Washington and Lee Law Review

Volume 72 | Issue 3 Article 3

Summer 5-1-2015

Government-Operated Drones and Data Retention

Gregory S. McNeal
Pepperdine University

Government-Operated Drones and Data Retention

Gregory S. McNeal*

Table of Contents

I. Introduction 1139
II. Background on Drones 1140
III. The President's Order Regarding Federal Government Drone Operations 1143
IV. The Need for Action in States and Municipalities Regarding Data Handling Procedures 1147
V. Data Retention Procedures for Drones 1149
A. Adopt Data Retention Procedures that Require Heightened Levels of Suspicion and Increased Procedural Protections Over Time 1149
B. Adopt Transparency and Accountability Measures.....1151
C. Institutionalize Oversight 1154
D. Use Technology as a Way to Protect Privacy, Not Merely Gather Data 1157
VI. Conclusion.....1159

I. Introduction

The revelations about the National Security Agency's surveillance programs have raised significant questions about how government agencies handle sensitive information gathered

* Associate Professor of Law and Public Policy, Pepperdine University; Co-Founder of AirMap. This Essay is adapted from Gregory S. McNeal, *Drones and Aerial Surveillance*, GEO. WASH. L. REV. (forthcoming 2015), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2498116.

through surveillance techniques and other electronic means. As drones become an important tool used by the government, questions will arise about how government agencies store and protect information gathered by drones. This Essay outlines key data retention considerations that government operators of drones should examine.

This Essay makes three key points. First, to address the possibility that drones and other sophisticated aerial surveillance technology will allow the government to build a comprehensive picture of an entire community's daily movements (a different persistent surveillance harm), governments should enact laws mandating data retention procedures that require heightened levels of suspicion and increased procedural protections for accessing stored data gathered by aerial surveillance, coupled with a requirement that data be deleted after a legislatively-mandated period of time.

Second, governments should impose enhanced transparency and accountability measures, requiring agencies to publish on a regular basis information about the use of aerial surveillance devices—both manned and unmanned—and should consider creating local oversight boards to police the use of surveillance technologies.

Third, legal reformers should recognize that technology such as auto-redaction may make aerial surveillance by drones more protective of privacy than human surveillance.

II. Background on Drones

On the Sunday of President's Day weekend, 2015, Secretary of Transportation Anthony Foxx and FAA Administrator Michael Huerta convened a hastily arranged public conference call to announce pending regulations that would allow for the integration of drones into the national airspace. The regulations are historic; for the first time in American history, aircraft operating without onboard pilots would have a regulatory regime to govern their use. Sunday of a holiday weekend was an odd time to announce the most significant aviation-related regulations since the creation of the FAA, but the agency's hand was forced. A little more than twenty-four hours before the conference call, I wrote a column for

Forbes that revealed the details of the pending regulations—the Associated Press and the Wall Street Journal credited the column with first reporting the news that forced the FAA to announce their regulations.[1]

The use of drones for surveillance has to date been a sparsely discussed topic in legal scholarship; the FAA's proposed changes to federal law, however, make it all but certain that drones will be a catalyst for new ways of thinking about privacy and surveillance.[2] This Essay seeks to frame future discussions about how state and local governments will handle the privacy issues associated with aerial surveillance by proposing innovative reforms that move beyond the call for requiring warrants for the use of drones.

The FAA's proposed rule is just the start of a new era in aviation, as it is estimated that 30,000 drones will be flying in the

---

1. *See* Gregory S. McNeal, *Leaked FAA Document Provides Glimpse Into Drone Regulations,* FORBES (Feb. 14, 2015), http://www.forbes.com/sites/gregorymcneal/2015/02/14/the-faa-may-get-drones-right-after-all-9-insights-into-forthcoming-regulations/ (last visited June 23, 2015) (noting "AP and The Wall Street Journal credited this post with first reporting the story about the regulations, which are now out for public comment") (on file with the Washington and Lee Law Review); Jack Nicas, *Federal Document Sheds Light on Proposed Drone Rules*, WALL ST. J. (Feb. 14, 2015), http://www.wsj.com/articles/online-document-sheds-light-on-proposed-drone-rules-1423960620 (last visited June 23, 2015) (acknowledging that the impending regulations were first reported by Forbes) (on file with the Washington and Lee Law Review); Joan Lowy, *FAA Seeking Drone Rules Favorable to Commercial Operators,* ASSOCIATED PRESS (Feb. 14, 2015), http://hosted2.ap.org/APDEFAULT/f70471f764144b2fab526d39972d37b3/Article_2015-02-14-US--FAA-Drones/id-381ad5339b3348d984da077c86a22b25 (last visited June 23, 2015) (noting that the story was first reported by Forbes) (on file with the Washington and Lee Law Review).

