Congressional Research Service
Informing the legislative debate since 1914

Domestic Drones and Privacy: A Primer

Richard M. Thompson II
Legislative Attorney

March 30, 2015

Congressional Research Service
7-5700
www.crs.gov
R43965

CRS REPORT
Prepared for Members and
Committees of Congress

Summary

It has been three years since Congress enacted the FAA Modernization and Reform Act of 2012 (FMRA), calling for the integration of unmanned aircraft systems (UAS), or "drones," into the national airspace by September 2015. During that time, the substantive legal privacy framework relating to UAS on the federal level has remained relatively static: Congress has enacted no law explicitly regulating the potential privacy impacts of drone flights, the courts have had no occasion to rule on the constitutionality of drone surveillance, and the Federal Aviation Administration (FAA) did not include privacy provisions in its proposed rule on small UAS. This issue, however, has not left the national radar. Congress has held hearings and introduced legislation concerning the potential privacy implications of domestic drone use; President Obama recently issued a directive to all federal agencies to assess the privacy impact of their drone operations; and almost half the states have enacted some form of drone legislation.

There are two overarching privacy issues implicated by domestic drone use. The first is defining what "privacy" means in the context of aerial surveillance. Privacy is an ambiguous term that can mean different things in different contexts. This becomes readily apparent when attempting to apply traditional privacy concepts such as personal control and secrecy to drone surveillance. Other, more nuanced privacy theories such as personal autonomy and anonymity must be explored to get a fuller understanding of the privacy risks posed by drone surveillance. Moreover, with ever-increasing advances in data storage and manipulation, the subsequent aggregation, use, and retention of drone-obtained data may warrant an additional privacy impact analysis.

The second predominant issue is which entity should be responsible for regulating drones and privacy. As the final arbiter of the Constitution, the courts are naturally looked upon to provide at least the floor of privacy protection from UAS surveillance, but as will be discussed in this report, under current law, this protection may be minimal. In addition to the courts, the executive branch likely has a role to play in regulating privacy and drones. While the FAA has taken on a relatively passive role in such regulation, the President's new privacy directive for government drone use and multi-stakeholder process for private use could create an initial framework for privacy regulations. With its power over interstate commerce, Congress has the broadest authority to set national standards for UAS privacy regulation. Several measures were introduced in the 113th Congress that would have restricted both public- and private-actor domestic UAS operations, and reintroduction of these bills is likely in the 114th Congress. Lastly, some have argued that under our system of federalism, the states should be left to experiment with various privacy schemes. It is reported that by the end of 2014, 20 states have enacted some form of drone regulation.

This report will provide a primer on privacy issues related to various UAS operations, both public and private, including an overview of current UAS uses, the privacy interests implicated by these operations, and various potential approaches to UAS privacy regulation.

Contents

Contacts

Introduction

It has been three years since Congress enacted the FAA Modernization and Reform Act of 2012 (FMRA), calling for the integration of unmanned aircraft systems (UAS), or "drones," into the national airspace by September 2015.[1] During that time, the substantive legal privacy framework relating to UAS on the federal level has remained relatively static: Congress has enacted no law explicitly regulating the potential privacy impacts of drone flights; the courts have had no occasion to rule on the constitutionality of drone surveillance; and the Federal Aviation Administration (FAA) did not include privacy provisions in its proposed rule on small UAS.[2] However, this issue has not left the national radar. Congress held several hearings in the 113th Congress on the potential privacy impacts of domestic drone use on American citizens;[3] Members have introduced legislation to regulate both public- and private-actor use of drones;[4] the executive branch has taken various measures to assess the privacy impact of its drone operations;[5] and almost half the states have enacted UAS legislation.[6]

As this report will discuss, there are two overarching privacy issues implicated by domestic drone flights. The first issue is defining and understanding what the chameleon phrase "privacy" means in the context of aerial surveillance. Traditional privacy concepts such as the right to control information about oneself or secrecy do not adequately capture potential privacy concerns raised by visual surveillance; instead, privacy concepts such as personal autonomy and anonymity must be explored to get a fuller understanding about the scope of privacy interests implicated by UAS operations. Additionally, a separate set of privacy interests might be implicated by the subsequent aggregation, use, and retention of drone-obtained information. For instance, the Supreme Court's aerial surveillance cases generally hold that it is not a Fourth Amendment search to conduct surveillance of private property while flying in navigable airspace.[7] However, one could argue that beyond the initial collection of data, a unique privacy interest is at risk by aggregating multiple flights over one's home, using drone-obtained data in ways never envisioned by the initial collection, or retaining that data indefinitely.

The second predominant issue is which entity should be responsible for regulating UAS privacy issues. The courts can be expected to apply traditional privacy rules encompassed in the Fourth Amendment's prohibition against unreasonable searches and privacy torts found largely in state statutory and common law. Since drone use has been relatively limited to date, the courts have yet to address how these laws apply to UAS flights. Privacy safeguards might also come from

[1] FAA Modernization and Reform Act of 2012, P.L. 112-95, §§331-336, 126 Stat. 11, 72-78.

[2] *See* Operation and Certification of Small Unmanned Aircraft Systems, 80 Fed. Reg. 9544, 9552 (proposed Feb. 23, 2015).

[3] *See, e.g.*, *The Future of Drones In America: Law Enforcement and Privacy Considerations: Hearing Before the S. Comm. on the Judiciary*, 113th Cong. (2013) (hereinafter Senate Judiciary Hearing); *Eyes in the Sky: The Domestic Use of Unmanned Aerial Systems: Hearing Before the H. Comm. on the Judiciary Subcomm. on Crime, Terrorism, Homeland Security, and Investigations*, 113th Cong. (2013).

[4] *See* Drone Aircraft Privacy and Transparency Act of 2013, S. 1639, 113th Cong. (2013); H.R. 2868, 113th Cong. (2013); Preserving Freedom from Unwarranted Surveillance Act of 2013, H.R. 972, 113th Cong. (2013), S. 3287, 112th Cong. (2012); Preserving American Privacy Act of 2013, H.R. 637, 113th Cong. (2013).

[5] *See* "Executive Branch," *infra* p. 17.

[6] *See* "States," *infra* p. 26.

[7] *See, e.g.*, California v. Ciraolo, 476 U.S. 207, 215 (1986).

executive branch policies. On February 15, 2015, President Obama issued a memorandum charging all federal agencies that use drones in their operations to evaluate the privacy impact of such use and develop policies to mitigate any privacy concerns.[8] The need for this new initiative may have been prompted, in part, by the FAA's relatively passive role in setting privacy rules for drone operations. The FAA's recently proposed rule for small UAS operations and certifications did not include any privacy provisions, and it is likely the FAA will remain in an advisory, rather than regulatory, role with respect to this issue.[9] With its power over interstate commerce,[10] Congress has the broadest authority to set national standards for UAS privacy regulation. For instance, Congress could create a broad legislative scheme regulating all UAS uses; it could pass more narrow proposals such as a warrant requirement for law enforcement use; or it could create a scheme regulating the subsequent use, retention, and dissemination of drone-obtained data. Federal legislation introduced in the 113th Congress, and likely to be introduced in the 114th Congress, utilized, to some extent, these various approaches.[11] Lastly, some have argued that under our system of federalism, the states should be left to experiment with various privacy schemes.[12] Indeed, the states have taken up this call with 20 states reportedly enacting laws addressing UAS issues by the end of 2014.[13]

In reviewing these various forms of regulation, it is clear that understanding privacy rights vis-à-vis drones is not as simple as applying Supreme Court case law or federal and state statutes. Rather, regulations may come from myriad sources, some statutory, some regulatory, and some practical. With this in mind, this report will provide a primer on privacy issues relating to various UAS operations, both public and private, including an overview of current UAS uses, the privacy interests implicated by these operations, and various potential approaches to UAS privacy regulation.[14]

Background

The FMRA defined an "unmanned aircraft" to mean "an aircraft that is operated without the possibility of direct human intervention from within or on the aircraft."[15] An "unmanned aircraft system" (UAS) is the unmanned aircraft and its "associated elements (including communications

[8] PRESIDENTIAL MEMORANDUM: PROMOTING ECONOMIC COMPETITIVENESS WHILE SAFEGUARDING PRIVACY, CIVIL RIGHTS, AND CIVIL LIBERTIES IN DOMESTIC USE OF UNMANNED AIRCRAFT SYSTEMS (Feb. 15, 2015) [hereinafter Presidential Memorandum on UAS].

[9] Operation and Certification of Small Unmanned Aircraft Systems, 80 Fed. Reg. at 9552.

[10] U.S. CONST. art. I, §8, cl. 3.

[11] *See* Drone Aircraft Privacy and Transparency Act of 2013, S. 1639, 113th Cong. (2013); H.R. 2868, 113th Cong. (2013); Preserving Freedom from Unwarranted Surveillance Act of 2013, H.R. 972, 113th Cong. (2013), S. 3287, 112th Cong. (2012); Preserving American Privacy Act of 2013, H.R. 637, 113th Cong. (2013).

[12] *See* WELLS C. BENNETT, CIVILIAN DRONES, PRIVACY, AND THE FEDERAL-STATE BALANCE, BROOKINGS INSTITUTION (2014); Margot E. Kaminski, *Drone Federalism, Civilian Drones and the Things They Carry*, 4 CAL. L. REV. CIRCUIT 57 (2013).

[13] National Conference of State Legislatures, 2014 Unmanned Aircraft Systems (UAS) Legislation, *available at* http://www.ncsl.org/research/civil-and-criminal-justice/2014-state-unmanned-aircraft-systems-uas-legislation.aspx

[14] For a more in-depth look at privacy and drones, see CRS Report R42701, *Drones in Domestic Surveillance Operations: Fourth Amendment Implications and Legislative Responses*, by Richard M. Thompson II and CRS Report R42940, *Integration of Drones into Domestic Airspace: Selected Legal Issues*, by Alissa M. Dolan and Richard M. Thompson II.

[15] P.L. 112-95, §331, 126 Stat. 72.

links and the components that control the unmanned aircraft) that are required for the pilot in command to operate safely and efficiently in the national airspace system."[16] UAS, commonly referred to as "drones," can range from the size of an insect—sometimes called nano or micro drones—to the size of a traditional jet.[17] Drones can be outfitted with an array of sensors, including high-powered cameras,[18] thermal imaging devices,[19] license plate readers,[20] and laser radar (LADAR).[21] In the near future, drones might be outfitted with facial recognition or soft biometric recognition, which can recognize and track individuals based on attributes such as height, age, gender, and skin color.[22] In addition to their sophisticated sensors, the technical capability of drones is rapidly advancing. For instance, the Defense Advanced Research Projects Agency (DARPA), the technology research arm of the U.S. military, is working on a drone that can enter a building through a window and fly at speeds up to 20 meters/second without communication to the operator and without GPS waypoints.[23] As discussed below, these advanced sensors and capabilities have the capacity to heighten privacy risks posed by drones.

