SILVERMCKENNA
The Internet and Privacy Law Group of STSW

SILVERMAN|THOMPSON|SLUTKIN|WHITE
ATTORNEYS AT LAW

26th Floor
201 North Charles Street
Baltimore, Maryland 21201

Anne T. McKenna, Group Chair
www.silvermckenna.com
Main Phone: 410-385-2225
Direct Dial: 443-909-7496
Fax: 410-547-2432
amckenna@silvermckenna.com

LEGAL MEMORANDUM

Legal Analysis of UAV-Collected Data: Notice, Retention, Use

TO: **The Police Foundation and the U.S. Department of Justice – COPS Office**

FROM: **Anne T. McKenna, Esquire**
Silverman|Thompson|Slutkin|White|LLC

DATE: **May 21, 2014; edited July 14, 2014**

RE: ***Community Policing and UAS Guidelines to Enhance Community Trust***
2013-CK-WX-K002
Legal Analysis of UAV-Collected Data: Notice, Retention, Use

MEMORANDUM OVERVIEW

This legal memorandum has been drafted pursuant to the principal legal consultant contract entered into between The Police Foundation and Anne T. McKenna to provide legal analysis and memoranda to be used by the Police Foundation, its Project Advisory Group, and the U.S. Department of Justice – COPS Office in the project entitled "*Community Policing and UAS Guidelines to Enhance Community Trust*" (the "COPS Contract"). Pursuant to the COPS Contract Task 1 (detailed description of work appended to the COPS Contract), this memorandum ("Legal Analysis of UAV-Collected Data Practices") provides legal analysis of questions and concerns surrounding UAS/UAV-gathered electronic data, including: potentially applicable legislation; data collection; data retention; preservation of evidence; data sharing with other law enforcement; and permissible and impermissible uses of such data.

This Memo, Legal Analysis of UAV-Collected Data Practices, is structured as follows:

I. UAS-Gathered Electronic Data: Subject Introduction

****

I. UAS-GATHERED ELECTRONIC DATA: SUBJECT INTRODUCTION

Domestic law enforcement agencies lawfully use a myriad of electronic devices to collect electronic data about citizens. Such devices include video surveillance systems in public spaces,

GPS tracking devices,[1] and automatic license plate readers,[2] as well as devices that collect fingerprints and other biometric identifiers such as iris scans and face recognition technology.[3]

Unfortunately, little guidance exists as to how law enforcements agencies should collect, store, use and share such electronic data.[4]

The lack of legislative regulation and policy guidance is cause for concern for law enforcement agencies and for privacy advocates, but this concern is heightened and compounded when such surveillance technologies are harnessed aboard UAVs. Setting the question of UASs/UAVs aside, concerns over indiscriminate and unlimited surveillance by law enforcement and the increasingly vast amount of electronic data that result from such surveillance have been voiced in a variety of contexts. Justice Sonia Sotomayor recently shared these concerns in her concurrence to *US v. Jones*, the Supreme Court's 2012 decision on GPS monitoring:

> Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse. The net result is that GPS monitoring--by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track--may 'alter the relationship between citizen and government in a way that is inimical to democratic society.'[5]

Because UAS/UAV can be equipped with GPS tracking technology, as well as video-recording and facial-recognition technology, the monitoring capacities of UAS/UAV thus are equally susceptible, if not more, to facilitating the limitless data collection Justice Sotomayor apprehends.