2. Technically known as unmanned aerial vehicles or unmanned aircraft systems, this Essay will refer to these devices by their colloquial name—drones. For some of the prescient articles discussing drones or surveillance issues that might touch on drones, see generally M. Ryan Calo, *The Drone As Privacy Catalyst*, 64 STAN. L. REV. ONLINE 29 (2011); David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62 (2013); Margot E. Kaminski, *Drone Federalism: Civilian Drones and the Things They Carry*, 4 CAL. L. REV. CIRCUIT 57 (2013); Troy A. Rule, *Airspace in an Age of Drones*, 95 B.U. L. REV. 155 (2015); Michael L. Smith, *Regulating Law Enforcement's Use of Drones: The Need for State Legislation*, HARV. J. LEGIS. (forthcoming), *available at* http://ssrn.com/abstract=2492374; Andrew B. Talai, *Drones and Jones: The Fourth Amendment and Police Discretion in the Digital Age*, 102 CAL. L. REV. 729 (2014); Wells C. Bennett, *Civilian Drones, Privacy, and the Federal-State Balance*, BROOKINGS (Sept. 2014), http://www.brookings.edu/research/reports2/2014/09/civilian-drones-and-privacy (last visited Oct. 20, 2015) (on file with the Washington and Lee Law Review).

national airspace (NAS) by the end of the decade.[3] But even more drones are coming. According to the FAA, "[O]nce the entire integration process is complete, the FAA envisions the NAS populated with UAS that operate well beyond the operational limits proposed in [the rule announced on February 15, 2015.]"[4]

Drones will be a catalyst for new ways of thinking about privacy and surveillance, but contrary to the hopes of many advocates, the issue of privacy was not addressed in the FAA's proposed rules.[5] Rather, the FAA explicitly stated that matters related to privacy, civil rights, and civil liberties were beyond the

---

3. *The Future of Drones in America: Law Enforcement and Privacy Considerations: Hearing Before the S. Comm. on the Judiciary*, 113th Cong. 2 (2013) (statement of Sen. Patrick J. Leahy, Chairman, S. Comm. on the Judiciary).

4. Operation and Certification of Small Unmanned Aircraft Systems, at 34 (proposed Feb. 15, 2015) (to be codified at 14 C.F.R. pts. 21, 43, 45, 47, 61, 91, 101, 107 & 183) [hereinafter NPRM], https://www.faa.gov/regulations_policies/rulemaking/recently_published/media/2120-AJ60_NPRM_2-15-2015_joint_signature.pdf.

5. *See, e.g.*, Patrice Hendriksen, *Unmanned and Unchecked: Confronting the Unmanned Aircraft System Privacy Threat Through Interagency Coordination*, 82 GEO. WASH. L. REV. 207, 212 (2013) (proposing FAA involvement in an interagency process among UAS federal stakeholders to address privacy); Kellan Howell, *Invasion: 7,500 Drones in U.S. Airspace Within 5 Years, FAA Warns*, WASH. TIMES (Nov. 7, 2013), http://www.washingtontimes.com/news/2013/nov/7/faa-chief-announces-progress-drone-regs/?page=all (last visited June 23, 2015) (on file with the Washington and Lee Law Review); Keith Lain, *Markey: Privacy Before Drone Deliveries*, HILL (Dec. 2, 2013, 10:53 AM), http://thehill.com/policy/transportation/191722-markey-protect-privacy-before-drone-deliveries (last visited June 23, 2015) ("Sen. Ed Markey (D-Mass.) said privacy protections need to be in place before Amazon starts delivering packages with drones.") (on file with the Washington and Lee Law Review); Matthew J. Schwartz, *FAA Promises Privacy Standards For Domestic Drones*, DARK READING (Feb. 15, 2013, 11:39 PM), http://www.darkreading.com/risk-management/faa-promises-privacy-standards-for-domestic-drones/d/d-id/1108691? (last visited June 23, 2015) ("The Federal Aviation Administration Thursday announced that it will publicly develop privacy policies to cover the use of unmanned aerial vehicles (UAVs), more often referred to as drones, in U.S. airspace.") (on file with the Washington and Lee Law Review); Jay Stanley, *New Eyes in the Sky: Protecting Privacy from Domestic Drone Surveillance*, ACLU (Dec. 15, 2011), http://www.aclu.org/blog/national-security-technology-and-liberty/new-eyes-sky-protecting-privacy-domestic-drone (last visited June 23, 2015) ("In the report, we discuss the current drone landscape (technology and use), talk about the privacy issues, and conclude with recommendations for protections we believe must be put in place to ensure they don't destroy our privacy.") (on file with the Washington and Lee Law Review).

scope of their rulemaking.[6] Instead, President Obama directed that those privacy issues related to the federal government's use of drones would be handled according to terms outlined in a Presidential Memorandum, while the issues raised by private uses of drones would be addressed through rules that will be created in a multi-stakeholder process led by the National Telecommunications and Information Administration (NTIA), a subordinate agency of the Department of Commerce.[7]

III. The President's Order Regarding Federal Government Drone Operations

The federal government has taken very little action with regard to data retention procedures for drones. Rather than directing the FAA to promulgate regulations to address privacy, the President instead issued an executive order, styled as an executive memorandum.[8] That memorandum directed the federal

---

6. NPRM, *supra* note 4, at 36.

7. *Id.*; *see* Gregory S. McNeal, *What You Need To Know About The Federal Government's Drone Privacy Rules*, FORBES (Feb. 15, 2015), http://www.forbes.com/sites/gregorymcneal/2015/02/15/the-drones-are-coming-heres-what-president-obama-thinks-about-privacy/ (last visited June 23, 2015) ("The President directed the Department of Commerce's, National Telecommunications & Information Administration (NTIA) to initiate a process for creating privacy, accountability and transparency rules for commercial and private uses of drones.") (on file with the Washington and Lee Law Review); Presidential Memorandum, *Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems*, WHITE HOUSE, § 2(b) (Feb. 15, 2015) [hereinafter Drone Privacy Memo] https://www.whitehouse.gov/the-press-office/2015/02/15/presidential-memorandum-promoting-economic-competitiveness-while-safegua (last visited Oct. 5, 2015) ("Within 90 days of the date of this memorandum, the Department of Commerce, through the National Telecommunications and Information Administration, and in consultation with other interested agencies, will initiate this multi-stakeholder engagement process . . . .") (on file with the Washington and Lee Law Review).