Authorization and Uses

Currently, all UAS operators who do not fall within the recreational use exemption (discussed below) must apply directly to the FAA for permission to fly.[24] The process for obtaining permission to operate differs depending on whether the operator is a public operator or a private commercial operator.

Public Operators

UAS operated by federal, state, or local agencies must obtain a certificate of authorization or waiver (COA) from the FAA.[25] After receiving COA applications, which can be completed online, the FAA conducts a comprehensive operational and technical review of the UAS and can

---

[16] *Id.*

[17] See CRS Report R42136, *U.S. Unmanned Aerial Systems*, by Jeremiah Gertler, for a description of the various types of drones operated in the United States.

[18] *US Army unveils 1.8 gigapixel camera helicopter drone*, BBC NEWS (December 29, 2011 6:11 p.m.), http://www.bbc.com/news/technology-16358851.

[19] *See* Draganflyer X6, Thermal Infrared Camera, http://www.draganfly.com/uav-helicopter/draganflyer-x6/features/flir-camera.php.

[20] This sensor can recognize and permit drones to track vehicles based on license plate numbers. Customs and Border Protection Today, Unmanned Aerial Vehicles Support Border Security (July 2004), http://www.cbp.gov/xp/CustomsToday/2004/Aug/other/aerial_vehicles.xml.

[21] This sensor produces three-dimensional images, and has the capability to see through trees and foliage. U.S. ARMY, UAS CENTER FOR EXCELLENCE, "EYES OF THE ARMY" US ARMY ROADMAP FOR UNMANNED AIRCRAFT SYSTEMS 2010-2035, at 83 (2010).

[22] *See* Clay Dillow, *Army Developing Drones that Can Recognize Your Face from a Distance*, POPSCI (September 28, 2011, 5:01 p.m.), *available at* http://www.popsci.com/technology/article/2011-09/army-wants-drones-can-recognize-your-face-and-read-your-mind.

The issue of weaponizing drones, which presents unique legal issues, is beyond the scope of this report.

[23] Fast Lightweight Autonomy (FLA), Defense Sciences Office, Defense Advanced Research Projects Agency (last visited Feb. 24, 2015), http://www.darpa.mil/Our_Work/DSO/Programs/Fast_Lightweight_Autonomy_%28FLA%29.aspx.

[24] FAA, "Unmanned Aircraft Operations in the National Airspace System," 72 Fed. Reg. 6689 (Feb. 13, 2007).

[25] *Id.*

place limits on its operation in order to ensure its safe use in airspace.[26] COAs are not generally publicly available, but have been released in response to Freedom of Information Act (FOIA) requests. The most recent FOIA request on the FAA's website revealed 426 UAS COA files.[27]

Customs and Border Protection

The most prominent domestic user of UAS among federal agencies is the Department of Homeland Security's (DHS's) U.S. Customs and Border Protection (CBP).[28] As of September 2013, CBP was reported to own 10 UAS, which are operated by CBP's Office of Air and Marine (OAM).[29] The bulk of CBP's flight missions involve patrolling the nation's borders, interdicting persons and contraband illegally entering the United States. CBP's COA allows it to operate in an airspace that covers a 100 mile corridor along the northern border and within 20 to 60 miles along the southern border, excluding urban areas. In addition to its border missions, CBP has provided unmanned aerial support to various federal and state agencies, including the Drug Enforcement Administration (DEA), Immigration and Customs Enforcement (ICE), the U.S. Marshals Service, the U.S. Coast Guard, the Bureau of Land Management, and the Texas Department of Public Safety, among others.[30] In one prominent case, CBP used one of its Predator drones to assist local police in North Dakota to monitor an individual suspected of cattle theft and threatening police officers.[31] The number of these "loan" operations has steadily increased each year since 2010. For instance, CBP flew one flight for the DEA in 2010, 19 flights in 2011, and 66 in 2012.[32]

Department of Justice

The other primary federal agency currently using UAS in its operations is the Department of Justice (DOJ), the nation's chief law enforcement agency. In 2013, DOJ's Office of the Inspector General issued a report reviewing the various UAS programs underway within DOJ.[33] All of the UAS purchased by DOJ so far have been what the FAA calls "small UAS," those 55 pounds or less. The Federal Bureau of Investigation (FBI) has been the most prominent component of DOJ to use UAS in the field and has been doing so since 2006.[34] The FBI noted in a July 2013 letter to Senator Rand Paul that it had used UAS in 10 operations, including those related to search and rescue, drug interdictions, kidnapping, and fugitive investigations.[35] The Bureau of Alcohol,

---

[26] *See generally* FAA "Unmanned Aircraft Systems," *available at* http://www.faa.gov/about/initiatives/uas/cert/.

[27] Freedom of Information Act Responses, FEDERAL AVIATION ADMINISTRATION (last visited March 4, 2015), https://www.faa.gov/uas/public_operations/foia_responses/.

[28] Before operating a UAS in the national airspace, CBP, as with any other governmental entity, must obtain a Certificate of Authorization (COA) from the FAA. See CRS Report R42940, for a discussion of FAA's UAS licensing process.

[29] DEP'T OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT FOR THE AIRCRAFT SYSTEMS 4 (2013).

[30] Customs and Border Protection Drone Flight List – Supplemental, Electronic Frontier Foundation (last visited Feb. 19, 2015), *available at* https://www.eff.org/document/eff-v-dhs-cbp-supplemental-agency-list.

[31] *See* Jason Koebler, *First Man Arrested With Drone Evidence Vows to Fight Case*, U.S. NEWS (April 9, 2012), *available at* http://www.usnews.com/news/articles/2012/04/09/first-man-arrested-with-drone-evidence-vows-to-fight-case.

[32] Customs and Border Protection Drone Flight List, *supra* note 30.

[33] U.S. Dep't of Justice, Office of the Inspector General, Interim Report on the Department of Justice's Use and Support of Unmanned Aircraft Systems (2013), *available at* http://www.justice.gov/oig/reports/2013/a1337.pdf.

[34] *Id.* at 5.

[35] Letter from Stephen D. Kelly, Office of Congressional Affairs, Federal Bureau of Investigation to Senator Rand Paul (continued...)

Tobacco, Firearms and Explosives (ATF) has plans to use UAS in its future operations but has not done so yet.[36] And while the DEA and the Marshals Service have purchased several UAS, as of 2012 they had no plans to use them in future operations.[37] This might be attributed to the DEA and Marshals Service use of CBP drones in their operations.

Other Federal Uses

In addition to DHS and DOJ, the FAA has issued COAs to various other federal entities—both military and civilian.[38] On the defense side, COAs have been issued to DARPA, the U.S. Army, the Navy, the Marine Corps, and the Air Force, for operations in U.S. airspace. On the civilian side, COAs have been issued to the Departments of State, Interior, and Energy, the National Aeronautics and Space Administration (NASA), and the National Institute of Standards and Technology (NIST).

State and Local Governmental Operations

Like their federal counterparts, state and local governmental entities must obtain a COA in order to conduct drone operations. As of 2012, the FAA has issued several hundred COAs to state and local governmental entities to operate UAS.[39] These have included state and city governments, such as Houston, Texas, and the Colorado Department of Transportation; local fire and police departments, including the Miami-Dade Police Department; and state and local universities, like Indiana University.[40]

Private Operators

Until the FAA finalizes its small UAS rule as required under FMRA, there are currently only a limited number of ways to gain authorization for private commercial use of UAS. A private operator may obtain a special airworthiness certificate in the experimental category issued by the FAA.[41] These certificates have been issued on a limited basis for flight tests, demonstrations, and training. The second means of authorization is under FMRA's Section 333, which permits the FAA to authorize certain UAS flights before the FAA issues a final small UAS rule.[42] These Section 333 exemptions have been issued for such purposes as movie productions, precision agriculture, flare stack inspection, and bridge inspections.[43] Finally, certain recreational UAS users may fall within FMRA's model aircraft exception, meaning they are not required to obtain

(...continued)

(July 19, 2013).

[36] DOJ Inspector General Report, *supra* note 33, at 5.

[37] *Id.* at 6.

[38] *See* 2012 FAA Response to Congressman Markey on Drones, Electronic Frontier Foundation (Sept. 21, 2012), *available at* https://www.eff.org/document/2012-faa-response-congressman-markey-drones.

[39] *Id.*

[40] *Id.*

[41] *See* 72 Fed. Reg. 6689; 14 C.F.R. §§21.191, 21.193 (experimental certificates generally); 14 C.F.R. §91.319 (operating limitations on experimental certificate aircraft).

[42] P.L. 112-95, §333, 126 Stat. 75.

[43] Authorizations Granted Via Section 333 Exemptions, Federal Aviation Administration (last visited Feb. 19, 2015), *available at* https://www.faa.gov/uas/legislative_programs/section_333/333_authorizations/.

specific authorization from the FAA before flying UAS. Section 336 of FMRA prohibits the FAA from promulgating a rule regarding "model" aircraft if the aircraft is flown "strictly for hobby or recreational use" and meets several other requirements.[44]

Privacy Interests Implicated by UAS Operations

A threshold issue in analyzing drones and privacy is determining what privacy interests might be implicated by drone operations, both public and private. Privacy is an ambiguous term that can mean different things in different contexts, which becomes apparent when attempting to apply traditional privacy concepts to drone surveillance.

Surveillance

The first privacy interest implicated by the use of UAS is the initial collection of information about people—what can be called "surveillance"—whether it is conducted by a government or private actor. With respect to UAS operations, surveillance takes place in nearly all flights, as one of their major purposes is to collect information, namely visual surveillance, from the sky above. Surveillance might entail a broad and indiscriminate recording of people on the ground using a camera sensor on the aircraft. For instance, the U.S. Air Force recently rolled out the newest iteration of its "Gorgon Stare" sensor, a remotely controlled, aircraft-based Wide-Area Persistent Surveillance (WAPS) system.[45] This sensor allows a single UAS to monitor a 100km^2 area in high resolution for several hours at a time.[46] CBP uses a similar sensor while monitoring the U.S. border.[47] Alternatively, surveillance might consist of more targeted data collection, such as the FBI's use of a drone in 2013 to monitor a standoff with a child kidnapper.[48] Both types of surveillance, to one degree or another, implicate various privacy concepts, including personal control, secrecy, autonomy, and anonymity.

