerican.com/article.cfm?id=how-the-illusion-of-being-observed-can-make-you-better-person; M. Ryan Calo, "People Can Be So Fake: A New Dimension to Privacy and Technology Scholarship," 114 Penn St. L. Rev. 809, online at http://www.pennstatelawreview.org/articles/114/114%20Penn%20St.%20L.%20Rev.%20809.pdf.
[27] "Did NYPD Cameras Invade A Couple's Privacy?" WCBS-TV report, Feb. 24, 2005, video no longer available online; Jim Dwyer, "Police Video Caught a Couple's Intimate Moment on a Manhattan Rooftop," *New York Times*, Dec. 22, 2005, online at http://www.nytimes.com/2005/12/22/nyregion/22rooftop.html.

and-a-half times more likely to be surveilled than one would expect from their presence in the population."[28]

- **Institutional abuse.** In addition to abuse by the inevitable "bad apples" within law enforcement, there is also the danger of institutional abuse. Sometimes, bad policies are set at the top, and an entire law enforcement agency is turned toward abusive ends. That is especially prone to happen in periods of social turmoil and intense political conflict. During the labor, civil rights, and anti-Vietnam war movements of the 20th century, the FBI and other security agencies engaged in systematic illegal behavior against those challenging the status quo. And once again today we are seeing an upsurge in spying against peaceful political protesters across America.[29]

- **Automated enforcement.** Drones are part of a trend toward automated law enforcement, in which cameras and other technologies are used to mete out justice with little or no human intervention. This trend raises a variety of concerns, such as the fact that computers lack the judgment to fairly evaluate the circumstances surrounding a supposed violation, and may be susceptible to bugs and other software errors, or simply are not programmed to fairly and properly encapsulate the state of the law as passed by legislatures.[30]

One point that is often made about new surveillance technologies is that, while they may increase government surveillance of individuals, they can also increase individuals' ability to record the activities of officials, which can serve as a check on their power. Too often, however, the authorities seek to increase their surveillance over individuals (for example, by installing surveillance cameras throughout public spaces) while restricting individuals' ability to use that same technology as a check against their power (for example, by attempting to prevent individuals from videotaping police[31]). Already, security experts have started expressing concern that unmanned aircraft could be used for terrorism[32]—which naturally raises the question: will individuals be able to make use of the new technology for their own purposes, or will government seek a monopoly over the new technology by citing fears of its use for terrorism?

V. The Fourth Amendment and the Use of Drones

The Supreme Court has never taken a position on whether the Fourth Amendment places limits on government use of UAV surveillance. However, it allowed some warrantless aerial surveillance from *manned* aircraft.

---

[28] Clive Norris and Gary Armstrong, "The Unforgiving Eye: CCTV Surveillance in Public Spaces," Centre for Criminology and Criminal Justice at Hull University, 1997.
[29] See ACLU "Spyfiles" web site at www.aclu.org/spyfiles.
[30] Danielle Keats Citron, "Technological Due Process," 85 Washington University Law Review 1249 (2008), online at http://lawreview.wustl.edu/inprint/85/6/Citron.pdf.
[31] See Jay Stanley, "You Have Every Right to Photograph That Cop," ACLU, online at http://www.aclu.org/free-speech/you-have-every-right-photograph-cop.
[32] Agence France Press, "Flying Robot Attacks 'Unstoppable' Say Experts," Agence France Press, May 11, 2006, available online at http://www.rense.com/general71/sspm.htm.

- In the 1986 decision **California v. Ciraolo**, the Supreme Court focused on whether an individual has a privacy interest in being free from aerial surveillance of his backyard. The police had received a tip that Dante Ciraolo was growing marijuana in his backyard, but high fences prevented them from viewing his backyard from the street. The police borrowed a plane, flew it over the backyard and easily spotted marijuana plants growing there. Ciraolo argued that his Fourth Amendment rights were violated because the government did not get a warrant. The Court rejected this argument, explaining that there was no intrusion into his privacy because "[a]ny member of the public flying in this airspace who glanced down could have seen everything that these officers observed."[33]

- **Dow Chemical Co. v. United States**, also decided in 1986, the Supreme Court addressed whether the Environmental Protection Agency violated Dow's Fourth Amendment rights when it employed a commercial aerial photographer to use a precision aerial mapping camera to take photographs of a chemical plant. The Court found no violation, in part because the camera the EPA used was a "conventional, albeit precise, commercial camera commonly used in mapmaking," and "the photographs here are not so revealing of intimate details as to raise constitutional concerns." However, the Court suggested that the use of more sophisticated, intrusive surveillance might justify a different result. It wrote, "surveillance of private property by using highly sophisticated surveillance equipment not generally available to the public, such as satellite technology, might be constitutionally proscribed absent a warrant."[34]

- In **Florida v. Riley**, decided in 1989, the police had received a tip that Michael Riley was growing marijuana in a greenhouse on the property surrounding his home. The interior of the greenhouse was not visible from the ground outside the property, and the greenhouse had a ceiling, though two panels in the ceiling were missing. A police officer flew over the greenhouse and spotted marijuana through the openings in the roof. While no reasoning commanded a majority of the Court, four justices concluded that its decision in *Ciraolo* applied because Riley had left part of the greenhouse open to public view, and so the search was constitutional.[35]

Because of their potential for pervasive use in ordinary law enforcement operations and capacity for revealing far more than the naked eye, drones pose a more serious threat to privacy than do manned flights. There are good reasons to believe that they may implicate Fourth Amendment rights in ways that manned flights do not.

Government use of UAVs equipped with technology that dramatically improves on human vision or captures something humans cannot see (such thermal or x-ray images) should be scrutinized especially closely by the courts. This follows from the Supreme Court's statement in Dow Chemical that using sophisticated technology not generally available to the public may be considered a search under the Fourth Amendment. It is also suggested by the 2001 case *Kyllo v.*

[33] 476 U.S. 207 (1986).
[34] 476 U.S. 227 (1986).
[35] 488 U.S. 445 (1989).

United States, in which the court rejected the use of thermal imaging devices to peer into a suspect's home without a warrant.[36]

Further, the Supreme Court has suggested that the pervasive or continuous use of a surveillance technology may heighten Fourth Amendment concerns. In *United States v. Knotts*, the Supreme Court addressed whether attaching primitive "beeper" tracking technology to a car violated the driver's Fourth Amendment rights.[37] Although it concluded that the use of the beeper in that case did not violate the Fourth Amendment, it held that if "such dragnet type law enforcement practices" as "twenty-four hour surveillance of any citizen of this country" ever arose, it would determine if different constitutional principles would be applicable.

Similarly, in *US v. Jones*, decided last year, a concurrence joined by 5 justices found that GPS tracking of a car implicated an individual's reasonable expectation of privacy and noted "society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period."[38] While this decision may eventually play a role in regulating drone usage, the technology is moving far more rapidly than our jurisprudence, and it is critical that Congress not delay action, especially with a looming 2015 deadline set by the FAA Reauthorization Act.

VI. Recommendations

UAVs can be an extremely powerful surveillance tool, and their use must be subject to strict limitations, as should all government power. Like any tool, UAVs have the potential to be used for good or ill. With implementation of good privacy ground rules, our society can enjoy the benefits of this technology without having to worry about its darker potential. Placing reasonable limitations on law enforcement is by no means a new idea. For example authorities may take a thermal image of someone's home only when they get a warrant. Congress should impose appropriate rules, limits and regulations on UAVs as well in order to preserve the privacy Americans have always expected and enjoyed.