8. On the subtle differences between an Executive Order and other forms of executive action such as presidential memoranda, see John Contrubis, *Executive Orders and Proclamations,* CONGRESSIONAL RESEARCH SERVICE REPORT FOR CONGRESS No. 95-722A (1999)

> Both are undefined, written instruments by which the President directs, and governs actions by, Government officials and agencies. They differ in that executive orders must be published in the Federal Register whereas presidential memoranda are similarly published only

government to create standards for how the federal government will address the privacy issues associated with drones.[9] Under the Order, federal government agencies and some recipients of federal funds will have one year to implement the President's policies and make them publicly available.[10]

The President's memorandum acknowledges that drones "may play a transformative role in fields as diverse as urban infrastructure management, farming, public safety . . . and disaster response."[11] The Order acknowledges that drones are a lower-cost alternative to manned aircraft and can reduce risks to human life.[12] The President's directive takes account of "the privacy, civil rights, and civil liberties concerns these systems may raise."[13] The memorandum segments federal government drone operations from privately operated drones and leaves the matter of state and locally operated drones—except those purchased with federal funds—to be addressed by the states.[14]

The President's order requires agencies to implement the guidelines below and inform the public about how to access their policies by February 15, 2016.[15] The memorandum requires federal agencies to examine their drone policies prior to the adoption of new drone technology and at least every three years thereafter.[16]

---

if the President determines that they have "general applicability and legal effect."

9. *See* Drone Privacy Memo, *supra* note 7 (establishing "transparent principles that govern the Federal Government's use of UAS in the NAS, and to promote the responsible use of this technology in the private and commercial sectors").

10. *See id.* § 1(e) ("Within 1 year of the date of this memorandum, agencies shall publish information on how to access their publicly available policies and procedures implementing this section.").

11. *Id.*

12. *See id.* ("As compared to manned aircraft, UAS may provide lower-cost operation and augment existing capabilities while reducing risks to human life.").

13. *Id.*

14. *See id.* § 1(c) ("[R]equire that State, local, tribal, and territorial government recipients of Federal grant funding for the purchase or use of UAS for their own operations have in place policies and procedures to safeguard individuals' privacy, civil rights, and civil liberties prior to expending such funds.").

15. *Id.* § 1(e).

16. *See id.* § 1(a) ("Accordingly, agencies shall, prior to deployment of new UAS technology and at least every 3 years, examine their existing UAS policies

The memorandum notes that drones must only be used in a manner consistent "with the Constitution, federal law, and other applicable regulations and policies."[17] It also reaffirms that individuals have the right to seek access to, and amendment of, records associated with drone usage.[18]

The President's memorandum also creates new requirements for the collection of information by drones and requires that agencies only collect information "to the extent that such collection or use is consistent with and relevant to an authorized purpose."[19] Information collected by drones that is not maintained in a system of records covered by the Privacy Act shall not be disseminated outside the agency, unless dissemination is required by law or fulfills an authorized purpose and complies with agency requirements.[20] If information collected using drones contains personally identifiable information (PII), that information

> shall not be retained for more than 180 days unless the retention 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.[21]

To address civil liberties, the memorandum mostly references existing laws. Specifically, it calls on agencies to ensure that they have policies to "prohibit the collection, use, retention, or dissemination of data in any manner that would violate the First Amendment" or would illegally discriminate based on protected categories like ethnicity, race, gender, etc.[22] It also mandates that drone-related activities are "performed in a manner consistent

---

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.").

17. *Id.* § 1.

18. *See id.* ("[A]nd permits individuals to seek access to and amendment of records.").

19. *Id.* § 1(a)(ii).

20. *See id.* § 1(a)(iii) ("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.").

21. *Id.* § 1(a)(ii).

22. *Id.* § 1(b)(i).

with the Constitution and applicable laws, Executive Orders, and other Presidential directives."[23] The memorandum requires agencies to ensure that they have in place a means to "receive, investigate, and address, as appropriate, privacy, civil rights, and civil liberties complaints."[24]

Oversight and accountability of Federal drone operations will require creation of new procedures or modification of existing procedures.[25] Agencies will be required to ensure that their oversight procedures "including audits or assessments, comply with existing policies and regulations."[26] Federal government personnel and contractors who work on drone programs will require rules of conduct and training, and procedures will need to be implemented for reporting suspected cases of misuse or abuse of drone technologies.[27]

In a passage particularly relevant to this Essay, the memorandum addresses the matter of drones shared with state and local governments, drones purchased with federal funds, and information gathered by drones that are shared with others. The memorandum directs that such operations must comply with the Executive Order and applicable laws and regulations.[28] If agencies authorize the use of drones in response to requests from federal, state, local, tribal, or territorial government operations, it will need to be conducted pursuant to established policies and procedures.[29] Also, state, local, tribal, or territorial government recipients of federal grant funding for the purchase or use of drones will need to have in place policies and procedures to safeguard

---

23. *Id.* § 1(b)(ii).