Personal Control

One of the leading privacy theories is the right to control information about oneself. According to one prominent privacy theorist, "[p]rivacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[49] This paradigm works in some mediums, for example, when we consent to a smart phone app tracking our location: we can decide whether the trade-off to our privacy is worth the service we will receive in exchange. However, with drones and aerial surveillance, however, this theory of privacy breaks down. For instance, should we be able to

[44] P.L. 112-95, §336, 126 Stat. 77.

[45] *See* Sierra Nevada Corporation Achieves Milestone for USAF's Advanced Wide-Area Airborne Persistent Surveillance (WAPS) System – Gorgon Stare Increment 2 (July 14, 2014), *available at* http://www.sncorp.com/AboutUs/NewsDetails/618.

[46] *See Sierra Nevada fields Argus-IS upgrade to Gorgon Stare pod, Flight Global* (July 2, 2014), *available at* http://www.flightglobal.com/news/articles/sierra-nevada-fields-argus-is-upgrade-to-gorgon-stare-400978/.

[47] Privacy Impact Assessment, *supra* note 29, at 8.

[48] *See* Victor Blackwell & Michael Pearson, *FBI: Bombs Found in Alabama Kidnapper's Bunker*, CNN (Feb. 5, 2013), *available at* http://www.cnn.com/2013/02/05/us/alabama-child-hostage/.

[49] ALAN WESTIN, PRIVACY AND FREEDOM 7 (1967).

control whether people can view us or our activities in public? How are we expected to exercise such control? And should it make a difference if a person sees us from a traditional aircraft versus a drone? Requiring consent before conducting aerial surveillance could undermine many uses of this new technology, making this theory of privacy as applied to drone surveillance unworkable.

Secrecy

Another prominent theory of privacy is the secrecy model. Under this model, an individual's privacy is invaded if previously concealed information about them is publicly disclosed; or, put another way, an individual is not entitled to privacy where that information has been revealed to another person.[50] The Supreme Court relied on this secrecy model in the three aerial surveillance cases from the 1980s, which held that surveillance conducted in public airspace does not even trigger—let alone violate—the Fourth Amendment's protection against unreasonable searches.[51] Citing to an earlier case, the Court observed in *California v. Ciraolo* that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[52] In addition to Fourth Amendment case law, the privacy tort intrusion upon seclusion applies this same secrecy model such that most activities revealed to the public would not constitute a violation of this tort.[53] If secrecy remains the primary model for the Fourth Amendment and privacy torts, individuals would have little protection from drone surveillance when their location and activities have been revealed to the public.

Autonomy

Another important theory of privacy is personal autonomy. Autonomy generally refers to the ability of an individual to make life decisions free from interference or control by both government and private actors.[54] Some have argued that surveillance represents a form of social control, mandating conformity in society, hindering independent thinking, and recording and notating people who stray from acceptable norms.[55] One such example is Jeremy Bentham's Panopticon, a prison facility designed to give inmates the perception of being watched at all times causing them to self-regulate their behavior to the desired norm.[56] Of course, some form of social control—say, crime control—is beneficial and expected in every society. As noted by Professor Daniel Solove, "many people desire the discipline and control surveillance can bring."[57]

---

[50] *See* Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 494 (2006).

[51] *See* Florida v. Riley, 488 U.S. 445, 450-51 (1989); Dow Chemical Co. v. United States, 476 U.S. 227, 239 (1986); California v. Ciraolo, 476 U.S. 207, 215 (1986).

[52] *Ciraolo*, 476 U.S. at 213 (1986) (quoting Katz v. United States, 389 U.S. 347, 351 (1967)).

[53] See "Privacy Torts," *infra* p. 14.

[54] *See* Whalen v. Roe, 429 U.S. 589, 599 (1977).

[55] *See* JOHN GILLIOM, OVERSEERS OF THE POOR: SURVEILLANCE, RESISTANCE, AND THE LIMITS OF PRIVACY 3 (2001) ("Surveillance of human behavior is in place to control human behavior, whether by limiting access to programs or institutions, monitoring and affecting behavior within those arenas, or otherwise enforcing rules and norms by observing and recording acts of compliance and deviance."); Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1426 (2000) ("The point is not that people will not learn under conditions of no-privacy, but that they will learn differently, and that the experience of being watched will constrain, ex ante, the acceptable spectrum of belief and behavior. Pervasive monitoring of every first move or false start will, at the margin, incline choices toward the bland and the mainstream. The result will be a subtle yet fundamental shift in the content of our character, a blunting and blurring of rough edges and sharp lines.").

[56] 4 JEREMY BENTHAM, THE WORKS OF JEREMY BENTHAM 40 (1843).

He notes that "[t]oo much social control, however, can adversely impact freedom, creativity, and self-development."[58] It would appear that potential risks to personal autonomy will depend, at least in part, on the pervasiveness of drone surveillance. Single, targeted operations would not appear to implicate this fear of societal control and harm to personal autonomy. However, some have questioned what effect 24-hour, *omnipresent* surveillance would have on our public spaces.[59] At this point, the shorter flight capabilities of small UAS—the aircraft likely to be most prevalent in the early stages of UAS integration—would limit the ability to conduct such pervasive surveillance. Yet, as this technology becomes more sophisticated and maximum possible flight times are extended, this risk to autonomy may heighten.

Anonymity

Anonymity is a "state of privacy" that "occurs when the individual is in public places or performing public acts but still seeks, and finds, freedom from identification and surveillance."[60] Professor Christopher Slobogin notes that "the right to public anonymity provides assurance that, when in public, one will remain nameless—unremarked, part of the undifferentiated crowd—as far as the government is concerned. The right is surrendered only when one does or says something that merits government attention, which most of the time must be something suggestive of criminal activity."[61] Others might argue that when we leave our doorstep, and enter into society, we give up this right to anonymity by permitting anyone to view our public movements and whereabouts. Potential blanket UAS surveillance over an urban landscape or a large public event (for instance, the Super Bowl or NASCAR racing), appears to pose a low risk to anonymity. Each person can remain a faceless person in the crowd, free from government identification. Take, for instance, CBP's surveillance at the border: its Predator-B drones reportedly fly at a minimum of 19,000 feet and are not able to identify specific persons on the ground.[62] However, the potential use of sensors such as Automated License Plate Readers (ALPRs)[63] or facial recognition technology,[64] or UAS surveillance specifically targeted at an individual, may have the capacity to eliminate one's anonymity when in public.

Post-Collection Activities

The second class of privacy risks posed by drone surveillance are those activities that occur after surveillance has been conducted—the aggregation, use, and retention of that data. In certain

(...continued)

[57] Solove, *supra* note 50, at 494.

[58] *Id.*

[59] *See* JAY STANLEY AND CATHERINE CRUMP, PROTECTING PRIVACY FROM AERIAL SURVEILLANCE: RECOMMENDATIONS FOR GOVERNMENT USE OF DRONE AIRCRAFT, AMERICAN CIVIL LIBERTIES UNION 11 (2011).

[60] Westin, *supra* note 49, at 7.

[61] Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 MISS. L.J. 213, 238 (2002).

[62] Privacy Impact Assessment, *supra* note 29, at 7.

[63] Customs and Border Protection Today, Unmanned Aerial Vehicles Support Border Security (July 2004), http://www.cbp.gov/xp/CustomsToday/2004/Aug/other/aerial_vehicles.xml.

[64] *See* Andrew Conte, *Drones with Facial Recognition Technology Will End Anonymity, Everywhere*, Business Insider (May 27, 2013), *available at* http://www.businessinsider.com/facial-recognition-technology-and-drones-2013-5.

instances, the initial collection may not directly implicate an individual's privacy interests, but the subsequent manipulation and storage of that data may warrant an alternative privacy analysis.

Aggregation

"Aggregation" is simply the gathering of information about a person whether from one or multiple sources.[65] In the pre-digital era, aggregating information about a person took concerted effort and lots of resources. With computer automation, information can be gathered and aggregated from many sources at the mere push of a button. The privacy theory of aggregation supposes that while the collection of bits of data about a person may not violate his or her privacy interests, extensive collection of information about him or her can rise to the level of a legal privacy intrusion. Professor Solove argues that this unique privacy intrusion arises because "when analyzed, aggregated information can reveal new facts about a person that she did not expect would be known about her when the original, isolated data was collected."[66] This theory was on display in the 2012 GPS tracking case *United States v. Jones*, where five Justices of the Supreme Court (in two separate concurrences) acknowledged that short-term location monitoring was likely not a Fourth Amendment search, but that 28 days of tracking should be considered a search.[67] Judge Richard Leon of the U.S. District Court for the District of Columbia also applied this aggregation theory when invalidating the National Security Agency's (NSA's) metadata program, observing,

> the ubiquity of phones has dramatically altered the *quantity* of information that is now available and, *more importantly,* what that information can tell the Government about people's lives. ... Records that once would have revealed a few scattered tiles of information about a person now reveal an entire mosaic—a vibrant and constantly updating picture of the person's life.[68]

In the context of UAS operations, aggregation may mean the surveillance of an individual for an extended time, or the combination of drone-obtained data with other independent information. A simple one time fly-over of a residence may not significantly implicate any of the privacy interests described above (e.g., secrecy, autonomy, anonymity), but continuous surveillance of a person may implicate this aggregation interest. Alternatively, aggregating drone-collected data with other seemingly personal information, such as telephone,[69] banking,[70] utility,[71] and other records—all of which can be obtained without a probable cause warrant—might entail a unique privacy infringement beyond the mere collection of those individual data sets.

---

[65] *See* Solove, *supra* note 50, at 507.

[66] *Id.*

[67] United States v. Jones, 132 S. Ct. 945, 954 (2012) (Sotomayor, J., concurring), *id.* at 957 (Alito, J., concurring in the judgment).

[68] Klayman v. Obama, 957 F. Supp. 2d 1, 35-36 (D.D.C. 2013). This case is currently before the D.C. Circuit Court of Appeals.

[69] *See* Smith v. Maryland, 442 U.S. 735 (1979).

[70] *See* United States v. Miller, 425 U.S. 435 (1976).

[71] *See* United States v. McIntyre, 646 F.3d 1107 (8th Cir. 2011); United States v. Starkweather, No. 91-30354, 1992 WL 204005, at *2 (9th Cir. August 24, 1992).

Use

The second post-collection privacy risk is the improper use of data—that is, data collected for an authorized purpose, but subsequently used in an unauthorized way. One commentator has argued that in the era of big data, where we inevitably share troves of personal information with the government and commercial entities, privacy rules that focus on the collection and retention of data are "becoming impractical for individuals, while also potentially cutting off future uses of data that could benefit society."[72] He argues that privacy laws should instead focus on controlling the *use* of that data.[73] Various federal laws embody this principle. For instance, the Privacy Act of 1974 requires any federal agency that maintains a database of personal records to inform each individual about whom it collects information of "the principal purpose or purposes for which the information is intended to be used."[74] Similarly, the Driver's Privacy Protection Act of 1994 made it a federal crime "for any person knowingly to obtain or disclose personal information, from a motor vehicle record, for any use not permitted" under that statute.[75] Instead of placing front-end restrictions on drone surveillance, such as requiring warrants before they are operated, policymakers might want to instead regulate how that information is used. For instance, a proposal may permit law enforcement officials to collect information for one purpose—say, traffic control—but prohibit it from using that information for other purposes, such as against an individual in a criminal prosecution absent a court order.