At a minimum, Congress should enact the following core measures to ensure that this happens:

- **Usage restrictions.** UAVs should be subject to strict regulation to ensure that their use does not eviscerate the privacy that Americans have traditionally enjoyed and rightly expect. Innocent Americans should not have to worry that their activities will be scrutinized by drones. To this end, the use of drones should be prohibited for indiscriminate mass surveillance, for example, or for spying based on First Amendment-protected activities. In general, drones should not be deployed except:
    - where there are specific and articulable grounds to believe that the drone will collect evidence relating to a specific instance of criminal wrongdoing or, if the

[36] 533 U.S. 27 (2001).
[37] 460 U.S. 276, 283-84 (1983).
[38] 132 S.Ct. 945.

drone will intrude upon non-public spaces where the government has obtained a warrant based on probable cause; or

- where there is a geographically confined, time-limited emergency situation in which particular individuals' lives are at risk, such as a fire, hostage crisis, or person lost in the wilderness; or

- for reasonable non-law enforcement purposes by non-law enforcement agencies, where privacy will not be substantially affected, such as geological inspections or environmental surveys, and where the surveillance will not be used for secondary law enforcement purposes.

- **Image retention restrictions.** Images of identifiable individuals captured by aerial surveillance technologies should not be retained or shared unless there is reasonable suspicion that the images contain evidence of criminal activity or are relevant to an ongoing investigation or pending criminal trial.

- **Public notice.** The policies and procedures for the use of aerial surveillance technologies should be explicit and written, and should be subject to public review and comment. While it is legitimate for the police to keep the details of particular investigations confidential, policy decisions regarding overall deployment policies—including the privacy trade-offs they may entail—are a public matter that should be openly discussed.

- **Democratic control.** Deployment and policy decisions surrounding UAVs should be democratically decided based on open information—not made on the fly by police departments simply by virtue of federal grants or other autonomous purchasing decisions or departmental policy fiats.

- **Auditing and effectiveness tracking.** Investments in UAVs should only be made with a clear, systematic examination of the costs and benefits involved. And if aerial surveillance technology is deployed, independent audits should be put in place to track the use of UAVs by government, so that citizens and other watchdogs can tell generally how and how often they are being used, whether the original rationale for their deployment is met, whether they represent a worthwhile public expenditure, and whether they are being used for improper or expanded purposes.

- **Ban on weaponization.** Weapons developed on the battlefield in Iraq and Afghanistan have no place inside the U.S. The national consensus on this issue is reflected by the fact that the Heritage Foundation and the International Association of Chiefs of Police join us in supporting sharp limits on weaponized drones.[39]

[39] International Assocation of Cheifs of Police, Aviation Committee, Recommended Guidelines for the use of Unmanned Aircraft. August 2012, see: http://www.theiacp.org/portals/0/pdfs/IACP_UAGuidelines.pdf; Paul Rosenzweig, Steven P. Bucci, Ph.D., Charles "Cully" Stimson and James Jay Carafano, Ph.D., *Drones in U.S.*

State legislatures are already responding to the need to safeguard against drone surveillance. According to the National Conference of State Legislatures, during the current legislative session 42 states have considered 95 different bills and resolutions concerning drones.[40] The vast majority of these bills are focused squarely on privacy issues associated with drone use. Already, Florida[41], Idaho[42], Montana[43], and Virginia[44] have enacted drones legislation; a bill awaits the governor's approval in Tennessee[45]; and legislation has passed one chamber in Illinois[46], Missouri[47], North Dakota[48], and Texas.[49] The amount of progress on drones this legislative session is impressive given that this is the first session in which state legislatures have considered the issue. The astonishing level of activity strongly indicates just how concerned state legislators and their constituents are about ensuring that any drone use respects individuals' privacy rights and expectations

The House Judiciary Committee has before it a very strong and privacy-protective solution to the problems created by drone use: H.R. 637, the Preserving American Privacy Act of 2013. This bipartisan measure, sponsored by Rep. Ted Poe (R-TX) and co-sponsored by numerous other members of the Judiciary Committee, sharply limits the potential misuse of drones by the government while still allowing responsible private sector use of the technology. It requires judicial approval for all drone flights by the government, limits unnecessary information collection, creates a suppression remedy for wrongly collected evidence, bans the weaponization of drones and establishes reporting requirements for drone use. Under the legislation the Attorney General may also withdraw licensing for government drones if they operate outside of allowable parameters.

Drone technology certainly has beneficial uses – for search and rescue missions, firefighting, dangerous police tactical operations – but also poses significant possible harms if left unchecked. Ultimately this powerful new technology should only be used if subject to an equally powerful framework that regulates its use in order to avoid abuse and invasions of privacy.

Airspace: Principles for Governance, The Heritage Foundation, September 20, 2012, see: http://www.heritage.org/research/reports/2012/09/drones-in-us-airspace-principles-for-governance

[40] National Conference of State Legislatures, 2013 Unmanned Aircraft Systems (UAS) Legislation, http://www.ncsl.org/issues-research/justice/unmanned-aerial-vehicles.aspx

[41] http://flsenate.gov/Session/Bill/2013/0092/BillText/er/HTML

[42] http://www.legislature.idaho.gov/legislation/2013/S1134.htm

[43] http://data.opi.mt.gov/bills/2013/billpdf/SB0196.pdf

[44] http://leg1.state.va.us/cgi-bin/legp504.exe?131+ful+CHAP0755

[45] http://wapp.capitol.tn.gov/apps/BillInfo/Default.aspx?BillNumber=SB0796

[46] http://www.ilga.gov/legislation/BillStatus.asp?DocNum=1587&GAID=12&DocTypeID=SB&LegID=72407&SessionID=85&SpecSess=&Session=&GA=98

[47] http://www.house.mo.gov/billsummary.aspx?bill=HB46&year=2013&code=R

[48] http://www.legis.nd.gov/assembly/63-2013/bill-actions/ba1373.html

[49] http://www.capitol.state.tx.us/BillLookup/Actions.aspx?LegSess=83R&Bill=HB912

Mr. SENSENBRENNER. Thank you very much, Mr. Calabrese.

The Chair will recognize Members to ask questions under the 5-minute rule, and the first up will be the Chairman of the full Committee, the gentleman from Virginia, Mr. Goodlatte.

Mr. GOODLATTE. Thank you, Mr. Chairman.

I appreciate your holding this hearing and for your forbearance, I would ask that my opening statement be made a part of the record.

Mr. SENSENBRENNER. Without objection.

[The prepared statement of Mr. Goodlatte follows:]

Prepared Statement of the Honorable Bob Goodlatte, a Representative in Congress from the State of Virginia, and Chairman, Committee on the Judiciary

Thank you, Chairman Sensenbrenner.

Technology in the United States continues to advance at a rapid pace, with profound implications for law enforcement and the privacy of U.S. citizens. From DNA technology to cyber attacks, we here at the Judiciary Committee are fully engaged in examining the effects of new technology on Americans, and on our legal system. Today we are discussing the increased use of unmanned aerial systems—or UAS—for domestic use.

As with much technological innovation, UAS bring both new opportunities and new challenges. These unarmed, unmanned platforms can be flown with cameras and other sensors and transmit information instantaneously to ground crews. In an era of record deficits, UAS could make law enforcement more efficient and cost effective. UAS can also enhance safety for law enforcement officers.

Law enforcement already uses manned helicopters and airplanes equipped with sophisticated technology and sensors. We saw an example of this during the manhunt for the suspects in the Boston Marathon bombing last month. After the surviving suspect was located in a boat in someone's back yard, the police surrounded the area. They did not know the condition of the suspect, who was armed and dangerous. So, they flew a manned helicopter, equipped with a thermal imager, over the boat.

The thermal imager was able to reveal the location and the movements of the suspect. Footage from the camera is now on the Internet, and anyone can see how the sensors clearly revealed the inside of the boat, and the suspect within. One advantage of UAS is that they could employ similar technology to achieve the same results more inexpensively and with less risk to law enforcement officers.