24. *Id.* § 1(b)(iii).

25. *See id.* § 1(a) ("Agencies shall update their policies and procedures, or issue new policies and procedures, as necessary.").

26. *Id.* § 1(c)(i).

27. *See id.* § 1(c)(ii) ("[V]erify the existence of rules of conduct and training for Federal Government personnel and contractors . . . establish policies and procedures, or confirm that policies and procedures are in place . . . .").

28. *See id.* § 1(b)(ii) ("[E]nsure that UAS activities are performed in a manner consistent with the Constitution and applicable laws, Executive Orders, and other Presidential directives . . . .").

29. *See id.* § 1(c)(3) ("[E]stablish policies and procedures, or confirm that policies and procedures are in place, to authorize the use of UAS in response to a request for UAS assistance in support of Federal, State, local, tribal, or territorial government operations . . . .").

privacy, civil rights, and civil liberties prior to expending such funds.[30] These are relatively minor changes that do very little to impact most drone operations, as most operations were likely already complying with federal laws and regulations—which, as the subsequent sections of this Essay point out, impose very few restrictions on aerial surveillance.

On transparency, the memorandum takes measures to provide the public with greater information about the federal government's use of drones. The memorandum attempts to balance privacy with national security and law enforcement interests. It requires agencies to provide notice to the public regarding where in the national airspace an agency's drones are permitted to operate.[31] Agencies must also keep the public informed of their drone programs and any changes that would significantly affect privacy, civil rights, or civil liberties.[32] On an annual basis, agencies must also provide a general summary of their drone operations during the previous fiscal year.[33] That summary must "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."[34]

IV. The Need for Action in States and Municipalities Regarding Data Handling Procedures

While the controversy over NSA surveillance techniques raised questions about how the NSA gathered information about targets (and collaterally gathered information about non-targets),

30. *See id.* § 1(c)(vi) ("[R]equire that State, local, tribal, and territorial government recipients of Federal grant funding for the purchase or use of UAS for their own operations have in place policies and procedures to safeguard individuals' privacy, civil rights, and civil liberties prior to expending such funds.").

31. *See id.* § 1(d)(i) ("[P]rovide notice to the public regarding where the agency's UAS are authorized to operate in the NAS . . . .").

32. *See id.* § 1(d)(ii) ("[K]eep the public informed about the agency's UAS program as well as changes that would significantly affect privacy, civil rights, or civil liberties . . . .").

33. *See id.* § 1(d)(iii) ("[M]ake available to the public, on an annual basis, a general summary of the agency's UAS operations during the previous fiscal year . . . .").

34. *Id.*

what was also revealed were the extensive administrative procedures governing the collection, retention, and access to stored data.[35] As state and local governments begin to collect massive amounts of information from drones, it raises significant questions about whether those local governments have the same sophisticated audit and compliance procedures that the federal government claims it has.

Focusing merely on federal rules and federal operations obscures a huge portion of the discussion, as state and local operators will be the government actors most likely to use drones in search and rescue operations and in support of law enforcement activity, like serving a warrant or documenting a crime scene.[36] Similarly, the information gathered from a drone for law enforcement will be stored on law enforcement computers and will be subject to state and local laws governing the handling of personally identifying information and information disclosure.[37]

---

35. *See infra* notes 36–37 and accompanying text (addressing said concerns and the various sources that cover related administrative procedures).

36. *Cf.* MATT LEWIS, MESA CNTY. SHERIFF'S OFFICE, MSCO UNMANNED AIRCRAFT SYSTEM TEAM: FREQUENTLY ASKED QUESTIONS 1 (2014), http://sheriff.mesacounty.us/WorkArea/linkit.aspx?LinkIdentifier=id&ItemID=11383&libID=11401 (last visited Oct. 20, 2015) ("We most often use [UAS] for crime scene photography, and search and rescue missions.") (on file with the Washington and Lee Law Review); *2011–2012 FAA List of Drone License Applicants*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/document/2012-faa-list-drone-applicants (last visited Feb. 25, 2015) (listing drone license applicants, including various federal, state, and educational entities) (on file with the Washington and Lee Law Review); Kevin Bonham, *Grand Forks County Drone Assists at Bemidji Blast Scene*, GRAND FORKS HERALD (Jan. 28, 2015, 6:35 PM), http://www.grandforksherald.com/news/region/3666035-grand-forks-county-drone-assists-bemidji-blast-scene (last visited June 22, 2015) (discussing how a Grand Forks County Sheriff's Department drone assisted in the investigation of a gas explosion that destroyed a house) (on file with the Washington and Lee Law Review); Cyrus Farivar, *San Jose Police Department Says FAA Can't Regulate Its Drone Use*, ARS TECHNICA (Aug. 6, 2014, 2:02 PM), http://arstechnica.com/tech-policy/2014/08/san-jose-police-say-faa-cant-regulate-its-drone-use-faa-disagrees/ (last visited June 22, 2015) (explaining that the San Jose police want to use drones mainly to access potential explosive devices) (on file with the Washington and Lee Law Review); Ed Pilkington, *"We See Ourselves as the Vanguard": The Police Force Using Drones to Fight Crime*, GUARDIAN (Oct. 1, 2014), http://www.theguardian.com/world/2014/oct/01/drones-police-force-crime-uavs-north-dakota (last visited June 22, 2015) (detailing the ways the Grand Forks Sheriff's department has used their drone) (on file with the Washington and Lee Law Review).