Retention

Another incident of the digital revolution is the near limitless ability of the government and private companies to store and retain information about individuals. The cost of storage has decreased exponentially over the past several decades and is no longer a hindrance to maintaining vast databases of personal data.[76] The Obama Administration's report on big data highlighted this concern when it noted that "the declining cost of collection, storage, and processing of data, combined with new sources of data like sensors, cameras, geospatial and other observational technologies, means that we live in a world of near-ubiquitous data collection."[77] This issue of data retention has been one of the drivers behind Europe's "right to be forgotten" law, which includes a provision requiring that data be retained "for no longer than is necessary for the purposes for which it was collected."[78] Generally speaking, when it comes to Fourth Amendment law, once information is lawfully collected, there are no additional constitutional hindrances to it being stored indefinitely. However, in the NSA metadata litigation, Judge Leon acknowledged that unique privacy interests were affected by the long-term storage of everyone's telephone call records.[79] He observed that in decades past, it was not expected that the government would retain

[72] *See* Craig Mundie, *Privacy Pragmatism*, FOREIGN AFFAIRS (April 2014), *available at* http://www.foreignaffairs.com/articles/140741/craig-mundie/privacy-pragmatism.

[73] *Id.*

[74] 5 U.S.C. §552a(e)(3)(B).

[75] 18 U.S.C. §2722(a).

[76] *See generally* Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. PA. L. REV. 373, 391 (2014).

[77] EXECUTIVE OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES (2014), *available at* http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf.

[78] *See* Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the Protection of Individuals with Regard to Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) Art. 6.

[79] *Klayman*, 976 F. Supp. 2d at 32.

a suspect's phone records once a case was concluded, whereas "[t]he NSA telephony metadata program ... involves the creation and maintenance of a historical database containing *five years'* worth of data."[80] The privacy impact of retention of UAS-derived data would largely depend on whether people could be identified in the recording. Retention of data that contains personally identifiable information and can be located based on this information would seem to implicate this retention interest.

Various Approaches to UAS Privacy Regulation

In addition to the general privacy concepts implicated by drone surveillance, one might question which government entity, if any, should regulate the potential privacy issues posed by the integration of thousands of UAS into domestic skies. Congress neither mentioned the word "privacy" in FMRA nor has it enacted any substantive privacy rules relating to drones subsequently. The FAA recently issued its proposed rule for operating small drones (55 pounds or less), but failed to include any privacy safeguards. Potentially in response to this dearth of privacy regulations, President Obama recently mandated that all federal agencies evaluate the privacy risks posed by their drone operations. This section will explore different approaches to UAS privacy regulation, focusing on the various government institutions—the courts, the executive branch, Congress, and state governments—that might conduct such regulation.

Courts

As the final arbiter of the Constitution,[81] the courts are frequently relied on to safeguard the privacy rights of Americans, whether through the suppression mechanism in criminal prosecutions,[82] or civil suits against government officials for violations of constitutional rights.[83] The Fourth Amendment, as applied by the courts, will provide a floor of legal protections against government actor use of drones. Likewise, privacy torts, which are given much of their content by the courts, will provide some legal recourse to potential privacy invasions caused by drones operated by private actors.

Fourth Amendment

The Fourth Amendment provides in relevant part: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated."[84] This Amendment, like most constitutional protections, applies only to acts by public actors,[85] and, as such, will provide the minimum legal requirements for government use of

[80] *Id.* (emphasis in original).

[81] *See* Marbury v. Madison, 5 U.S. 137, 177 (1803) ("It is emphatically the province and duty of the judicial department to say what the law is."); Cooper v. Aaron, 358 U.S. 1, 18 (1958) ("Marbury declared the basic principle that the federal judiciary is supreme in the exposition of the law of the Constitution, and that principle has ever since been respected by this Court and the Country as a permanent and indispensable feature of our constitutional system.").

[82] *See* Mapp v. Ohio, 367 U.S. 643 (1961).

[83] *See* 42 U.S.C. §1983.

[84] U.S. CONST. amend. IV.

[85] Burdeau v. McDowell, 256 U.S. 465, 475 (1921) ("The Fourth Amendment gives protection against unlawful searches and seizures, and as shown in the previous cases, its protection applies to governmental action. Its origin and (continued...)

drones.[86] In order for the Fourth Amendment to apply in a particular situation, a reviewing court must assess whether the government conducted a "search" by asking whether it invaded an individual's "reasonable expectation of privacy."[87] Although no court has had the opportunity to apply the Fourth Amendment to drone technology, similar cases regarding traditional aircraft and location monitoring provide insight.

In three cases from the 1980s, the Supreme Court upheld the government's warrantless use of traditional aircraft to surveil both private and commercial property.[88] In *Florida v. Riley*, the case most closely resembling potential UAS surveillance, the police flew a helicopter 400 feet above a private residence to determine if marijuana was growing in a greenhouse in the backyard.[89] The Court held that this fly-over was not a Fourth Amendment search, as anyone from the public could have seen the property from that vantage point since the aircraft was in federal airspace.[90] Similarly, in the 1983 case *United States v. Knotts*, the Court held that it was not a Fourth Amendment search to track a person's public movements using an electronic tracking device.[91] There is a general consensus among commentators that a *strict* application of these cases would accord limited privacy safeguards to individuals located on both public and private property from UAS surveillance being conducted from lawful federal airspace.[92]

(...continued)

history clearly show that it was intended as a restraint upon the activities of sovereign authority, and was not intended to be a limitation upon other than governmental agencies").

[86] For a more detailed look at how the Fourth Amendment might apply to UAS, see CRS Report R42701, *Drones in Domestic Surveillance Operations: Fourth Amendment Implications and Legislative Responses*, by Richard M. Thompson II.

[87] *See* Katz v. United States, 389 U.S. 347, 362 (Harlan, J., concurring).

[88] *See* Florida v. Riley, 488 U.S. 445, 450-51 (1989) ("Riley could not reasonably have expected that his greenhouse was protected from public or official observation from a helicopter had it been flying within the navigable airspace for fixed-wing aircraft."); Dow Chemical Co. v. United States, 476 U.S. 227, 239 (1986) ("We hold that the taking of aerial photographs of an industrial plant complex from navigable airspace is not a search prohibited by the Fourth Amendment."); California v. Ciraolo, 476 U.S. 207, 215 (1986) ("In 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. The Fourth Amendment simply does not require the police traveling in the public airways at this altitude to obtain a warrant in order to observe what is visible to the naked eye.").

[89] *Riley*, 488 U.S.at 448.

[90] *Ciraolo*, 476 U.S. at 213 ("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. Nor does the mere fact that an individual has taken measures to restrict some views of his activities preclude an officer's observation from a public vantage point where he has a right to be and which renders the activities clearly visible.").

[91] United States v. Knotts, 460 U.S. 276, 285 (1983).

[92] *See* Senate Judiciary Hearing, *supra* note 3, at 94 (2013) (written statement Ryan Calo, Law Professor, University of Washington School of Law) ("The Supreme Court has made it clear through a series of decisions in the nineteen-eighties that there is no search for Fourth Amendment purposes if an airplane or helicopter permits officers to peer into your backyard. I see no reason why these precedents would not readily extend to drones."); Joseph J. Vacek, *Big Brother Will Soon Be Watching—Or Will He? Constitutional, Regulatory, and Operational Issues Surrounding the Use of Unmanned Aerial Vehicles in Law Enforcement*, 85 N.D. L. REV. 673 (2009) ("Constitutionally, it seems that aerial surveillance by any method of any area in open view from any legal altitude does not implicate the Fourth Amendment, as long as the technology used to obtain the surveillance technology is in general public use and does not penetrate into the home"); Brandon Nagy, *Why They Can Watch You: Assessing Constitutionality of Warrantless Unmanned Aerial Surveillance by Law Enforcement*, 29 BERKELEY TECH. L. J. 135 (2014) ("Those concerned that increasing law enforcement UAS operations erode personal privacy at the expense of the Fourth Amendment do, indeed, have much to worry about. Current Supreme Court jurisprudence, although not directly addressing the Fourth Amendment implications of UAS surveillance, suggests that law enforcement UAS use, with certain limits, would be (continued...)

However, several more recent cases demonstrate that the Court has been uneasy about applying decade-old cases to new technology. In *Kyllo v. United States*, for instance, the use of sense-enhancing technology "not in general public use" to obtain information about the inside of a home was considered a Fourth Amendment search.[93] Similarly, in *United States v. Jones*, five Justices (in two separate concurrences) would have held that a month-long location monitoring using a GPS device constituted a search, even in the face of *Knotts*, which upheld the use of a more rudimentary tracking device.[94] The concurring Justices in *Jones* expressed concern about the sheer ability of these new technologies to collect vast amounts of information about individuals,[95] and their capacity to break down any natural barriers (such as time and resources) to excessive police surveillance.[96] This conundrum of applying old precedent to newer forms of technology is not unique for the federal courts. Several cases currently pending in the federal courts are wrestling with how to apply *Smith v. Maryland*, a case from the 1970s that addressed the collection of telephone numbers of one individual over several days,[97] to the NSA's collection of millions of telephone records over a five-year period.[98] With this trend in mind, federal judges may be persuaded that the sophistication and type of sensors used by UAS present a strong enough privacy risk to modify old precedents such as *Riley* or *Ciraolo* and adapt them to the new potential reality of UAS aerial surveillance. Additionally, depending on the duration of the surveillance and the amount of data collected on an individual, the courts may be inclined to apply an aggregation-type theory to long-term UAS surveillance.

This issue of the law keeping up with technology is a constantly recurring theme in Fourth Amendment jurisprudence. Some have argued that the judiciary is not the ideal forum for creating adequate privacy rules when fast-moving technology is involved.[99] Courts tend to be backward looking—resolving past factual scenarios between two discrete parties. This characteristic makes courts reactive rather than proactive, leading to privacy rules that might fall behind the particular technology in question. For instance, the Supreme Court has yet to resolve whether individuals are entitled to a reasonable expectation of privacy in their emails, a technology that has been around for decades.[100] Part of the problem is that the Court has been unsure of its role in

(...continued)

found constitutional if challenged under the Fourth Amendment.").