UAS could also be used for a multitude of other applications. For example, the Royal Canadian Mounted Police announced last week that they successfully used a small UAS, equipped with a thermal imager, to locate and treat an injured man whose car had flipped over in a remote, wooded area in near-freezing temperatures.

The Department of Homeland Security (DHS) uses UAS to police the nation's borders to deter unlawful border crossings by unauthorized aliens, criminals, and terrorists, and to detect and interdict the smuggling of weapons, drugs, and other contraband into the country.

Furthermore, DHS, in conjunction with local law enforcement agencies, has been testing UAS capabilities in other situations including detecting radiation, monitoring hostage situations, firefighting, and finding missing persons.

While there are many useful applications for UAS, there are also many reasons to be concerned about the privacy implications of UAS.

Unchecked law enforcement use of UAS could lead to violations of U.S. citizens' Constitutional rights. Overly aggressive bureaucrats behind the controls of UAS could lead to an expansion of the federal government's footprint, harassment and serious violations of privacy.

In fact, to protect against these types of abuses, the Virginia legislature recently passed a 2 year moratorium on the use of UAS by law enforcement, except in certain emergency situations, making Virginia the first state legislature in the country to pass such legislation.

In addition to government use of UAS, there is now a great movement to develop commercial use of UAS, which brings additional opportunities and challenges.

For example, companies are promoting use of UAS for sports photography, to film amateur climbers and surfers as they compete. And that is just one example—the potential for commercial use of UAS technology is virtually limitless.

However, this commercial development also brings forth new privacy questions. Can a private individual use a UAS to check whether a neighbor is building his fence in the right spot? Should a home owner's association be able to use a UAS to patrol a group of homes? Last month, the animal rights group, PETA, announced plans to acquire a UAS in order "to spy on hunters and catch them in the act as they terrorize animals and break game laws." Clearly, there are a host of privacy implications that we should consider as unmanned air activity becomes more prevalent.

Computer systems, combined with aviation, will make it possible for people, businesses and governments to use aviation on a scale never seen before. Many people believe that our legal system will adapt to this new technology the way it has in the past. Others believe that special measures should be taken in advance of UAS development to ensure that Americans' rights are protected.

The Judiciary Committee's challenge is to make sure our nation's legal structures continue to protect Americans' privacy, while allowing technology to flourish and improve our safety, security, and economic progress.

I thank Subcommittee Chairman Sensenbrenner for holding this hearing and I look forward to hearing the witnesses' testimony on this important subject.

Mr. GOODLATTE. Thank you. Is it Villasenor? I am close?

Mr. VILLASENOR. Close enough.

Mr. GOODLATTE. Which do you believe are in the best position to regulate UAS on privacy grounds, courts, Congress, or the States?

Mr. VILLASENOR. Well, in terms of actually regulating—is the question specific to privacy or more——

Mr. GOODLATTE. Primarily.

Mr. VILLASENOR. For privacy, I think with respect to law enforcement use, I am on record stating and I do believe that the Fourth Amendment is going to provide quite a bit more protection than is generally recognized, and in that case, of course, it would be through the courts.

With respect to private party use, which has not been the focus of as much attention as public use, it is of course at the State level that you have statutes against invasion of privacy, stalking, harassment, and the like, and so I think that there is a role at the State level to ensure that those statutes properly anticipate privacy abuses that could occur with unmanned aircraft.

Mr. GOODLATTE. Thank you.

Mr. McNeal, should Congress regulate the future commercial use of unmanned aircraft or should, as Mr. Villasenor suggested, that could be left to the States?

Mr. MCNEAL. I am not sure. So with regard to the privacy issues, I am not sure that you can get around privacy without Congress doing it. So let me sort of rephrase that. For commercial uses, if we are concerned about privacy, it seems that Congress is the most appropriate body to legislate in a way that we would have equal laws across the board, but I am in sort of the same camp as Mr. Villasenor that if we think that the Fourth Amendment protections that currently exist are sufficient, we could copy those over for commercial purposes and adopt those as our statutes for privacy protections.

The problem with commercial uses is that we have got a big body of law on privacy with regard to what law enforcement does but far fewer rules with regard to what private parties and our commercial parties might do, and so this is one of the things that I think people get really concerned about, commercial uses being just my neighbor flying around doing video for photography or for his

YouTube page or for real estate purposes that can then start to look a lot like snooping or Peeping Tom types of things. Some of that is covered by State laws, but when you look at the line of cases where people have been able to successfully sue when they feel like their privacy rights are being violated, you do not see a lot of success. It is a high bar for people to overcome, and so there might be some room there for Congress to regulate.

But I do not think that is the—when you look at the big time commercial uses, we are thinking about flight of unmanned systems for like FedEx and what not, privacy isn't really the big issue that is driving our concerns there; it is more safety concerns.

Mr. GOODLATTE. Thank you.

Mr. Calabrese, I take it from your warrant-based approach to use of UAS by governmental entities, you do have an exception for an emergency situation. So, for example, if the Tsarnaev brothers in Boston had been somehow detected by a drone, that would still be evidence admissible in court, under your circumstances, if they were following them down the street and they were either impeded from placing their explosives or were not impeded but that evidence was available to show that they were the perpetrators of that crime?

Mr. CALABRESE. Yes, that is correct. As Mr. Poe's legislation indicates, there is a strong emergency exception that allows in the cases of danger to life or limb the use of drones in order to provide—you know, you have to play out the scenario a little more in terms of, you know, where they are in the investigation, but, yes, there is clearly a very strong emergency exception as well as an ability to act before a warrant is issued.

Mr. GOODLATTE. And Mr. Maclin, can you explain how UAS may affect police discretion and whether police discretion is something that should be limited by statute?

Mr. MACLIN. I think it should certainly be limited by statute. When I talk about police discretion, I am talking about the ability of law enforcement to simply fly a drone over, examine, surveil without any probable cause or reasonable suspicion, and certainly if you do not have either one of those two things, you can not get a warrant.

I would take slight objection with the notion that if we are going to require warrants, we should allow, possibly allow warrants based on reasonable suspicion. I mean, the Court, I think, albeit other than the administrative search context, has said when you need a warrant, it has to be based on probable cause.

Mr. GOODLATTE. Thank you, Mr. Chairman.

Mr. SENSENBRENNER. The gentleman's time has expired.

The gentleman from Virginia, Mr. Scott.

Mr. SCOTT. Thank you, Mr. Chairman.

Mr. Calabrese, can you say a word about how the technology has complicated this issue in terms of the difference between one photograph all the way to tracking someone even in public for long periods of time, what the expectation is?

Mr. CALABRESE. Certainly, Mr. Scott, thank you. It is a great question.

To be clear, it is actually not just drones, right? I mean, if you think about the technologies at issue here, you can imagine track-

ing with the drone, coupled with tracking using a cell phone, which I know is something this Committee has considered recently, plus tracking with a license plate scanner, and all of these things could be used to couple to really provide mass surveillance all the time. But in terms specifically of drones, they have become smaller. They have become cheaper. The surveillance technologies on them can penetrate more deeply at night, you know, with smaller and greater cameras.

A Nova special recently indicated one camera, called the ARGUS, could cover multiple square miles and do detailed surveillance literally of an entire city. Imagine that technology coupled with surveillance. You know, it changes the way people think of as public and what a public space is. It really merits further regulation by Congress.

Mr. SCOTT. You mentioned the problem with weapons. Are weapons ever appropriate with drones?