37. *See* Stephen Rushin, *The Legislative Response to Mass Police*

Significant law and policy issues will arise at the local level, and it is not clear that local governments are prepared. In fact, state and local governments will be the preeminent battleground for law and policy debates about drones, and it appears they are far behind in crafting rules to handle the data they are about to collect.

V. Data Retention Procedures for Drones

A. Adopt Data Retention Procedures that Require Heightened Levels of Suspicion and Increased Procedural Protections Over Time

Many critics of drones raise the legitimate concern that the government's collection of aerial imagery and video will enable pervasive wide-area surveillance that allows the government to know what all citizens are doing at all points in time. Such warehousing of information may even allow government officials to review footage years after its collection, revealing the most intimate details about a person's life. This is not a problem unique to drones but is rather a recurring theme in critiques of all video and still imagery collection. Legislators should adopt policies that address collection and retention of information in a way that focuses on the information that is collected, how it is stored, and how it is accessed, rather than the particular technology used to collect the information. Thus, while this section speaks specifically about aerial surveillance, the principles articulated here apply to all forms of video and imagery collection.

To protect against pervasive surveillance and warehousing of data about citizens, legislators should enact retention policies and procedures that make it more difficult for the government to access information as time passes. Eventually, information collected by

---

Surveillance, 79 BROOK. L. REV. 1, 53–56 (2013) (discussing the data integrity, access, and privacy of surveillance data collected by police); Corey Ciocchetti, *Just Click Submit: The Collection, Dissemination, and Tagging of Personally Identifying Information*, 10 VAND. J. ENT. & TECH. L. 553, 617 (2008) (overviewing the laws regarding the collection of personally identifying information some states have in place for both state and local agencies and businesses); CAL. GOV'T CODE § 11019.9 (West 2015) (mandating each state agency enact and maintain a permanent privacy policy); COLO. REV. STAT. ANN. § 24-72-502 (West 2014) (requiring each government entity of the state create a privacy policy).

the government should be destroyed at the end of a pre-determined period of time. While the specific duration of time and processes may be subject to debate, all procedures and timelines should be legislatively determined, ensuring that they cannot be modified by individual agencies. To protect the rights of individuals, the information gathered and stored should be exempt from Sunshine Act requests but should be fully discoverable in any criminal prosecution.[38]

A few procedural ideas are outlined below that will form the bulk of any responsible retention procedure:

- From the moment of collection to up to thirty days after collection, information should be treated like any other contemporaneous or near contemporaneous observation. Government agents should be able to monitor aerial surveillance in real time or near real time, just as they observe CCTV's in real time or near real time. This thirty-day window will allow law enforcement to respond to immediate or nearly immediate complaints about violations of the law.
- After thirty days have passed from initial collection, information collected from aerial surveillance should be moved from servers openly accessible by law enforcement to servers that are only accessible with a court order and a showing of reasonable suspicion.
- After ninety days have passed from initial collection, police should not be allowed to access information stored on servers without a court order and a showing of probable cause that the information contained on the servers contains evidence of a crime.
- All information stored on servers should be automatically deleted after a period of time so that the government does not maintain a long-term archive of information about individuals. That period of time may be as short as 120 days but should not be longer than five years.

---

38. Note that while I argue the information gathered should be exempt from Sunshine Act requests, the transparency recommendations below contend that the *fact* of collection and the government's use of aerial surveillance technology should be subject to transparency and accountability reforms and heightened oversight.

As with prior proposals, these limits are general guidelines with inherent policy trade-offs. A jurisdiction may value law enforcement prerogatives over privacy and may choose to place a greater emphasis on having data accessible for longer periods of time without a showing of cause, and consequently might move the thirty-day limit to a sixty-day limit. That decision might enhance the law enforcement value of aerial surveillance data, but it would also impose a civil liberties cost. Such decisions are best calibrated at the local level, where legislatures can gauge their particular crime levels and their constituents' desires for privacy.[39]

B. Adopt Transparency and Accountability Measures

Transparency and accountability measures should be required, regardless of whether legislators follow the recommendations in this Essay or choose to follow the ill-conceived warrant based approach. Transparency and accountability measures may be more effective than suppression rules or warrants for controlling and deterring wrongful government surveillance. To hold law enforcement accountable, legislators should mandate that the use of all aerial surveillance devices—manned or unmanned—be published on a regular basis, perhaps quarterly, on the website of the agency operating the system.