[93] Kyllo v. United States, 533 U.S. 27, 34 (2001).

[94] United States v. Jones, 132 S. Ct. 945, 954 (2012) (Sotomayor, J., concurring), *id.* at 957 (Alito, J., concurring in the judgment).

[95] *Id.* at 956 (Sotomayor, J., concurring) ("I would take these attributes of GPS monitoring into account when considering the existence of a reasonable societal expectation of privacy in the sum of one's public movements. I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on.").

[96] *Id.* at 963-64 (Alito, J., concurring) ("In the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical. Traditional surveillance for any extended period of time was difficult and costly and therefore rarely undertaken. The surveillance at issue in this case—constant monitoring of the location of a vehicle for four weeks—would have required a large team of agents, multiple vehicles, and perhaps aerial assistance. Only an investigation of unusual importance could have justified such an expenditure of law enforcement resources. Devices like the one used in the present case, however, make long-term monitoring relatively easy and cheap.").

[97] *See* Smith v. Maryland, 442 U.S. 735 (1979).

[98] *Compare* Klayman v. Obama, 957 F. Supp. 2d 1, 35-36 (D.D.C. 2013), *with* ACLU v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013).

[99] *See* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 858 (2004).

[100] *See* City of Ontario v. Quon, 560 U.S. 746, 760 (2010) (assuming but not holding that individuals have a reasonable (continued...)

developing privacy rules when technology is in flux,[101] with some Justices preferring that legislatures, rather than the courts, take the lead role.[102] This is not to say that this approach is ineffective: this case-by-case approach allows the courts to formulate rules more cautiously based on concrete facts in an adversarial setting, and reduces the risk of creating rules with potentially unintended consequences.

This hesitancy to confront new technologies head-on might explain the Court's recent reliance on property rights as the basis for Fourth Amendment decisions, which, incidentally, might boost Fourth Amendment safeguards against UAS surveillance. In *Jones*, the five-Justice majority led by Justice Scalia rejuvenated a centuries old property-based theory of the Fourth Amendment by holding that the *physical attachment* of a GPS device on the undercarriage of a vehicle constituted an invasion of the owner's "effect" and therefore a Fourth Amendment search.[103] Justice Scalia observed that the *Katz* reasonable expectation of privacy formula added to, but did not replace, the traditional property-based test. Likewise, in *Florida v. Jardines*, the Court relied on this property theory in holding that the government's use of a trained police drug dog to investigate an individual's home and its immediate surroundings was a "search."[104] Depending on the flight path of the aircraft, and the height at which it is operating, this property theory might be employed to hold that flying a UAS onto someone's property with the intent to obtain information is a Fourth Amendment search for which a warrant would be required.

Privacy Torts

Like the Fourth Amendment, a body of laws collectively known as "privacy torts" might create safeguards against privacy invasions by both public- and private-actor use of unmanned aircraft. While some have held up privacy torts as proof that the existing body of case law is sufficient to regulate privacy issues arising from UAS operations,[105] others have asserted that such laws would provide minimal protection from drone surveillance, at least while in public.[106]

(...continued)

expectation privacy in electronic communications).

[101] *Id.* at 759 ("The Court must proceed with care when considering the whole concept of privacy expectations in communications made on electronic equipment owned by a government employer. The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear.").

[102] *Jones*, 132 S. Ct. at 945 (Alito, J., concurring in the judgment) ("In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative. A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way.") (internal citation omitted).

[103] *Jones*, 132 S.Ct. at 949.

[104] Florida v. Jardines, 133 S. Ct. 1409, 1417-18 (2013).

[105] *See* John Villasenor, *Observations from Above: Unmanned Aircraft Systems and Privacy*, 36 HARV. J. L. & PUB. POL'Y 457, 501 (2013) ("Although privacy expectations are greatly reduced outside the home, the non-governmental use of a UAS to capture images and other information taken while the individual is in a public setting could nonetheless constitute an invasion of privacy.").

[106] *See* Senate Hearing, *supra* note 3, at 71 (statement of Ryan Calo, Professor, University of Washington School of Law) ("[T]here are even fewer limitations on the use of drones by individuals, corporations, or the press. The common law privacy torts such as intrusion upon seclusion tend to track the constitutional doctrine that there should be no expectation of privacy in public.").

The genesis of the modern privacy tort sprung from the pens of Justice Louis Brandeis and Samuel Warren in their law review article "Right to Privacy."[107] There, they espoused the view that privacy could form the underpinning of civil liability absent other physical or tortious conduct. This new tort was later broken down into four discrete torts and included in a set of model rules intended for adoption by the states: (1) intrusion upon seclusion; (2) appropriation of one's name or likeness; (3) publicity given to private life; (4) publicity placing person in false light.[108] Of these four, the first and third will likely prove the most applicable to UAS surveillance.

The tort of intrusion upon seclusion, which may vary in its details from state to state, generally provides, "One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person."[109] This tort applies a "reasonable person standard"—that is, it tests whether a person of "ordinary sensibilities" would be offended by the alleged invasion.[110] Likewise, the intrusion must not only be offensive, but "*highly* offensive,"[111] or as one court put it, "outrageously unreasonable conduct."[112] Generally, a single incident will not suffice; instead, the intrusion must be "repeated with such persistence and frequency as to amount to a course of hounding" and "becomes a burden to his existence.... "[113] However, in a few cases a single intrusion was adequate.[114] The invasion of privacy must be intentional, meaning the defendant must desire that the intrusion would occur, or, as with other torts,[115] know with a substantial certainty that such an invasion would result from his actions.[116] An accidental intrusion is not actionable. Finally, in some states, the intrusion must cause mental suffering, shame, or humiliation to permit recovery.[117]

The tort "publicity given to private facts" provides, "One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public."[118] Like the intrusion upon seclusion tort, publicity given to private facts focuses on publicity given to an individual's private, as opposed to public, life.[119] As the comments to the model rules observe, a person cannot complain of someone taking his photograph while walking down the street, but when a photograph is taken without his consent in a private place, and then subsequently published, he will have a valid publicity

[107] *See* Louis D. Brandeis & Samuel D. Warren, *The Right to Privacy*, 4 HARV. L. REV. 193, 205 (1890).

[108] RESTATEMENT (SECOND) OR TORTS §§652B-652E.

[109] *Id.* §652B.

[110] *See* Shorter v. Retail Credit Co., 251 F. Supp. 329, 322 (D.S.C. 1966).

[111] RESTATEMENT (SECOND) OF TORTS §652B (emphasis added).

[112] N.O.C., Inc. v. Schaefer, 484 A.2d 729, 733 (N.J. Super. Ct. Law Div. 1984).

[113] RESTATEMENT (SECOND) OF TORTS §652B cmt. d.

[114] *See, e.g.*, Miller v. National Broadcasting Co., 187 Cal. App. 3d 1463 (Cal. Ct. App. 1986) (videotaping man in his home while being resuscitated after having suffered a heart seizure); Nader v. General Motors Corp., 25 N.Y.2d 560, 570 (1970) (surveilling plaintiff in bank in an "overzealous" manner).

[115] RESTATEMENT (SECOND) OF TORTS §652B.

[116] *See* 2 DAN B DOBBS ET AL., THE LAW OF TORTS §29 (2d ed. 2011).

[117] *See, e.g.,* DeAngelo v. Fortney, 515 A.2d 594, 596 (Pa. Sup. 1986); Burns v. Masterbrand Cabinets, Inc., 369 Ill. App. 3d 1006, 1012 (Ill. App. Ct. 2007).

[118] RESTATEMENT (SECOND) OF TORTS §652D.

[119] *See id.* at cmt. b.

claim.[120] Unlike the intrusion tort, publicity given to private life requires that the information be made available to the public at large, and furthermore, generally prohibits claims that involve matters that are of legitimate public concern.[121]

Under current law, the location of the target of the surveillance largely controls whether someone has a viable claim for both intrusion upon seclusion and publicity given to private life, and this is likely to hold true with drone surveillance. For the most part, using a drone to peer inside the home of another—whether looking through a window or utilizing extra-sensory technology such as thermal imaging—would likely satisfy the intrusion tort, and if photographs were taken and subsequently published, that person would also likely have a claim for publicity given to private life. [122]

The likelihood of a successful claim is significantly diminished, however, if the surveillance is targeted at individuals in a public space,[123] or even while on private property so long as they could be viewed from a public vantage point.[124] Take, for instance, the suit brought by Aaron and

[120] *Id.*

[121] *Id.* at cmt. a, d.

[122] *See, e.g.*, Wolfson v. Lewis, 924 F. Supp. 1413 (E.D. Pa. 1996) (recording plaintiff's home with sophisticated sound and video equipment); Souder v. Pendleton Detectives, 88 So.2d 716, 718 (La. Ct. App. 1956) (peeping into plaintiff's windows); Egan v. Schmock, 93 F. Supp. 2d 1090, 1094-95 (N.D. Cal. 2000) (filming plaintiff and family while in their home); *see also* RESTATEMENT (SECOND) OF TORTS §652B cmt. b, illus. 2.

[123] *See* Schifano v. Green County, 624 So. 2d 178 (Ala. 1993) (dismissing claim against race track operators who took picture of plaintiffs in winner's circle); Fogel v. Forbes, 500 F. Supp. 1081, 1084, 1087 (E.D. Pa. 1980) (dismissing claim for photographs taken at airport); Tellado v. Time-Life, 643 F. Supp. 904, 907 (D.N.J. 1986) (dismissing claim for photographs taken on battlefield in Vietnam); International Union v. Garner, 601 F. Supp. 187, 191-92 (M.D. Tenn. 1985) (dismissing claim for photographing license plates); Tedeschi v. Reardon, 5 F. Supp. 2d 40, 46 (D. Mass. 1998) (same); Jackson v. Playboy Enterprises, Inc., 574 F. Supp. 10, 13 (S.D. Ohio 1983) (dismissing claim for photographing person on sidewalk); *see also* RESTATEMENT (SECOND) OF TORTS §652B cmt. c (commenting that there is generally no liability for photographing or observing a person while in public "since he is not then in seclusion, and his appearance is public and open to the public eye."); William M. Prosser, *Privacy*, 48 CAL. L. REV. 383, 392 (1960) ("On the public street, or in any other public place, the plaintiff has no right to be alone, and it is no invasion of his privacy to do no more than follow him about. Neither is it such an invasion to take a photograph in such a place, since this amounts to nothing more than making a record, not differing essentially from a full written description, of a public sight which anyone present would be free to see.").