Mr. CALABRESE. I think we need to explore the question of weaponization carefully. I mean, by and large, the answer is no; weapons should not be used because a drone is not in the same kind of danger as a police officer is. Clearly, a police officer has got to be able to defend himself. We all understand that or take appropriate action to apprehend someone. A drone is not going to need to defend itself. It is not going to need to apprehend anyone. And a drone operator may not have the same judgment or expertise peering through a little camera as a police officer does on the ground. All of that argues against weaponization. There may be some limited exceptions for training or other purposes, but by and large, weapons do not belong on drones.

Mr. SCOTT. You mentioned the possibility of discrimination. Can you say a word about how you choose which areas are under surveillance?

Mr. CALABRESE. Well, I think that is an outstanding question. I mean, it goes to a couple of important issues. One is having the community be involved. You should know if there is surveillance. The community should be able to decide if they think getting a drone is an appropriate tool and how it should be used.

Also, just in the question of discrimination generally, we have seen in monitoring video cameras that video surveillance is frequently a very boring task for an operator. It is dull, you know, minds tend to wander. They tend to follow around—honestly, the research shows they tend to follow around pretty girls, and then they tend to follow their biases and look for particular, you know, racial minorities that they may think are more likely to commit crimes. We think it is very probable that that could happen with a drone as well.

Mr. SCOTT. You mean in terms of selecting the areas to be under surveillance?

Mr. CALABRESE. I think not just the areas under surveillance but the individuals who they might choose to follow. If you had mass surveillance over a particular area, they may be picking out particular individuals and deciding to follow them around and see if they are going to commit crimes.

Mr. SCOTT. If you have a legal exception for surveillance in a recording, what happens when you see something that you did not

have probable cause to suspect but you noticed because it was under surveillance?

Mr. CALABRESE. Well, I think that that is going to be relatively uncommon. We do have an exception for——

Mr. SCOTT. If you have got an entire traffic area that is doing a mile, and you are doing traffic surveillance, and you say that is okay, and you see some drug deal over on the side, does that, do you get to use that?

Mr. CALABRESE. Well, I think what we would say, first of all, is we would hope we would not have mass surveillance like that, that we would not have cameras up in the sky all the time. So, you know, we would assume that surveillance would largely be—by drone—would largely be directed and targeted, and so if individual, you know, if individual acts were already being monitored by law enforcement, we would expect that they would likely come under an existing reasonable suspicion standard if the investigation was done, for example, in public because we would already have a court order that would say that it is okay to do drone use in public at these particular times under a reasonable suspicion.

Mr. SCOTT. But if you have got all this stuff recorded, could there be a limitation on what you can do with it after you have got it?

Mr. CALABRESE. I think that there has to be, yes. I think that we do not want people to be recorded all the time. We do not want to feel like those drones are constantly monitoring them. And we want people to know that they are safe, but not just in private but also in public to live their lives without worrying that what they do is going to end up on YouTube.

Mr. SENSENBRENNER. The gentleman's time has expired.

Under the procedures that have been announced by the Chairman of the Committee, full Committee Members who are not Members of a Subcommittee are entitled to sit on the dais but are not entitled to ask questions, unless a Member yields them time to do so.

And under that procedure, the Chair yields his time, his 5 minutes to the gentleman from Texas, Mr. Poe.

Mr. POE. Thank you, Mr. Chairman.

I appreciate you yielding, and all four of you being here. I guess the crowning decision, concept is the Supreme Court's dicta, for lack of a better phrase, of expectation of privacy down the road is going to be not expanded but made smaller. I think that is what the Court, members of the Court to me are saying, which concerns me. So it seems to me that Congress in the area of drones needs to set a standard rather than let the courts down the road set a standard.

I am from Houston, and our local sheriff of the county, Sheriff Adrian Garcia, third largest county in the country, he will not use any kind of drones because he does not know what the law is going to be. And he does not want to wait for the Supreme Court to rule 10 years from now on a search, throw out a case that he has arrested some bad guy and put him in jail, so he is not using drones, so he is waiting for somebody to give him and other law enforcement agencies some direction on the use of drones.

It seems to be two issues—law enforcement use and private use—and what is the expectation of privacy in those areas, and should we do anything about it or just wait?

Mr. Calabrese, let me ask you, there has been comments made that the Court should make these decisions about the Fourth Amendment, which courts have been doing, applying what is lawful under the Fourth Amendment, what is not lawful under the Fourth Amendment. Should the courts be the answer for solving this issue of drones and the Fourth Amendment?

Mr. CALABRESE. Well, I think that your legislation does a very good job of creating a careful balance, something that Congress is particularly good at and the courts are not always particularly good at. When we think about how we would want to use a drone, it is clear that most of the uses—finding a missing person, fighting a forest fire—are not uses that particularly implicate the Fourth Amendment. And your legislation is very careful to carve those out, and I think by creating clarity, you allow the use of drones for all of these good purposes, including commercial purposes, where people do not have to worry that that drone in the sky is spying on them, while—so you allow for the growth of the industry while still protecting people's privacy in a reasonable way.

So, yes, I think Congress absolutely has a role, and I think it is a very strong role and one that you are well suited to perform.

Mr. POE. What about the FAA? Right now, the FAA decides who gets a permit for a drone. They make that decision. The President has weighed in on that, told the FAA to be sensitive to privacy concerns when giving new permits. What about the FAA making that decision?

Mr. CALABRESE. I think the FAA does have a role, clearly, in some of the things, like deciding what is going to happen with information once it is collected, providing notice of what particular drones are being flown and how, but I think Congress has the central role in regulating itself, regulating the government.

So, you know, you have got to be, Congress has got to be the one to decide how the police, how the Fourth Amendment should be interpreted, because, of course, Congress has a role in interpreting the Constitution as well. You are constitutional officers. So the FAA can certainly perform an expert function. I think that Congress' role has got to remain central.

Mr. POE. Since the issue of drones has come up, there are a lot in the industry, the drone industry and other industries saying, well, if we are going to talk about the Fourth Amendment, let's expand it and revisit the whole concept of the Fourth Amendment and not just with drones but with all new technologies. What do you think about that?

Mr. CALABRESE. Well, I certainly believe in expanding the Fourth Amendment, there is no question about that. I know you do as well. I think the Committee is doing that right now. I mean, you are not just considering drones. You are also considering surveillance of cell phones. The Committee has had another hearing on electronic communications privacy. So you really are revisiting the entire issue, and I think you are doing it in a very intelligent and very deliberative manner, so, you know this is a piece of that.

Mr. POE. So, once again, on the other technologies and some yet to be invented, should Congress set the standard perimeters on law enforcement civilian use, or should we just, again, wait for the Supreme Court to make those ultimate decisions?

Mr. CALABRESE. Well, I think that in the 21st century, as we have gotten new technologies, we have got to make sure that our values come with us—right—that we do not lose those constitutional values as we move to new technologies. You, of course, are perfectly suited to do that.

Mr. POE. Thank you, Mr. Chairman.

Mr. SENSENBRENNER. The gentleman's time has expired.

The gentleman from Michigan, Mr. Conyers.

Mr. CONYERS. Thank you very much.

Could I ask, Mr. Villasenor, Professor McNeal, and Professor Maclin, have you heard about the Poe legislation 637, Preserving American Privacy Act, and are you able to comment on it at all? Please do.

Mr. VILLASENOR. Yes. I am certainly, first of all, very appreciative of any attention that Congress is giving to this very important issue.

One of the concerns I have with overly broad warrant requirements is that the problems that could arise. I certainly agree that we should not countenance government fishing expeditions using unmanned aircraft or any other technology, but, for example, suppose that a law enforcement unmanned aircraft is monitoring a traffic intersection after an accident, and on the sidewalk next to the intersection, a terrible assault takes place, and suppose that the video evidence from the unmanned aircraft is the only evidence that clearly identifies the perpetrator of that assault. I think it would defy reason for us all to say to the victim, well, we know who the perpetrator is, but we are going to let the perpetrator go because we did not have a warrant, and there was some legislation that said we can not use it. So I think we need to be cognizant of the potentially bad, unintended consequences of what sounds at first blush like something which is only going to be good.