These usage logs should detail who operated the system, when it was operated, where it was operated (including GPS coordinates), and what the law enforcement purpose for the operation was. Legislators may even mandate that unmanned systems operated in their jurisdictions come equipped with software that allows for the easy export of flight logs that contain this information. Such logs will allow privacy advocates and concerned citizens to closely monitor how aerial surveillance

39. I say "might" enhance the law enforcement value because, as the amount of data increases, law enforcement will face challenges analyzing that data. *Cf.* Sandra I. Erwin, *Too Much Information, Not Enough Intelligence*, NAT'L DEF. MAG. (May 2012), http://www.nationaldefensemagazine.org/archive/2012/May/Pages/TooMuchInformation,NotEnoughIntelligence.aspx (last visited June 22, 2015) ("Intelligence experts say the military is drowning in data but not able to convert that information into intelligible reports that break it down and analyze it.") (on file with the Washington and Lee Law Review).

devices are being used, enabling the political process as a mechanism to hold operators accountable.

In circumstances where publishing usage logs may reveal information that is law enforcement sensitive, such as an ongoing investigation, the agency operating the drone may keep their usage logs confidential until the investigation is closed. The agency should be required to make the logs public within thirty days of the close of an investigation. To facilitate public accountability, legislators should mandate that all logs be published in an open and machine-readable format consistent with the President's Executive Order of May 9, 2013.[40]

For evidence that this flight log approach works, one need only look across the Atlantic to the United Kingdom, where many police departments publish their helicopter flight logs on their webpage; in fact, some even live tweet their helicopters' activities.[41] While there is no law in the United Kingdom that specifically requires police departments or law enforcement agencies to publish the flight logs of their helicopters, their version of the Freedom of Information Act appears to be the legislative authority prompting publication of police helicopter logs.[42]

Like the United States, there are a number of public watchdog groups in the United Kingdom that monitor police activity, including groups whose sole purpose is to monitor the activity—and related noise complaints—of police helicopters.[43] These groups, and their respective websites, act as a forum for noise and privacy complaints from various individuals across the Kingdom, and several of these groups organize and lobby Members of

---

40. *See* Barack Obama, *Executive Order—Making Open and Machine Readable the New Default for Government Information*, WHITE HOUSE (May 9, 2013), https://www.whitehouse.gov/the-press-office/2013/05/09/executive-order-making-open-and-machine-readable-new-default-government- (last visited Oct. 8, 2015) (providing an open data policy with directions for implementing the policy) (on file with the Washington and Lee Law Review).

41. *See infra* notes 43–49 and accompanying text (describing these police departments' programs in greater detail).

42. *See, e.g.*, *Issue of Police Helicopter Flights at Night over South Hampstead London NW6 (LB Camden)*, WHATDOTHEYKNOW, http://www.whatdotheyknow.com/request/issue_of_police_helicopter_fligh (last visited Feb. 25, 2015) (providing the results of a FOIA request for information regarding certain police helicopter flights) (on file with the Washington and Lee Law Review).

43. *See, e.g.*, *id.* (same).

Parliament (MPs) to pass legislation restricting helicopter flyovers.[44] These groups, and the advocacy that they generate, appear to be largely responsible for the recent trend of many UK police departments publishing their helicopters' flight logs or creating Twitter accounts for their helicopters that publish real-time or delayed-time updates of the aircrafts' activity.[45]

These helicopter Twitter accounts, which have become a growing trend amongst British police departments, have had an immediate and powerful effect on public relations in their respective jurisdictions. In Islington, the police department went from struggling to handle the overload of noise complaints relating to the department's use of its helicopter to receiving no complaints after the creation of its Helicopter Twitter feed.[46] The Twitter account gained over 7,000 followers within its first few weeks, and the public criticism of police helicopter activity ceased entirely.[47] The department reflected on the effectiveness—as well as future potential—of the Twitter feed by issuing this statement:

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

---

44. *See Early Day Motion 394: Helicopter Flights over London*, UK PARLIAMENT, http://www.parliament.uk/edm/2012-13/394 (last visited Feb. 25, 2015) (proposing legislation to regulate/reduce the amount of noise pollution caused by nighttime police helicopter flyovers in London) (on file with the Washington and Lee Law Review).

45. Not all activity is published. The Cleveland (UK) Police Department's website indicates that: "This page is intended to provide basic information to the general public regarding the work of the police helicopter and will be updated on a daily basis. . . . Please note that not all items are always listed due to operational sensitivity or ongoing investigation." *Helicopter Watch*, CLEVELAND POLICE, http://www.cleveland.police.uk/news/helicopter-watch.aspx (last visited Feb. 25, 2015) (on file with the Washington and Lee Law Review).

46. *See* Jon Dean, *Police Helicopter Twitter Account Stops Islington Complaints*, ISLINGTON GAZETTE (Feb. 12, 2012), http://www.islingtongazette.co.uk/news/police_helicopter_twitter_account_stops_islington_complaints_1_1206725 (last visited June 22, 2015) ("The Air Support Unit (ASU) say objections from Islington residents have dropped to zero since the *Gazette* published details of where and when the helicopters operated.") (on file with the Washington and Lee Law Review).

47. *See id.* ("'We have been staggered by the response to the Twitter account—we have 7,000 followers and it has only been going a few weeks.'").