There have been some successful claims for intrusion upon seclusion involving surveillance conducted in public, *see* Kramer v. Downey, 684 S.W. 2d 524, 525 (Tex. Ct. App. 1984) ("[W]e now hold that the right to privacy is broad enough to include the right to be free of those willful intrusions into one's personal life at home and at work which occurred in this case."); Daily Times Democrat v. Graham, 276 Ala. 380, 381 (1964); Huskey v. National Broadcasting Co., Inc., 632 F. Supp. 1282, 1285 (N.D. Ill. 1986); *see also* RESTATEMENT (SECOND) OF TORTS §652B cmt. c ("Even in a public place, however, there may be some matters about the plaintiff, such as his underwear or lack of it, that are not exhibited to the public gaze, and there may still be invasion of privacy when there is intrusion upon these matters."), although this is limited to highly embarrassing situations and appears to be the exception rather than the norm. *See* Jennifer R. Scharf, *Shooting for the Stars: A Call for Federal Legislation to Protect Celebrities' Privacy Rights*, 3 BUFF. INTELL. PROP. L.J. 164, 183 (2006) ("Modifying intrusion to apply in public places would be necessary in order to provide any relief.").

[124] *See* McClain v. Boise Cascade Corp., 271 Or. 549, 556 (1975) (dismissing claim where insurance investigator's entered property to take photographs of plaintiff); Mojica Escobar v. Roca, 926 F. Supp. 30, 32-33 (D.P.R. 1996) (dismissing claim against newspaper for photographing outside of home); GTE Mobilnet of South Texas, LTD. Partnership v. Pascouet, 61 S.W. 3d 599, 605 (Tex. Ct. App. 2001) (dismissing claim against company for cell tower workers looking onto property when they serviced nearby cell tower); Aisenson v. American Broadcasting Co, 220 Cal. App. 3d 146, 162-63 (1990) (holding that broadcast of plaintiff while in his driveway and car was not an intrusion upon seclusion); Wehling v. Columbia Broadcasting System, 721 F.2d 506, 509 (5th Cir. 1983) (holding that broadcast of the outside of plaintiff's home taken from public street was not an invasion of privacy); Munson v. Milwaukee Bd. of School Directors, 969 F.2d 266, 271 (7th Cir. 1992) (same).

Christine Boring against Google for photographs taken of their home and subsequently published online as part of Google's Street View program.[125] To create this program, Google employees attach panoramic cameras to their vehicles and drive around taking photographs of areas along the streets. The Borings, who live on a posted private road, discovered that Google had taken photographs of their private residence and swimming pool from their driveway. The Borings sued, among other claims, for intrusion upon seclusion and publicity given to private facts. Both claims were dismissed by the district court. On appeal, the Third Circuit Court of Appeals affirmed the dismissal on both counts, holding that the photographs failed to meet the "highly offensive" standard required under both privacy torts. The court found that "no person of ordinary sensibilities would be shamed, humiliated, or have suffered mentally as a result of a vehicle entering in his or her ungated driveway and photographing him or her from there."[126] The view of the Borings' house, pool, and driveway could "be seen by any person who entered onto their driveway, including a visitor or a delivery man."[127] Recording someone with a drone in a public place or even on private property that can be viewed from a public vantage point, as in the Google Street View case, would likely not constitute an invasion under either of these privacy torts.

Executive Branch

In addition to the courts, the executive branch is likely to play a significant role in regulating the privacy implications of UAS operations. Although the FAA has attempted to focus on safety and other regulatory issues, privacy remains a perennial topic for the FAA as it leads the federal government's UAS integration efforts. Some have posited that instead of the FAA, other executive branch agencies, such as DHS and DOJ, should take the lead role in overseeing the privacy implications of their own unmanned operations.[128] President Obama recently issued a new memorandum taking a similar approach, directing all federal agencies to evaluate the privacy impact of their UAS operations and developing policies to mitigate such concerns.

FAA—Privacy Rules at the Test Sites and Beyond

In FRMA, Congress charged the FAA with integrating UAS into the national airspace.[129] Since passage of this legislation, the FAA has become the center of debate on the privacy implications of these new aircraft. Some in the industry and law enforcement have questioned FAA's authority to regulate privacy at all, arguing that it is both outside its expertise and its legislative grant of authority.[130] Others have argued that precisely because the FAA is charged with integrating UAS

[125] Boring v. Google, Inc., No. 09-2350, 362 Fed. Appx. 273 (3d Cir. 2013).

[126] *Id.* at 279.

[127] *Id.*

[128] Senate Judiciary Hearing, *supra* note 3, at 51 (answer from Michael Toscano, President and Chief Executive Officer, Association of Unmanned Vehicle Systems International).

[129] P.L. 112-95, §332, 126 Stat. 123-24.

[130] *See, e.g.,* Press Release, Association for Unmanned Vehicle Systems International, AUVSI to FAA: Focus on your Mission, Proceed with UAS Integration (Nov. 28, 2012) ("As an industry, we support a continued, civil dialogue on privacy, but any such conversations should take place concurrent with the integration. The selection process for the six test sites are a separate issue and should be treated as such. Meanwhile, the FAA should adhere to its mission and do what it does best – focus on the safety of the U.S. airspace – while other, more appropriate institutions consider privacy issues."), *available at* http://www.auvsi.org/AUVSINews/AssociationNews.

that it must resolve one of the most pressing issues involved with such integration—privacy.[131] As a general matter, the FAA has stated that its "mission does not include developing or enforcing policies pertaining to privacy or civil liberties,"[132] but several of its obligations in FMRA have kept the FAA enmeshed in this privacy debate.

The first such obligation was FMRA's mandate that the FAA establish six test sites to help facilitate the integration of UAS into the national airspace. Neither the program requirements nor the list of attributes for selecting the test sites expressly granted the FAA authority to regulate privacy, or even mentioned "privacy" as a general matter of consideration.[133] Nonetheless, the FAA sought public comment on a proposed privacy policy for UAS operations at the sites on February 22, 2013, and issued a final rule on November 14, 2013.[134] The privacy rules, which are contained as a provision in the contracts (known as an "Other Transaction Agreement," or OTA) between the FAA and each site operator include the following requirements: (1) operations at the test sites must adhere to existing federal, state, and local laws regarding an individual's right to privacy; (2) the test site operator must develop a publicly available privacy policy that is informed by the Fair Information Practice Principles (a generally accepted set of rules that regulate how data should be stored, used, and disseminated); (3) the site operator must maintain a record of all UAS operating at the test site; and (4) the site operator must require each UAS operator to have a written plan for the operator's use and retention of data collected by the UAS.[135] The authority to create these rules was purportedly under the FAA's contracting authority and not its general statutory authority.[136] Although the FAA retains the authority to rescind an OTA for a site operator in violation of existing privacy laws, ultimately, this privacy policy signals a hands-off approach, leaving the policing of privacy rules to private parties affected by operations at the test sites, to the test site operators themselves, and to local and state government bodies that oversee the test site operators.[137]

Despite this relatively passive approach to privacy at the test sites, the FAA has recognized the political and legal importance of privacy in both its proposed small UAS rule and its various planning documents required under FMRA. On February 15, 2015, the FAA issued its proposed operating requirements to allow small UAS (less than 55 pounds) to operate for non-hobby or non-recreational purposes.[138] As was expected, the FAA noted that privacy concerns "were

[131] *See* Keith Laing, *Markey: FAA Drone Plan 'Falls Far Short*,' THE HILL (Nov. 7, 2013), *available at* http://thehill.com/policy/transportation/189603-markey-faa-drone-plan-falls-far-short; Electronic Frontier Foundation, The FAA Creates Thin Privacy Guidelines for the Nation's First Domestic Drone "Test Sites," (Dec. 10, 2013), *available at* https://www.eff.org/deeplinks/2013/12/faa-creates-thin-privacy-guidelines-nations-first-domestic-drone-test-sites.

[132] *See* FEDERAL AVIATION ADMINISTRATION, INTEGRATION OF CIVIL UNMANNED AIRCRAFT SYSTEMS (UAS) IN THE NATIONAL AIRSPACE SYSTEM (NAS) ROADMAP 11 (Nov. 7, 2013), *available at* https://www.faa.gov/uas/legislative_programs/uas_roadmap/media/UAS_Roadmap_2013.pdf.

[133] P.L. 112-95, §332(c), 126 Stat. 73-4 (2012).

[134] Unmanned Aircraft System Test Site Program, 78 Fed. Reg. 68360 (Nov. 14, 2013).

[135] *Id.* at 68,364.

[136] *Id.* at 68,361 ("The FAA's authority for including the Final Privacy Requirements in the Test Site OTAs is set forth in 49 U.S.C. §106(l)(6). That statute authorizes the FAA Administrator to enter into an OTA 'on such terms and conditions as the Administrator may consider appropriate.' The FAA believes that it is appropriate to comply with the Final Privacy Requirements.").

[137] *Id.* at 68,632 ("[T]he FAA believes that Test Site operators will be responsive to local stakeholders' privacy concerns and will develop privacy policies appropriately for each Test Site. ... The FAA expects that [the test site operators] will be responsive to stakeholders concerns.").

[138] Notice of Proposed Rulemaking, Operation and Certification of Small Unmanned Aircraft Systems, Federal (continued...)

beyond the scope of this rulemaking."[139] However, the FAA also noted it would participate in the "multi-stakeholder engagement process" (described below) to assist in a privacy framework concerning commercial and private use of drones. Also, in its five-year roadmap required under FMRA, the FAA noted that while its primary mission "does not include developing or enforcing policies pertaining to privacy or civil liberties, experience with the UAS test sites will present an opportunity to inform the dialogue ... concerning the use of UAS technologies and the areas of privacy and civil liberties."[140] Likewise, in its Comprehensive Plan, also required under FMRA, the FAA devoted a whole section to highlighting the privacy and civil liberties concerns that all federal agencies must take into account as UAS are integrated into the national airspace.[141] While safety will undoubtedly remain the top priority of FAA officials as it navigates the difficult task of integrating drones in the national airspace, with its prominent role of testing and licensing both government, commercial, and private use of drones, it will remain a significant voice in the ongoing privacy debate.

President's Memorandum on UAS and Privacy

On February 15, 2015, the same day the FAA issued its proposed small UAS rule, President Obama issued a memorandum entitled "Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems."[142] This presidential memorandum establishes two new frameworks relating to the potential privacy implications of drone operations by both government and private actors.

UAS Policies and Procedures for Federal Government Use

The memorandum first observes that all operations conducted by federal agencies must comply with the Constitution, federal law, and other applicable regulations and policies, an obligation to which agencies are already subject. The memorandum requires that, prior to deployment of new UAS technology and at least every three years, all federal agencies must "examine their existing UAS policies and procedures relating to the collection, use, retention, and dissemination of information obtained by UAS, to ensure that privacy, civil rights, and civil liberties are protected."[143] Agencies that collect information through UAS shall ensure their policies and procedures adhere to the following requirements:

(...continued)

Aviation Administration (Feb. 15, 2015), *available at* http://www.faa.gov/regulations_policies/rulemaking/recently_published/media/2120-AJ60_NPRM_2-15-2015_joint_signature.pdf.