Mr. CONYERS. Uh-huh.

Mr. McNeal?

Mr. MCNEAL. So Mr. Villasenor highlighted one of the points that I make in my written testimony where I provide a few examples where the legislation, the current Preserving American Privacy Act and the one of 2012 as well, where they both create a circumstance where we might be suppressing inadvertently discovered information, so we are out doing a search-and-rescue mission, for example, in public parks or something, and along the way while looking for that lost hiker you come across evidence of a crime, and now that evidence can not be used.

Some privacy advocates want a ban on the use of this secondary evidence in all circumstances, and I understand the impulse. The idea is that if you say that you are using it for search and rescue purposes and then you use the evidence for crime collection purposes, it presents this circumstance where we might have the general surveillance that we are all somewhat concerned with. But I think there has to be some way in the legislation that we craft an exception for that.

Mr. CONYERS. Uh-huh.

Thank you.

Professor Maclin?

Mr. MACLIN. Mr. Conyers, I am not in a position to comment on it because I have not studied it, so I would not want to express an opinion.

Mr. CONYERS. Of course.

Let me turn now to the very disturbing consideration of this general subject. You know, this is a prime example of technology overtaking established law, and I think we are going to have to go beyond the Fourth Amendment. There are going to have to be a body of statutes that go into some of this detail. It is not all about privacy, but privacy is, of course, always a continuing exception.

Do any of you want to recommend to this Subcommittee, which might be the ones that take on this responsibility, any courses of action that we might take to examine all of this? As has been remarked, this goes beyond drones, because there could be new technology coming out to further complicate it.

Mr. MCNEAL. Congressman, I think you hit the nail on the head when you said this goes beyond drones, and I will just give you an example. In New York City, NYPD has a helicopter; they call it 23, I think, for the 23 NYPD officers killed on 9/11. It has a camera that can observe activity 2 miles away. It is more—it can see the detail on people's faces, read their name tag if they have a name tag on their shirt or something from up to 2 miles away. So this isn't a drone-specific thing. It is really an advancement of technology thing.

And so I think that the approach if Congress wanted to legislate on this would be to look at the issue of surveillance, define what surveillance is, and I put some definitions in my written testimony, and then create some lines based on the duration of surveillance that would—maybe we allow officers at their own discretion to observe individuals from any platform for a period of time, let's say 2 hours in a 7-day period, but then once we get to the end of that 7-day period, maybe they need reasonable suspicion to continue the surveillance for a 48-hour period of time, and then anything longer than that might require a warrant.

And the times that I have thrown out are just my sort of best guess at what might be good privacy protection. Some might put it lower, at 20 minutes; some might put it much higher. But by doing that, we are treating all technology the same, so a camera trained on someone's home persistently day after day will be treated the same as if it is a camera on a drone or someone, you know, standing on a rooftop using the camera. We are treating that technology and the invasion, the persistent surveillance the same.

Mr. SENSENBRENNER. The gentleman's time has expired.

Mr. CONYERS. Thank you.

Mr. SENSENBRENNER. The gentleman from Arizona, Mr. Franks.

Mr. FRANKS. Well, thank you, Mr. Chairman.

Mr. Chairman, I have the privilege of being on the Armed Services Committee, where we quite often have to struggle with issues of unmanned aerial vehicles because more and more, the technology is allowing us almost to pilot from the ground in many different circumstances, and this is also true of missile technology. It

is guided missiles and piloted-on-the-ground aerial vehicles. This technology is beginning to emerge, and it does present some pretty significant challenges. You know, we like to say never send a man to do a missile's job. But the reality is that the technology is becoming more and more difficult, and it raises constitutional issues, as I think the previous gentleman very astutely articulated.

So I guess my first question is how to apply the time-honored constitutional principles essentially according to original intent in a way that is reasonable and appropriate. So let me give this example, and I will ask Mr. Maclin if he would respond to it.

Just recently, the City of Boston endured, obviously, a terrible terrorist attack, and the street cameras recording the scene from every angle were key to law enforcement in the hunt for the terrorists. Then the police used thermal images from helicopters to locate the armed suspect as he hid from the police. Now, any of these images could have been derived from unmanned aircraft. So, constitutionally, Mr. Maclin, and this is not a trick question. I thought Mr. Conyers' point was very spot on. Does it matter to you constitutionally whether those street images in that particular case came from a street camera or from an unmanned aerial surveillance?

Mr. MACLIN. Constitutionally speaking, no, I do not think it matters. What matters is who is responsible for those cameras.

Now, I may be mistaken, but I believe one of the cameras was from Lord & Taylor, the Lord & Taylor store, but let's assume that they were put up by the City of Boston. No, constitutionally speaking, it does not matter. It does not matter.

Mr. FRANKS. Well, then let me direct a question to Mr. Calabrese, am I saying that properly, sir?

Mr. CALABRESE. Calabrese.

Mr. FRANKS. Okay. You stated in your testimony that the UAS would be acceptable to you for, quote, reasonable nonlaw enforcement purposes by nonlaw enforcement agencies, where privacy will not be substantially affected, where the surveillance will not be used for secondary law enforcement purposes, and to the previous gentleman's, Mr. Maclin's comment, so it is your position, if I am—that the Fourth Amendment applies only to law enforcement agencies for law enforcement purposes?

Mr. CALABRESE. To the government generally. I am sorry. As opposed to—the Fourth Amendment applies to government generally.

Mr. FRANKS. But, I mean, for reasonable nonlaw enforcement purposes, then that would no longer apply?

Mr. CALABRESE. That is correct—well, I would not say that the Fourth Amendment does not apply. I would say that I think the biggest—because the Fourth Amendment is always going to apply, no matter what I say.

Mr. FRANKS. But I am reading what you said.

Mr. CALABRESE. Right, yeah, I understand. I am sorry. What we believe the biggest danger is, is that the law enforcement will use drones in an invasive manner, so—but we still want to create the ability of government to use drones in a non-invasive manner. So, for example, a firefighter is obviously a government agent. They should still be able to use a drone to investigate a fire, and we do not want to keep that from happening. Whether or not the Fourth

Amendment applies there, we certainly—which it does, but of course it's not a search for law enforcement purposes.

Mr. FRANKS. It seems to be a pretty challenging parse there if one tries to apply the Fourth Amendment to nonlaw enforcement agencies different than law enforcement agencies when the effect is the same, and I know that is one of the issues we will grapple with a very long time.

Would anyone else on the panel like to address either of those questions?

Mr. MCNEAL. Congressman, I just want to direct you to page 6 of my testimony, where I try and thread this needle which is by—I think the Fourth Amendment issue, I think what we need to focus on is the legislation that will address this policy concern that you have brought up, and that requires some definitions of what a "search" is, that might go beyond the Fourth Amendment. And I think the big thing that we have been bandying about here is the distinction between a general search, parking a blimp over a town, versus a targeted search against a particular individual. And I think that we will want to address those two different types of searches in different ways, because New York City, for example, you are subject to a general search at all points in time because of the cameras, and that is different than the targeted search.

Mr. FRANKS. Thank you.

Mr. SENSENBRENNER. The time of the gentleman has expired.

The gentlewoman from California, Ms. Bass.

Ms. BASS. Thank you very much, Mr. Chair.

I just wanted to ask some questions of the panel in general about what you believe laws and restrictions should be placed on drone use by private citizens to conduct aerial surveillance. It is my understanding that if a private citizen wants to use a drone they have to get FAA approval, but beyond that, I wanted to know if you had suggestions.