In this Memo, we analyze these legal issues and provide an overview of laws and policies that may apply to law enforcement use of UASs/UAVs. Specifically, we focus upon recommendations for data gathered by Automatic License-Plate Recognition (ALPR) technology and biometric identification technology, because these recommendations for data gathered by use of these technologies provide useful analogy to potential UAS/UAV data collection. We use the term "recommendations" because the federal government, as well as most states and localities,

---

[1] *See, e.g., United States v. Jones*, 132 S. Ct. 945 (2012)
[2] Stephen Rushin, *The Judicial Response to Mass Police Surveillance*, U. Ill. J.L. Tech. & Pol'y, Fall 2011, at 281, 286-87
[3] Sabrina A. Lochner, *Saving Face: Regulating Law Enforcement's Use of Mobile Facial Recognition Technology & Iris Scans*, 55 Ariz. L. Rev. 201, 202 (Spring 2013).
[4] *Id.* at 202-203.
[5] *United States v. Jones*, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring) (quoting United States v. Cuevas-Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring)).

have done little or nothing to regulate the rapidly expanding use of such technologies when deployed via UASs.[6]

II. POTENTIALLY APPLICABLE LEGISLATION

At present, no federal legislation *explicitly* regulates UAS/UAV-gathered electronic data, and little regulation exists under state law.[7] However, depending on (1) how surveillance is conducted via UAS, (2) what type of surveillance technology is utilized, and (3) what data is collected, there are potentially applicable laws as well as promulgated guidelines. We have set these federals laws forth in this section and then discuss these laws in more detail throughout Data Collected via UAVs Memo where context appropriate. Subpart D of this section discusses an example of legislation emerging at the state level to regulate UAS/UAV data collection.

A. The Privacy Act of 1974

The Privacy Act of 1974, P.L. 93-579, § 2, 88 Stat. 1896, is 40-year-old Watergate reform legislation critically in need of an overhaul. The Privacy Act seeks to ensure that individual records are disclosed and used only for a "necessary and lawful purpose."[8] Section 552a(b) of the Privacy Act enumerates a series of specific conditions under which disclosure is permissible.[9] In the absence of consent by the individual, federal agencies cannot disclose an individual's records protected by the Privacy Act to any person or any agency unless one of these specific conditions are met.[10]

B. The E-Government Act

The E-Government Act of 2002, Pub.L. 107–347, 116 Stat. 2899, 44 U.S.C. § 101, H.R. 2458/S. 803, requires federal agencies to conduct "Privacy Impact Assessments" (PIAs) prior to "developing or procuring IT systems or projects that collect, maintain or disseminate information in identifiable form from or about members of the public."[11] A PIA must analyze what information is collected; when, how, and why this information is collected; disclosure and security of collected information; and "should address the impact the system will have on an

[6] Stephen Rushin, *The Judicial Response to Mass Police Surveillance*, U. Ill. J.L. Tech. & Pol'y, Fall 2011, at 281, 286-87 (noting that legislative regulation of indiscriminate data collection by ALPR does exist in New Hampshire and Maine, but remains generally unregulated nationwide).
[7] See Sect. III.D. for an example of state legislation.
[8] Privacy Act of 1974, Congressional Findings and Statement of Purpose, Act of Dec. 31, 1974, P.L. 93-579, § 2, 88 Stat. 1896.
[9] 5 U.S.C. § 552(a)(b).
[10] 5 U.S.C. § 552(a)(b).
[11] Memorandum from Joshua B. Bolten, Director, Office of Mgmt. and Budget to Heads of Executive Departments and Agencies, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002* (Sept. 26, 2003), available at http://www.whitehouse.gov/omb/memoranda/m03-22.html; Jeremy Brown, Pan, Tilt, Zoom: Regulating the Use of Video Surveillance of Public Places, 23 Berkeley Tech. L.J. 755, 781 (2008).

individual's privacy."[12] However, this provides little in the way of substantive regulation or guidance on issues related to the actual implementation of such technology.