[139] *Id.* at 36.

[140] Federal Aviation Administration, Integration of Civil Unmanned Aircraft Systems (UAS) in the National Airspace System (NAS) Roadmap (Nov. 7, 2013), *available at* https://www.faa.gov/uas/legislative_programs/uas_roadmap/media/UAS_Roadmap_2013.pdf.

[141] Federal Aviation Administration, Unmanned Aircraft Systems (UAS) Comprehensive Plan: A Report on the Nation's UAS Path Forward 7 (Sept. 2013), *available at* https://www.faa.gov/about/office_org/headquarters_offices/agi/reports/media/UAS_Comprehensive_Plan.pdf.

[142] Presidential Memorandum, *supra* note 2.

[143] Beyond privacy, the President's memorandum requires that agencies shall ensure they have policies in place that prohibit the collection, use, retention, and dissemination of data in a manner that would violate the First Amendment or would discriminate against persons based upon their ethnicity, race, gender, national origin, religion, sexual orientation, or gender identity, in violation of law. *See* Presidential Memorandum, *supra* note 2.

> (i) Collection and Use. Agencies must only collect information using UAS, or UAS-collected information, to the extent that such collection or use is consistent with and relevant to an authorized purpose.
>
> (ii) Retention. Information collected using UAS that may contain PII [personally identifiable information] shall not be retained for more than 180 days unless retention of the information is determined to be necessary to an authorized mission of the retaining agency, is maintained in a system of records covered by the Privacy Act, or is required to be retained for a longer period by any other applicable law or regulation.
>
> (iii) Dissemination. UAS-collected information that is not maintained in a system of records covered by the Privacy Act shall not be disseminated outside of the agency unless dissemination is required by law, or fulfills an authorized purpose and complies with agency requirements.

To ensure accountability, the memorandum requires, among other things, that agencies develop protocols for receiving, investigating, and addressing potential privacy complaints; ensure they have rules of conduct and training for federal government personnel and contractors; establish meaningful oversight of individuals who have access to sensitive information collected by UAS; develop policies and procedures to authorize the use of UAS in response to a request for UAS assistance of federal, state, tribal, or territorial government operations; and ensure that local entities that purchase UAS through federal funding have policies in place to safeguard privacy and civil liberties prior to expending such funds.

To promote transparency, the memorandum requires agencies to provide notice to the public regarding where the agency's UAS are authorized to operate; keep the public informed about the agency's UAS program as well as changes that would significantly affect privacy; and make available to the public, on an annual basis, a general summary of the agency's UAS operations during the previous fiscal year, to include a brief description of types or categories of missions flown, and the number of times the agency provided assistance to other agencies, or to state, local, tribal, or territorial governments.

The agencies must report to the President within 180 days from the date of the issuance of the memorandum with a status on the implementation of these policies and procedures, and must make these policies publicly available within one year.

Multi-Stakeholder Engagement Process for Commercial and Private UAS Use

The President's memorandum also charges the Department of Commerce, through the National Telecommunications and Information Administration (NTIA), to initiate "a multi-stakeholder engagement process to develop a privacy framework regarding privacy, accountability, and transparency for commercial and private UAS use."[144] The end result is expected to be a set of voluntary best practices for privacy issues implicated by commercial and private UAS use.

[144] Presidential Memorandum, *supra* note 8.

Privacy Impact Assessments and Privacy Working Groups

Prior to the President's memorandum, several federal agencies had taken steps to assess and address the privacy impacts of their UAS operations. In September 2013, DHS's Chief Privacy Officer, in conjunction with CBP's Office of Air and Marine, issued a Privacy Impact Assessment (PIA) primarily evaluating the privacy impact of its operations at the U.S. border.[145] This was prompted, in part, by statutory obligations under federal law.

Under the E-Government Act of 2002, federal agencies must conduct a PIA before (1) "developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form"; or (2) "initiating a new collection of information that will be collected, maintained, or disseminated using information technology ... [and] includes information in an identifiable form permitting the physical or online contacting of a specific individual."[146] Specific to the Department of Homeland Security, under the Homeland Security Act of 2002, DHS must conduct PIAs "of proposed rules of the Department or that of the Department on the privacy of personal information, including the type of personal information collected and the number of people affected."[147] More generally, the Privacy Officer of DHS is required to coordinate with the Officer for Civil Rights and Civil Liberties to ensure that "(A) programs, policies, and procedures involving civil rights, civil liberties, and privacy considerations are addressed in an integrated and comprehensive manner; and (B) Congress receives appropriate reports on such programs, policies, and procedures."[148]

DHS's PIA evaluated the various uses of UAS in DHS's operations, including its operations at the border, and concluded that such operations have minimal privacy impact. Because current DHS operations limit flights to an altitude of 19,000 feet, the report noted that cameras on UAS do not permit the operator to specifically identify people on the ground nor do they use technology that sees through walls or collects information regarding the interior of buildings. The report noted that personally identifiable information (PII) is generally not retrieved, but that images may later be associated with specific individuals if they are apprehended and the surveillance feed is associated with them. Acknowledging that UAS can stay in flight longer than traditional aircraft, the report concludes that the privacy impact of this technological difference is mitigated by various safeguards including well-defined flight operations, restrictions on accessing collected data, and security protocols for storing data. It is likely that DHS will utilize this PIA when developing any new policies and procedures required by the President's new memorandum.

In addition to PIAs, in late 2012, DHS's Office for Civil Rights and Civil Liberties and its Privacy Office spearheaded the "Working Group to Safeguard Privacy, Civil Rights, and Civil Liberties in the Department's Use and Support of Unmanned Aerial Systems."[149] The working group was intended to assess all active and planned uses of UAS by the various components of DHS and flag any privacy or civil liberties issues potentially raised by such operations. The goal

[145] Privacy Impact Assessment, *supra* note 29.

[146] 44 U.S.C. §3501 (note).

[147] 6 U.S.C. §142.

[148] 6 U.S.C. §142(a)(5).

[149] Dep't of Homeland Security, Working Group to Safeguard Privacy, Civil Rights, and Civil Liberties in the Department's Use and Support of Unmanned Aerial Systems (Sept. 14, 2012), *available at* https://www.dhs.gov/sites/default/files/publications/foia/working-group-to-safeguard-privacy-civil-rights-and-civil-liberties-in-the-departments-use-and-support-of-unmanned-aerial-systems-uas-s1-information-memorandum-09142012.pdf.

was to develop a set of best practices for safeguarding these various legal interests, and it was reported in September 2014 that such a document would be out by the end of 2014.[150] DHS has yet to release this best practices document. It may be that this document will be subsumed into the larger obligations placed on DHS through the President's new memorandum.

DOJ Inspector General UAS Report

There has been some debate within DOJ concerning the extent to which unmanned aerial surveillance differs from manned aerial surveillance, and whether these differences warrant new rules for deploying UAS in law enforcement operations. A report issued by DOJ's Office of Inspector General explained that both the FBI and ATF did not see a practical difference in how UAS collect evidence as compared to their manned counterparts.[151] As such, these entities did not see a need to develop specialized UAS privacy protocols. DOJ's Inspector General disagreed with the assessment of the FBI and ATF and concluded the following in its interim report:

> We found that the technological capabilities of UAS and the current, uncoordinated approach of DOJ components to UAS use may merit the DOJ developing consistent, UAS-specific policies to guide the proper use of UAS. Unlike manned aircraft, UAS can be used in close proximity to a home and, with longer-lasting power systems, may be capable of flying for several hours or even days at a time, raising unique concerns about privacy and the collection of evidence with UAS. Considering that multiple components are using or have the potential to use UAS, we believe the Office of the Deputy Attorney General (ODAG), which has the primary responsibility within DOJ for formulating cross-component law enforcement policies, should consider the need for a DOJ-wide policy regarding UAS uses that could have significant privacy or other legal implications.[152]

This conclusion that unmanned operations pose a unique and potentially greater privacy threat than manned operations mirrors that of the President's new memorandum on UAS operations. Even when DOJ, like all other federal agencies using UAS, adopts specific policies and procedures addressing the privacy impact of its UAS operations, this inevitably prompts the question whether federal agencies should be left to police their own surveillance activities. While praising the White House drone memorandum as "an important and welcome step in advancing drone technology," one commentator noted that the memo itself "does not establish strong privacy and transparency drone standards for agencies, leaving it up to the agencies to develop these standards."[153] He continues: "Because the memo's requirements are not specific, the drone policies the agencies set for themselves will be key to how individuals' privacy is actually protected. Congress still has a role to play in setting strong privacy and transparency standards for drone use."[154]

[150] DEP'T OF HOMELAND SECURITY, PRIVACY OFFICE, 2014 ANNUAL REPORT TO CONGRESS 19 (Sept. 30, 2014), *available at* http://www.dhs.gov/sites/default/files/publications/dhs-privacy-office-2014-annual-report-FINAL.pdf.

[151] DOJ Inspector General Report, *supra* note 33, at ii.

[152] *Id.*

[153] Harley Geiger, White House Drone Memo Right to Focus on Privacy, Center for Democracy and Technology (Feb. 15, 2015), *available at* https://cdt.org/press/white-house-drone-memo-right-to-focus-on-privacy/.

[154] *Id.*

Congress

Several measures were introduced in the 113th Congress that would have restricted both public- and private-actor domestic UAS operations, and reintroduction of these bills is likely in the 114th Congress. The proposed regulations in these bills range from warrant requirements for law enforcement operations to comprehensive data collection and minimization statements to privacy-tort-like prohibitions against private-actor intrusions. Additionally, Congress has utilized its oversight authority to hold hearings and probe executive branch agencies to disclose when and where they are using drones and the potential privacy implications of such uses.

Legislation

Drone Aircraft Privacy and Transparency Act of 2013 (S. 1639, H.R. 2868)

In the 113th Congress, Senator Ed Markey and Representative Peter Welch introduced nearly identical legislation entitled the Drone Aircraft Privacy and Transparency Act of 2013 (S. 1639, H.R. 2868).[155] These bills would have amended FMRA to create a comprehensive scheme to regulate both government and private-actor use of drones, including data collection requirements, a warrant requirement for law enforcement, and various enforcement mechanisms.