Mr. VILLASENOR. Well, maybe I can at least partially try to respond to that question. So, first of all, currently commercial use in the United States of unmanned aircraft is not yet permitted. The FAA is in the process under the FAA Modernization and Reauthorization Act of 2012, under the process of drafting those regulations. So—but the question is still——

Ms. BASS. That is to come, right?

Mr. VILLASENOR. That is to come, and by—and according to the schedule laid out in that legislation by late 2015 those regulations would be complete. So the question is an eminently reasonable one. There is a very significant body of common law as well as in most States statutes, both civil and criminal, related to invasion of privacy. And those statutes are usually tied to this concept of reasonable expectation of privacy. So if a private party used an unmanned aircraft in a manner that does invade privacy, it is actionable under usually multiple grounds, and so I am confident that there are existing protections, although there is also a good reason to sort of look at those statutes to make sure things like harassment and stalking statutes also cover potential misuses by unmanned aircraft.

Ms. BASS. And in my area, there is a concern over the paparazzi, which has gone to some extreme lengths to invade people's privacy.

Mr. VILLASENOR. I am certainly not going to defend the privacy invasions that the paparazzi commit. I think we all know that they happen, and that is not a technology problem; that is a paparazzi problem.

Ms. BASS. Any other comments from anyone?

Mr. CALABRESE. I would just say that the private use does raise serious First Amendment concerns. We think there is a lot of existing law around invasions of privacy, at both the State level but also to some extent at the Federal level. It is both intentional invasions of privacy under tort law; it is Peeping Tom laws.

Ms. BASS. Right.

Mr. CALABRESE. It is trespass laws, and of course, there is California-specific paparazzi law as well. So I think that, unlike the Fourth Amendment government context, where we spent a lot of time talking, where it is largely unregulated and I think the Committee needs to focus, I think here there is a fair amount of existing law, and it may be appropriate to see how that plays out before we do a lot of legislating in the private use area.

Ms. BASS. Anyone else?

You know, when I learn about some of the drones being so small, like the size of a bird or whatever, how do you see in the future that being regulated? I mean, what is to stop an individual from just getting that without FAA approval?

Mr. VILLASENOR. Well, I think there is already a hobbyist exception for unmanned aircraft, model aircraft as defined in the legislation, and I think, frankly, it as very important to provide exceptions for hobbyists and so that, you know, a parent who goes and flies a model aircraft at a flying field with his or her child does not need to get FAA approval before doing so. So, at the very small end, there is certainly going to be some flexibility in terms of acquiring these platforms. But, again, it is the use where we draw the line, and to the extent that these platforms might be used in an invasive or unlawful, otherwise unlawful manner, that is where we would then address that behavior.

Ms. BASS. Okay, thank you.

Yield back my time.

Mr. SENSENBRENNER. The gentleman from Utah, Mr. Chaffetz.

Mr. CHAFFETZ. Thank you, Mr. Chairman.

I thank the panel for being here. I think this is an important topic because obviously the rapid expansion of technology—technology is great as long, as it is used in the right and proper way.

I want to talk a little bit about the Jones case if we could. My apologies, I walked in a little bit late. I was interested by Justice Sotomayor's opinion on this. Obviously a 9-0 ruling is fairly conclusive, but it does beg the question of what other areas should this be applicable to. From your perspective and experience, our current Justice Department and the implementation by the FBI and others, have they taken this Jones case and implemented it the way you see it should be implemented, or are they missing something here? What should the Justice Department and the Federal Government be doing with that Jones case? I will start with Mr. Calabrese if we could.

Mr. CALABRESE. Well, obviously, the Jones case deals with location tracking. And in the ACLU's view, the government has been

deficient in applying Jones. We believe that a majority of the court, no matter how you read it, said that systematic tracking of individuals over time is an invasion, it implicates the Fourth Amendment, and is a search. Given that rationale, we believe that all manner of tracking currently undertaken by the government, whether that is cell phone tracking, whether that is tracking with a GPS device by a car, implicates the Fourth Amendment and should be done with a warrant.

I think it is a very interesting question as to whether that same rationale should be expanded to drones. Clearly, drones could be used to track an individual for long durations in a very detailed manner. Perhaps *U.S. v. Jones* will also come to regulate how drones are used as well.

Mr. CHAFFETZ. Does anybody else care to comment?

Yes.

Mr. MACLIN. Well, I would just say this about Jones. I think the story on Jones and the scope of Jones is unwritten. Certainly, Justice Sotomayor and Justice Alito's opinion talk about electronic monitoring. Justice Scalia's opinion is careful not to rely on the Katz test and not to rely on any concerns about electronic monitoring. His opinion was solely about the physical intrusion and the purpose for the governmental conduct.

And I think if you read the most recent ruling from the court in this area, *Florida v. Jardines*, with, again, Justice Scalia writing the majority opinion, you will again see the focus of Scalia's concern on the physical intrusion in that case.

So I think with respect to Jones, I am not——

Mr. CHAFFETZ. What is your opinion about it? It seems to be shortsighted to think that just the physical intrusion——

Mr. MACLIN. I agree with that. My own personal opinion is that the concerns with the monitoring are more important because we are already at a time where government does not need a physical intrusion.

Mr. CHAFFETZ. No. You can triangulate things electronically without actually physically attaching something. And that is my concern, Mr. Chairman.

I have a geolocation bill that we have done with Senator Wyden in a bipartisan way. You have been very supportive of this. I do not think it is just merely the physical intrusion of attaching a GPS device and technology over the course of time.

And let me get the other two gentlemen's opinion of this. I think one of the things we need to look at, Mr. Chairman, is air space. If you have private property, and you may have something very small, you may have something large, say a 5-acre parcel of land, I do think there is a reasonable expectation of privacy that isn't just limited by walking down the street and okay, you put up a fence. But I think the air space is something in general that we should look at. But maybe if you could talk to that and the Jones. I want to leave time for our last—the other person as well.

Mr. MCNEAL. Congressman, what you have articulated as the reasonable expectation of privacy that I think you expect and that your constituents expect is something that is broader than the Supreme Court has articulated. So going back to the Oliver case and the other aerial surveillance cases, going to Katz, what we know-

ingly expose to the public isn't a matter of Fourth Amendment concern.

And so, if you want to protect the air space over someone's yard and whatnot, it will require legislation because the court does not seem prepared to identify that yet.

Mr. CHAFFETZ. My time is almost up.

Mr. VILLASENOR. I actually read Jones more optimistically than perhaps many with respect to prohibiting long-term extended surveillance. Majority of the Justices—Justice Alito was joined by three Justices in concurrence—that makes four. And then Justice Sotomayor agreed with Justice Alito's statement that long-term tracking itself, even without the actual trespass associated with the attachment of the device, violated a reasonable expectation of privacy. And even Justice Scalia in his majority opinion said it may be unconstitutional. So I am actually quite encouraged that the Supreme Court would find that unconstitutional.

Mr. CHAFFETZ. I think that is the right direction.

Mr. SENSENBRENNER. The gentleman's time has expired.

The gentleman from Louisiana, Mr. Richmond.

Mr. RICHMOND. Thank you, Mr. Chairman.

Mr. Maclin, let me start with you. Because a lot of conversation and a lot of what goes on depends on reasonable expectation of privacy, as we discussed another bill.

Do you think it is ever going to get to a point where we have to say what a reasonable expectation of privacy is, period? Because the more and more that things evolve, the more and more I think that I have any expectation of privacy. And at some point, will someone say your expectation of privacy is just unreasonable?