> was missing in Islington, we could Tweet our followers to keep an eye out.[48]

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

> We hope to use the Twitter feed to highlight the positive work being done by the Air Operations Unit and to keep members of the public informed as to why the helicopter has been deployed. We hope people will enjoy finding out more about the Unit and hopefully our tweets will give some explanation as to why we have been deployed and give some interesting insights into a very important policing tool.[49]

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

C. Institutionalize Oversight

State and local governments may also want to create oversight boards modeled after the federal Privacy and Civil Liberties Oversight Board. The local board could be comprised of appointees drawn from the community. Such a surveillance oversight board

---

48. *Id.*

49. Suffolk Police, *UK's Suffolk Police Helicopter Unit Now on Twitter*, HELIHUB (Sept. 3, 2012), http://helihub.com/2012/09/03/uks-suffolk-police-helicopter-unit-now-on-twitter/ (last visited June 22, 2015) (on file with the Washington and Lee Law Review).

could have a cross-section of civil liberties and law enforcement minded individuals who could conduct audits of surveillance activities. Such audits might include reviewing data that was collected, checking for compliance with accountability procedures, or searching for areas where discriminatory targeting may be occurring.

Independent oversight bodies can provide policymakers with a transparency-oriented means to ensure accountability and expose wrongdoing, but they may also deter wrongdoing.[50] If police departments know that an oversight board will be auditing their activity, it may convince them to live up to the expectations and standards embedded in law.[51] This, of course, assumes that policymakers want to change the status quo, but the amount of drone-related legislation being proposed in various jurisdictions suggests that legislators are in fact interested in making changes.[52] Moreover, the intense public interest in the issue suggests that there are many incentives for elected officials to exercise greater oversight of drone surveillance, as there is substantial interest group advocacy associated with the topic. While legislators may have interest in the topic, they may not have the time or resources to exercise intense oversight. A dedicated oversight board could specialize in overseeing surveillance activities.

There are good reasons to believe that independent oversight of surveillance might be quite successful.[53] As legal scholars Eric Posner and Adrian Vermeule have pointed out, independent commissions can be established to review policies before and after

---

50. For a lengthier discussion of accountability, see generally Gregory S. McNeal, *Targeted Killing and Accountability*, 102 GEO. L.J. 681 (2014).

51. *See* ROBERT D. BEHN, RETHINKING DEMOCRATIC ACCOUNTABILITY 14 (2001) (discussing deterrence).

52. For a discussion of the status quo, see Gregory S. McNeal, *Preventative Detention: The Status Quo Bias and Counterterrorism Detention*, 101 J. CRIM. L. & CRIMINOLOGY 855, 882–83 (2012) (describing the status quo bias in policymaking); *cf.* FRANK R. BAUMGARTNER ET AL., LOBBYING & POLICY CHANGE: WHO WINS, WHO LOSES, AND WHY 43 (2009) ("Even if policy makers recognize that the policy is imperfect or the result of an error, . . . it may still be a hard sell to convince others, especially those in leadership positions, that the current policy is working so badly that it must be overhauled.").

53. *Cf.* McNeal, *supra* note 50, at 785–93 (discussing plausible accountability reforms that could enhance the accountability of the targeted killing process).

the fact, and politicians might gain credibility by binding themselves to give the commissions authority along various dimensions.[54] Policymakers might promise to follow the recommendations of a commission and give power to a commission to review the success of policy choices related to drones.[55] Independent oversight boards can be successful because they signal the interests of politicians in maintaining credibility and winning the support of the public, and a willingness to make information available that could subject the government to criticism.[56] Independent oversight boards allow politicians to claim that they are holding law enforcement accountable, while at the same time shifting the blame for poor accountability decisions to others—ensuring that politicians can exercise oversight without needing to fear blowback from powerful law enforcement unions.[57]

The first challenge associated with such an approach is to ensure that police departments provide surveillance information to the oversight board, which requires the board to be empowered by law. Second, for an oversight board to be successful from the outset, it will require political support. A failure on the part of politicians to empower an oversight board may engender political fallout for the policymakers who established the oversight board, but only if the commissioners have a means to communicate their lack of empowerment. The board, once appointed, may operate as independent investigators who will have an interest in ensuring that they are not stonewalled. Because these members will be appointed by politicians with their own agendas, however, or the board members themselves may have political ambition, the

---

54. *See* ERIC A. POSNER & ADRIAN VERMEULE, THE EXECUTIVE UNBOUND: AFTER THE MADISONIAN REPUBLIC 141 (2010) (discussing independent commissions).

55. *See id.* (same).

56. *Cf.* McNeal, *supra* note 50, at 787 (discussing how reporting requirements for certain information could encourage civilian protection).

57. For a discussion of the power of law enforcement unions, see generally HERVEY A. JURIS & PETER FEUILLE, POLICE UNIONISM: POWER AND IMPACT IN PUBLIC-SECTOR BARGAINING (1973); David Alan Sklansky, *Not Your Father's Police Department: Making Sense of the New Demographics of Law Enforcement*, 96 J. CRIM. L. & CRIMINOLOGY 1209 (2006); Michael Tracey, *The Pernicious Power of the Police Lobby*, VICE (Dec. 4, 2014), http://www.vice.com/read/the-pernicious-power-of-police-unions (last visited June 22, 2015) (on file with the Washington and Lee Law Review).

individuals chosen may have reason to avoid exposing abusive surveillance practices that might create political enemies amongst law enforcement. That reality may temper the success of an independent oversight board, but these challenges are inherent in any form of oversight—for example, local elected judges who approve warrant applications are not immune from these influences.