First, these bills would have required the Secretary of Transportation, with input from the Secretary of Commerce, the Chairman of the Federal Trade Commission, and the Chief Privacy Officer of the Department of Homeland Security, to study any potential threats to privacy protections posed by the introduction of drones in the national airspace. They would have prohibited the FAA from issuing a license to operate a drone unless the application included a "data collection statement." This statement would have had to include a list of individuals who would have the authority to operate the drone; the location in which the drone would be used; the maximum period it would be used; and whether the drone would be collecting information about individuals. If the drone would be used to collect personal information, the statement would have had to provide the circumstances in which such information would be used; the kinds of information collected and the conclusions drawn from it; the type of data minimization procedures to be employed; whether the information would be sold, and if so, under what circumstances; how long the information would be stored; and the procedures for destroying irrelevant data.

The statement also would have had to include information about the possible impact on privacy protections posed by the operation under that license and steps to be taken to mitigate this impact. Additionally, the statement would have had to include the contact information of the drone operator; a process for determining what information had been collected about an individual; and a process for challenging the accuracy of such data. Finally, the FAA would have been required to post the data collection statement on the Internet.

In addition to the data collection statement, any law enforcement agency which operates a drone would have had to file a "data minimization statement" with the FAA. This statement would have required adoption of policies by the agency that minimize the collection of information and data unrelated to the investigation of a crime under a warrant; required the destruction of data that is

[155] S. 1639, 113th Cong. (2013); H.R. 2868, 113th Cong. (2013).

no longer relevant to the investigation of a crime; established procedures for the method of such destruction; and established oversight and audit procedures to ensure the agency operates a UAS in accordance with the data collection statement filed with the FAA.

S. 1639 and H.R. 2868 would have provided several enforcement mechanisms. First, the FAA could have revoked a license of a user that did not comply with these requirements. The Federal Trade Commission would have had the primary authority to enforce the data collection requirements. Additionally, the Attorney General of each state, or an official or agency of a state, would have been empowered to file a civil suit if there was reason to believe that the privacy interests of residents of that state had been threatened or adversely affected. These bills would have also created a private right of action for a person injured by a violation of this legislation.

These bills would also have prohibited a governmental entity from using a drone, or obtaining information from another person using a drone, for protective activities, or for law enforcement or intelligence purposes, except with a warrant. This prohibition would not apply in "exigent circumstances," which was defined to mean imminent danger of death or serious physical injury or high risk of terrorist attack as determined by the Secretary of Homeland Security.

Preserving Freedom from Unwarranted Surveillance Act of 2013 (S. 1016, H.R. 972)

Senator Rand Paul and Representative Austin Scott's companion bills, the Preserving Freedom from Unwarranted Surveillance Act of 2013 (S. 1016, H.R. 972), would have focused exclusively on government drone operations.[156] These bills would have required any entity acting under the authority of the federal government to obtain a warrant based upon probable cause before conducting drone surveillance to investigate violations of criminal law or regulations. S. 1016 and H.R. 972 included several exceptions to this warrant requirement: (1) when necessary to prevent or deter illegal entry of any persons or illegal substances into the United States; (2) when a law enforcement officer possesses reasonable suspicion that under particular circumstances "swift action to prevent imminent danger to life or serious damage to property, or to forestall the imminent escape of a suspect, or destruction of evidence" is necessary; or (3) when the Secretary of Homeland Security determines credible intelligence indicates a high risk of a terrorist attack by a specific individual or organization. H.R. 972 would have created a right to sue for any violation of its prohibitions. Unlike H.R. 972, S. 1016 included an express exclusionary rule for evidence obtained in violation of the act.

Preserving American Privacy Act of 2013 (H.R. 637)

Representative Ted Poe introduced the Preserving American Privacy Act of 2013 (H.R. 637), which would have regulated both public and private use of drones under various mechanisms.[157] As to law enforcement use, H.R. 637 would have created a general prohibition on the use of drones to collect covered information or disclose covered information so collected. "Covered information" was defined as "information that is reasonably likely to enable identification of an

[156] H.R. 972, 113th Cong. (2013). Senator Rand Paul filed similar legislation in the 112th Congress, but did not re-introduce it in the 113th Congress. *See* S. 3287, 112th Cong. (2012). Unlike H.R. 972, S. 3287 included an express exclusionary rule for evidence obtained in violation of the act.

[157] H.R. 637, 113th Cong. (2013).

individual" or "information about an individual's property that is not in plain view." This prohibition was subject to the following exceptions: (1) law enforcement obtains a court-issued warrant and serves a copy of the warrant on the target of the search within 10 days of the surveillance. However, notice need not be provided if it would jeopardize an ongoing criminal or national security investigation.(2) Law enforcement obtains a court-issued order based upon "specific and articulable facts showing a reasonable suspicion of criminal activity and a reasonable probability" that the operation "will provide evidence of such criminal activity." The order may authorize surveillance in a stipulated public area for no more than 48 hours which may be renewed for a total of 30 days. Notice of the operation must be provided to the target no later than 10 days after the operation. Alternatively, notice may be provided not less than 48 hours before the operation in a major publication, on a government website, or with signs posted in the area of the operation. (3) Operation is within 25 miles of national border. (4)The targeted individual has provided prior written consent. (5) Emergency situation involves danger of death or serious physical injury, conspiratorial activities threatening the national security interest, or conspiratorial activities characteristic of organized crime, where a warrant cannot be obtained with due diligence. Law enforcement must then obtain a warrant within 48 hours of such operation. Any evidence obtained in violation of this act would not have been admissible in any trial or adjudicative proceeding.

Additionally, H.R. 637 would have required any governmental entity applying for a certificate or license to operate a UAS to also file a data collection statement with the Attorney General, which would have included the purpose for which the UAS will be used; whether the UAS is capable of collecting covered information; the length of time the information will be retained; a point of contact for citizen feedback; the particular unit of governmental entity responsible for safe and appropriate operation of the UAS; the rank and title of the individual who may authorize the operation of the UAS; the applicable data minimization policies barring the collection of covered information unrelated to the investigation of crime and requiring the destruction of covered information that is no longer relevant to the investigation of a crime; and applicable audit and oversight procedures.

Under H.R. 637, the Attorney General would have been empowered to request that the Secretary of Transportation revoke the license or certificate of any entity that fails to file a data collection statement. Further, H.R. 637 contained a provision permitting administrative discipline against an officer who intentionally violates a provision of this act.

H.R. 637 would also have made it unlawful to intentionally operate a private UAS to capture images in a manner highly offensive to a reasonable person where the person is engaging in a personal or familial activity under circumstances in which the individual has a reasonable expectation of privacy, regardless of whether there is a physical trespass.[158]

Oversight

In addition to its authority to enact federal law, Congress can and has utilized its oversight function to shape the debate surrounding the privacy implications of drone surveillance. For instance, both the Senate and House Judiciary Committees held hearings in the 113th Congress specifically addressing the privacy impact of drone operations. Additionally, individual members probed executive branch officials on when and where they were using drones and the potential

[158] H.R. 637, 113th Cong. (2013).

privacy implications of such uses. One such example of this oversight function is demonstrated by correspondence between the Senator Rand Paul and the FBI in the summer of 2013. In a July 25, 2013, letter to FBI Director Mueller, Senator Paul asked how the Bureau defined "reasonable expectation of privacy" in the context of UAS surveillance, as Paul feared that "an overbroad interpretation of this protection would enable more substantial information collection on an individual in a circumstance they might not have believed was subject to surveillance."[159] The FBI responded by arguing that based on the Supreme Court's three aerial surveillance cases from the 1980s, it need not obtain a warrant for any surveillance "open to public view" and that the "Fourth Amendment principles applicable to manned aerial surveillance discussed in these cases apply equally to UAVs."[160] Similar oversight is likely to continue in the 114th Congress.

States

Justice Brandeis once observed that "it is one of the happy incidents of the federal system that a single courageous state may, if its citizens choose, serve as a laboratory; and try novel social and economic experiments without risk to the rest of the country."[161] Some have argued that under this theory of federalism, the states are best situated to experiment with various UAS policies to determine the most appropriate legal framework for their state.[162] Others have countered that applying a patchwork of 50 different privacy regimes would be overburdensome on both public and private users of UAS. According to the National Conference of State Legislatures (NCSL), by the end of 2014, 20 states had enacted laws addressing UAS issues.[163]

State laws in this area have mainly come in three forms. The first, and perhaps most numerous, are laws that create broad prohibitions on their own state law enforcement entities, subject to various exceptions that differ from state to state.[164] These exceptions include obtaining a warrant based upon probable cause; countering a high risk of terrorist attack; responding to threats of imminent harm of human life; locating a missing person; and conducting crime scene and traffic photography, among others. The second category relates to use restrictions of data collected by UAS. For instance, Illinois requires law enforcement to destroy all information gathered by a UAS within 30 days of collection unless there is reasonable suspicion that the information contains evidence of criminal activity or the information is relevant to an ongoing criminal investigation.[165] While the relevancy standard is a very low evidentiary threshold, it does prevent limitless retention of private data. Similarly, Alaska prohibits the retention of records collected by drones unless it is required as part of an investigation or prosecution, is used for training purposes, or is required by federal or state law.[166] Images that are retained under Alaska's statute are considered confidential and not subject to the state's public records laws. The third category

[159] Letter from Senator Rand Paul to Federal Bureau of Investigation Director Robert Mueller (July 25, 2013), *available at* http://www.paul.senate.gov/files/documents/072513Paulresponse.pdf.

[160] Letter from Stephen D. Kelly, Assistant Director, Office of Congressional Affairs, Dep't of Justice to Senator Rand Paul (July 29, 2013), *available at* http://www.paul.senate.gov/files/documents/072913FBIResponse.pdf.

[161] New State Ice Co. v. Liebmann, 285 U.S. 262 (1932) (Brandeis, J., dissenting).

[162] *See* Bennett, *supra* note 12; Kaminski, *supra* note 12.

[163] National Conference of State Legislatures, 2014 Unmanned Aircraft Systems (UAS) Legislation, *available at* http://www.ncsl.org/research/civil-and-criminal-justice/2014-state-unmanned-aircraft-systems-uas-legislation.aspx

[164] *See, e.g.*, ALASKA STAT. §18.65.902; FLA. STAT. ANN. §934.50.

[165] 725 ILL. COMP. STAT. §167/20.

[166] ALASKA. CODE §18.65.902.

relates to regulation of private actors, generally through the creation of private causes of action for privacy invasions caused by UAS surveillance. For instance, Idaho prohibits recording individuals on their residence without their consent, or from photographing an individual for the purpose of publishing or otherwise publicly disseminating such photograph no matter where the target is located.[167] Undoubtedly, this third category of proposals creates tension between the public's First Amendment right to gather news and the individual privacy interests at stake, requiring legislatures to fine tune this balance when enacting UAS legislation.

Author Contact Information

Richard M. Thompson II
Legislative Attorney
rthompson@crs.loc.gov, 7-8449

[167] IDAHO CODE §21-213.