Mr. MACLIN. Of course. I agree with you. I think this Committee, and Congress in general, can use their powers under section 5 of the 14th Amendment to enforce the Fourth Amendment and say, yes, a reasonable expectation of privacy includes the following.

Mr. RICHMOND. Mr. Calabrese, you talked earlier about the fact that we have tort laws and other things for

nongovernmental actors. As I watched the news this morning, there is an incident in New York where a guy took pictures of people in the adjacent building; did not capture their face but caught very intimate moments. Those pictures are now in a gallery selling for $8,000. The subjects of them were very upset. And the lawyers that talked about it said there is no recourse for them. I guess it is that sort of thing that concerns me in terms of if we get to drones, how do we reconcile that?

Mr. CALABRESE. They are very difficult questions. But they are very difficult questions both because they are potential real invasions but also because of the powerful need to protect the First Amendment. I think that Peeping Tom laws would deal with a drone right up on someone's window. Across the building but with a powerful camera, it is a harder question.

The First Amendment protects our right to gather information for really important reasons: regulating how government operates, giving people the ability to talk about what is going on in their lives, share information, the obvious need to protect the press. We have seen that this week.

So we are going to have to balance those. We do think that there is a lot of law in this area. So I think we are going to have to tread carefully in regard to the First Amendment. And I do think there are more existing protocols and controls around First Amendment-related activity for private use than there are for the Fourth Amendment space in government use.

Mr. RICHMOND. We talked a little bit about the drones and the fact that they will have the capability of license plate readers. But my police chief is excited about the fact that he is putting license plate readers on every stoplight. At what point do you think we get to—or do you think police now would need some authorization to record and store the data from license plate readers, for example, if you have a spree of burglaries, that they can go back and see if there is any car that went through the red lights close to any of those homes. Can they just store that information?

Mr. CALABRESE. I believe that there is a reason that we have license plate readers. I believe, for example, looking for stolen cars is a perfectly appropriate reason to have a license plate reader. I believe that information should be destroyed at the end of the shift, once the purpose that you gathered it for is no longer operative. And I do believe that that is because if we do not do that, we are going to live in a society where we have mass surveillance. We live in a world of records now. Everything we do generates a record. So if we are going to start saying, Let's keep it just in case, our entire lives are going to be out there to be investigated anytime someone wants to poke through those records.

Mr. RICHMOND. And that is what I was worried about, the "just in case."

Did anyone else want to comment on that?

Mr. VILLASENOR. I guess I will just add that while I fully am sympathetic to these concerns, there is a gray area here. It is very difficult. If, as Mr. Calabrese suggested, all of these records were destroyed at the end of a shift, suppose there was a kidnapping or missing persons report that was not reported for 48 hours after it happened. Again, I do not think anyone would deem it a positive thing if we had intentionally destroyed information that might have led us to solve that more quickly. So I do not claim to have any perfect answer, but those are hard questions.

Mr. RICHMOND. Thank you, Mr. Chairman, and I yield back. I see my time has expired.

Mr. SENSENBRENNER. The gentleman from South Carolina, Mr. Gowdy.

Mr. GOWDY. Thank you, Mr. Chairman.

Gentlemen, I think Justice Alito said this, new technology made provide increased convenience or security at the expense of privacy, and many people may find the tradeoff worthwhile.

How will we know whether people find the tradeoff

worthwhile and who gets to make that decision?

Mr. MACLIN. Can I comment on that, Congressman?

Mr. GOWDY. Sure.

Mr. MACLIN. That is a catchy statement. The problem is with an individual——

Mr. GOWDY. Well, it is not my statement.

Mr. MACLIN. I know it is not yours. I understand that. My concern with that statement is that because society or members of society would be willing to make that tradeoff, the individual will be the one who suffers the harm. And I think, again, that is the job—I assume that is one of the reasons why this Committee is holding these hearings, is get a view. And I agree with Congressman Richmond that this body should make a determination of that because if it is just a matter of what society would prefer for what tradeoffs society would be willing to make, individuals are going to be the ones who suffer.

Mr. GOWDY. So if I remember common law correctly, the Bill of Rights kind of sets the minimum. And if States or this entity, perhaps, wanted to have a more arduous view of one of the amendments, like the Fourth Amendment, we could do so, right?

Mr. MACLIN. Well, I would just caution, because the jurisprudence under *City of Boerne v. Flores*, as I am sure Members of this Committee understand, does not lend itself to Congress going beyond what the Supreme Court has done. That said, however——

Mr. GOWDY. I thought the Constitution allowed Congress to in some instances set the jurisdiction of the courts.

Mr. MACLIN. Allowed to set the jurisdiction of the court. But under section 5, the court has been somewhat restrictive. The City of Boerne is the main case, and there have been recent precedence since then, and it is go be interesting to see what they do with the Shelby County case, but the court has invalidated several congressional statutes where Congress has imposed on States restrictions that the court has found constitutional.

Mr. GOWDY. How does the expenditure of manpower or womanpower impact a Fourth Amendment analysis? I can see an analysis where if you had to invest detectives or line officers in surveillance, that is one analysis. And it would be a different analysis than just having a computer doing it. Am I dreaming up that the investiture of resources would be part of—I mean Jason, my friend, love him to death, he has got a bill dealing with GPS tracking. And part of the analysis, I think, is that at least when you are having a person doing it, you are investing time, you are investing resources. That is a different analysis than just having some device do it. So how does that play into it?

Mr. MACLIN. Well, I know of no Supreme Court case in which the court has said how much resources or the degree of resources invested makes any difference in the Fourth Amendment question.

Mr. GOWDY. I think there is, but you guys are the experts.

The gentleman beside you is shaking his head, probably to agree with you and not with me, but you can go right ahead.

Mr. MCNEAL. I think I agree with you, Congressman. I think the appropriate place for us to calibrate these expectations is in the legislature, rather than letting judges write things up. This body here is in the best position to know what your constituents expect with regard to privacy. And if we want to control the types of surveillance, be it GPS or geolocation data or whatnot, then Congress can pass legislation to require a warrant before getting that, rather than allowing it to be obtained through a subpoena. I think that is completely appropriate.

Mr. GOWDY. Do all of you agree that technology can impact whether or not a search is considered reasonable?

Mr. VILLASENOR. I think I can at least partially answer that. The Supreme Court has ruled that if the government uses a large team of agents to literally follow somebody around, that that is not a violation of the Fourth Amendment. Whereas, the Supreme Court, in the Jones majority, is on record leaving open the question of performing that same tracking with technology may be a violation of the Fourth Amendment.

Of course, as I mentioned a moment ago, Justice Alito and four other Justices think that it is a violation of the Fourth Amendment.

Mr. GOWDY. Do you agree—and I know I am almost out of time—that technology impacts our reasonable expectation of privacy and that it is a scale that changes from culture or generation to generation?

Mr. VILLASENOR. I think to some extent we are all far more comfortable with the concept of photography than people were in the late 1800's when it first became possible to capture an irrefutably accurate image of somebody at will. So technology does impact our views of privacy, but it does not mean that we do not have privacy.

Mr. MACLIN. I would agree with that, Congressman. Technology does affect our Fourth Amendment.

Mr. GOWDY. Well, I am out of time.

Mr. SENSENBRENNER. The gentleman's time has expired.

The gentlewoman from California, Ms. Chu.

Ms. CHU. Thank you, Mr. Chair. I would like to ask Mr. Calabrese about the issue of the storage of data and its implications for privacy. We know that local police departments are applying to obtain permits from the FAA to use drones for law enforcement purposes. And I understand that there is some potential that a large amount of data could be collected by drones and stored for a very long period of time. I am concerned that limitless data collection can pose a threat to Americans' privacy. Can you tell us what types of data these drones can collect and if those law enforcement agencies who acquire drones have data minimization policies in place?