D. Use Technology as a Way to Protect Privacy, Not Merely Gather Data

Perhaps the biggest problem with a warrant requirement is that it fails to recognize that, someday, surveillance from unmanned aircraft may be more protective of privacy than manned surveillance. Technology continues to evolve at such a rapid pace that it is possible drones and other aerial surveillance technologies may enable targeted surveillance that protects collateral privacy harms, while still allowing for the collection of evidence. Technology can further the goal of privacy by using geofencing to only collect evidence from specific locations and using redaction programming to automatically obscure information—such as faces—at the point of collection.[58] Creative policymakers can embrace technology by writing laws requiring that aerial surveillance devices have systems to protect privacy.

For example, imagine that the police receive a tip about marijuana growing in the backyard of 123 Main Street. They dispatch a helicopter to gather aerial photographs of the 123 Main Street property from an altitude of 700 feet. While the police are overhead photographing 123 Main Street, they look down and see a woman sunbathing in the adjacent property at 125 Main Street. While the inadvertent observation of the woman at 125 Main Street does not violate her Fourth Amendment rights, it will likely be viewed from her perspective as an offensive intrusion that

---

58. *Cf. What is Geofencing?*, TECHOPEDIA [hereinafter *Geofencing*], http://www.techopedia.com/definition/14937/geofencing (last visited Feb. 25, 2015) ("Geofencing is a technology that defines a virtual boundary around a real-world geographical area. In doing so, a radius of interest is established that can trigger an action in a geo-enabled phone or other portable electronic device.") (on file with the Washington and Lee Law Review).

violates her personal expectation of privacy—even if it is not one that society, per Supreme Court jurisprudence, is willing to deem reasonable. But now imagine the same collection scenario, this time conducted by a drone or a camera on a manned helicopter with software that is programmed to protect privacy. Prior to the mission, the aircraft would be instructed to only document the activities ongoing at 123 Main Street. The software could be required to automatically redact any additional information gathered from adjoining properties—such as 125 Main Street, the home of our hypothetical sunbather.[59] Furthermore, legislators could also require that software automatically redact the faces of individuals.[60]

The redaction could be removed at a later date, perhaps after a showing of reasonable suspicion or probable cause (the particular standard to be determined by the legislature) to believe that the auto-redacted person's face is important because they are or were involved in criminal activity. If a state or local government required that aircraft engaged in aerial surveillance be coded for privacy, the rights of the adjacent sunbather and any other inadvertently observed individuals would be protected. If such policies were imposed, society may evolve to the point where drones are mandated when manned flights might place law enforcement officers in a situation where they could be tempted to make unwanted observations of innocent people. Warrant

---

59. *Cf. id.* (defining geofencing and its capabilities); Chris Hackett & Michael Grosinger, *The Growth of Geofence Tools Within the Mapping Technology Sphere*, PDVWIRELESS (Dec. 15, 2014), http://www.pdvwireless.com/the-growth-of-geofence-tools-within-the-mapping-technology-sphere/ (last visited Aug. 10, 2015) ("Geofencing also represents a critical element within telematics hardware and software. It allows system users to draw zones around places of work, customer sites and secure areas.") (on file with the Washington and Lee Law Review).

60. *See* 2seas uav, *3i Movie*, YOUTUBE (Sept. 23, 2014), https://youtube/wHQnpfgvK1o (describing the capabilities of "smart surveillance" technologies); Eric Pfeiffer, *How a Seattle Programmer Used Public Records Laws to Push Police to Fix a Surveillance Video Tech Headache*, GOV'T EXEC. (Jan. 8, 2015), http://www.govexec.com/state-local/2015/01/seattle-police-camera-video-redaction/102483/ (last visited June 22, 2015) ("We can use a software program to transcribe and remove audio. It would really deal with the privacy issues. I wrote a simple script that looks for and is able to properly remove the personal information exactly how they do it by hand. It's very precise.") (on file with the Washington and Lee Law Review).

requirements do little to allow this type of privacy protective technology to develop; they merely act as a soft ban on drones.

VI. Conclusion

This Essay argues that state and local governments will need to address data retention issues related to drones. It argues that governments should enact laws mandating data retention procedures that require heightened levels of suspicion and increased procedural protections for accessing stored data gathered by aerial surveillance, coupled with a requirement that data be deleted after a legislatively mandated period of time.[61] Second, governments should impose enhanced transparency and accountability measures, requiring agencies to publish information about the use of aerial surveillance devices—both manned and unmanned—on a regular basis and should consider creating local oversight boards to police the use of surveillance technologies.[62] Third, cities should institutionalize oversight and auditing procedures.[63] Fourth, legal reformers should recognize that technology such as auto-redaction may make aerial surveillance by drones more protective of privacy than human surveillance.[64]

---

61. *See supra* Part V.A (setting forth this argument).

62. *See supra* Part V.B (outlining these methods of achieving transparency and accountability).

63. *See supra* Part V.C (advising municipalities on this matter).

64. *See supra* Part V.D (describing how technology could work to actually protect citizens' privacy).