Mr. CALABRESE. Those are all incredibly good questions, Congresswoman, that do not necessarily have clear answers at this point. Let me try to sketch a view of the parameters out for you. I think that absolutely the widespread collection of detailed information, say HD camera level video, can create huge privacy implications. It really changes way we consider public space. We do not consider ourselves to be recorded when we are in public. We may be in public but not preserved over time. We can also apply powerful new technologies like face recognition to that detailed video. We can use it to zoom in, for example, or examine particular things that we might not have noticed at the time.

In terms of data retention policies, we think those are best practices. We think every police department should limit the amount of collection for particular purposes and discard it after it no longer needs it for those purposes. Whether that is happening now, I think it is tough to say on a local level the particular data collec-

tion practices. We certainly hope it will be something the FAA requires and that all local law enforcement does.

Ms. CHU. Do you think we should require that agencies who use drones have some sort of data minimization policy in place, and what kind of policy would be best in terms of considering civilian drone usage?

Mr. CALABRESE. Yes, I do believe the data minimization policy is vital. I would say that it is bounded by the other reasons for collection. You put a drone up for a particular reason. Once that reason is expired, you have examined the person, searched the person, or followed the person that you are looking into, the case is over, you no longer need it, discard the data. If you do not do any mass surveillance, then you will not have to worry about keeping data for long periods of time.

Ms. CHU. We have to update many of our other Federal laws that deal with electronic communications, but what can we learn from our experiences in dealing with other technologies when it comes to protecting individual privacy?

Mr. CALABRESE. Well, I think that we have powerful frameworks in place now. Certainly, the Privacy Act in itself has all the principles that we believe would apply here. They have some Privacy Act exceptions, but it also is a powerful framework. Clearly, we do not want to discard things like the very strong protections of the Wiretap Act, for example, against listening to peoples' communication. Those all have to remain in place. I think what we can learn is to articulate, I hope, some of the things that we believe should be in any bill, which is use limitations, collection only for a particular purpose, not converting it to other purposes, discarding it when it is done, notifying people about when their information is being collected, and why, and giving them input into that.

Ms. CHU. Okay. Mr. Villasenor, I would like to focus on the positive benefit of drones. As a representative from southern California, we face many dangerous and costly

wildfires each year, and we certainly can benefit from additional tools to fight these fires. For example, the station fire in the Angeles National Forest in my district killed two firefighters and burned 160,000 acres, and it was the largest wildfire in the modern history of LA County.

Is the FAA Modernization Act helping to accelerate the production of firefighting prevention drones so that local firefighters can have these tools in the near future? Are there any barriers that warrant any congressional review?

Mr. VILLASENOR. I think the FAA is very well aware of the importance of applications like firefighting. The FAA, of course, is not involved in the production of the aircraft but is working diligently and hard on the regulations that are enabling uses, such as firefighting, that nobody in this room I am sure finds objectionable in the least. And so I think that is moving at a pace quite well.

Ms. CHU. Thank you.

And I yield the balance of my time to Congress Member Sheila Jackson Lee.

Mr. SENSENBRENNER. The gentlewoman is recognized for 15 seconds.

Ms. JACKSON LEE. Thank you.

Mr. Calabrese, I just have a simple question. What is the opportunity for racial profiling and how dangerous is that with the utilization of drones?

Mr. CALABRESE. We have certainly seen racial profiling in the use of video cameras. It seems logical to believe it might be applied here.

Mr. SENSENBRENNER. The gentlewoman's time is expired.

The gentleman from Texas, Mr. Gohmert.

Mr. GOHMERT. Thank you, Mr. Chairman.

I do appreciate your being here. I would like to follow up on Ms. Chu. I am curious, the line of questioning she had. I will give an example. There is a doctor friend in Tyler, my hometown, who set his incredible new camera with incredible new lens skyward and took pictures of a shuttle going over and then later saw on the news that it had broken up and got that to the paper. Didn't sell it, just put it out. And it was the most—it was a photograph that has been on more front pages of publications than any other.

On the other hand, if he took that same camera and pointed it in someone's window from a long distance, then you would get an issue. So, obviously, technology makes a difference. And it seems that we do get into some intent issues.

But I am curious, Mr. Calabrese, you say that there is a lot of law in this area—and I was not sure which area you were talking about—but I am curious, if Congress went about setting what we believed—and I think there is a lot of room for agreement on both sides. I appreciated Ms. Bass, Ms. Chu's questions, Mr. Richmond's questions. I think we agree on a great deal in this area. So if we came to an agreement on what we in Congress believed was an appropriate, reasonable expectation of privacy, are you guys aware of a law that would create a problem for us setting such an reasonable expectation of privacy?

Mr. CALABRESE. No, I do not believe so. I believe you have got a very powerful piece of legislation in front of you right now, H.R. 637, and I think that is a very good beginning on setting the parameters for how drones should be used. I think that is a great place to start.

Just to answer your question in terms of the area where there is existing law, I was largely talking about private use. So keeping time logs, stuff like that.

Mr. GOHMERT. Is anybody aware of laws that would be adverse to us trying to set a reasonable expectation of privacy?

Mr. MCNEAL. I am not aware of that, but I would just urge some caution here, Congressman, in that the courts have had decades to try and define reasonable expectation of privacy.

Mr. GOHMERT. I understand. It is a difficult area.

Mr. MCNEAL. I think you might be better served by focusing on the government conduct that you want to control, defining terms like "search" and "public place" and whatnot and controlling, focusing your legislation there rather than trying to define privacy. What is a reasonable expectation of privacy in New York City is very different than what it might be somewhere else.

Mr. GOHMERT. Sure. And Ms. Bass was pointing out she has a lot of paparazzi. In east Texas, we do not have that. But her concern is still my concern. It is not just public government entities,

but if you have a nosy neighbor that has that telescope and points it to your backyard or inside your house, instead of skyward, there ought to be some point that you can expect privacy, right?

Mr. MCNEAL. Right. Focusing, again, on the conduct that we would want to control, it would be either the collection of that information by a private party or the subsequent use of that information. And so sometimes you walk down the street at night in Georgetown and people leave their blinds open, you can see the fancy houses and whatnot. They might feel their privacy is violated, but it is not something that we would want to legislate. If you start snapping photos and using them, then maybe the use of that information internal in the home is the thing that we would want to control.

Mr. MACLIN. Congressman, I would just say this. There is one example of this. In the mid-1970's in *United States v. Miller*, the Supreme Court said we do not have a reasonable expectation of privacy with respect to our banking records. Congress passed legislation which effectively reversed that ruling and gave individuals more privacy.

Mr. GOHMERT. That is a good point. Let me ask this real quick because my time is running out. Is anybody aware of any laws that would prohibit you shooting down a drone in an area in which you were allowed to shoot? I had this question come up with somebody. If it is over your air space, your home, and it is a private, not a government, drone.

Mr. VILLASENOR. I think it would be a very bad idea.

Mr. GOHMERT. No, I am just asking if there are any laws. I had a guy from Georgia say, Hey, we need at least 50 rounds because that is about how many it takes to bring down a drone.

Mr. VILLASENOR. If they did it and ended up hurting some else, they could be charged with reckless discharge.

Mr. GOHMERT. I understand that. But specifically, can you shoot down a drone over your property?

Mr. SENSENBRENNER. Fortunately, the gentleman's time has expired.

Mr. GOHMERT. I appreciate that, Mr. Chairman, since you normally allow people to answer questions that were already asked.

Mr. SENSENBRENNER. All Members of the Subcommittee either having used or yielded their time, those who have been present, without objection, the Subcommittee stands adjourned.

[Whereupon, at 10:18 a.m., the Subcommittee was adjourned.]

○