Section 208 of the E-Government Act requires careful consideration: Section 208 establishes Government-wide requirements for conducting, reviewing, and publishing PIAs. The Department of Defense (DOD) provides some helpful guidance in the use of new Information Technology (IT) systems, although DOD's guidance is directed to DOD-affiliated agencies or "components." As summarized by the Defense Logistics Agency (DLA), Section 208 of the E-Government Act requires DOD components:

> [T]o conduct reviews of how privacy issues are considered when purchasing or creating new Information Technology (IT) systems or when initiating new electronic collections of information in personally identifiable form. A PIA addresses privacy factors for all new or significantly altered Information Technology (IT systems or projects that collect, maintain, or disseminate personal information from or about members of the public - excluding information on DoD personnel). The OMB government-wide guidance directs all federal agencies, including the Department of Defense, to conduct PIAs on a slightly broader category of individuals, i.e., including contractors. Therefore, the DLA guidance mirrors the OMB government-wide guidance and adheres to this standard.[13]

Given that UASs/UAVs are "IT systems or projects that collect, maintain, or disseminate personal information from or about members of the public," the E-Government Act provides useful guidance for non-federal domestic law enforcement in terms of conducting PIAs before implementing a UAS program, and it also provides useful guidance in terms of data collection and interagency data sharing.

C. Title III of the Omnibus Crime Control and Safe Streets Act (the "Wiretap Act")

Title III of the Omnibus Crime Control and Safe Streets Act (the "Wiretap Act")[14] is instructive with regards to UAV/UAS surveillance that utilizes audio- or video-recording devices. The ABA Standards on Technologically-Assisted Physical Surveillance, while not legally binding, also provide useful guidance on this topic.[15] The following sections will review the applicability of existing federal legislation and legal principles to UAS/UAV-gathered

[12] Id.
[13] Def. Logistics Agency, *E-Government Act of 2002 (Privacy Impact Assessments)*, http://www.dla.mil/foia-privacy/Pages/eGovernment.aspx (last visited May 20, 2014).
[14] 18 U.S.C. §§ 2510-2522.
[15] American Bar Association, *Standards for Criminal Justice-Electronic Surveillance* (3d ed.), Section B: Technologically-Assisted Physical Surveillance (hereafter ABA Standards).

electronic data in terms of issues related to data collection, data retention, and data use and disclosure.

D. State Legislative Example

Some examples of regulation of UAS/UAV-gathered electronic data have emerged at the state level in recent years.[16] The most specific example of state legislation targeting UAS/UAV surveillance by law enforcement is Illinois's "Freedom from Drone Surveillance Act."[17] The Act explicitly addresses police surveillance and data collection via UAS/UAV, stating that "a law enforcement agency may not use a drone to gather information."[18] Information is defined by the Act as "any evidence, images, sounds, data, or other information gathered by a drone."

The Act's general ban on law enforcement agencies' use of UAS/UAV to gather information is subject to five specific exceptions. Agencies may use UAS/UAV:

(1) In response to terrorist threats;

(2) After first obtaining a search warrant;

(3) For a period of 48 hours during emergency situations;

(4) To locate a missing person, if such activity is separate from a criminal investigation; and

(5) To photograph crime scenes and traffic crashes, provided that the scope of such photography is sufficiently limited.[19]

Retention and disclosure of UAS/UAV-gathered information is explicitly limited under the Act. Where a law enforcement agency deploys UAS/UAV pursuant to one of these authorized uses, "the agency within 30 days shall destroy all information gathered by the drone."[20] Agency supervisors are granted limited authority to retain information beyond 30 days "if (1) there is reasonable suspicion that the information contains evidence of criminal activity, or (2) the information is relevant to an ongoing investigation or pending criminal trial."[21] The authority to disclose this information is also granted solely to agency supervisors, who can share information

[16] For a more comprehensive overview of current state regulation of UAS/UAV use, see the Police Foundation's State Legislation Memorandum and this Firm's State Legislation Chart summarizing and depicting state laws and municipal ordinances pertaining to or proscribing UAS use in general and with respect to law enforcement use.
[17] S.B. 1587, 98th Gen. Assemb., Reg. Sess. (Ill. 2013), *available at* http://www.ilga.gov/legislation/fulltext.asp?DocName=&SessionId=85&GA=98&DocTypeId=SB&DocNum=1587&GAID=12&LegID=72407&SpecSess=&Session=.
[18] S.B. 1587.
[19] Id.
[20] Id.
[21] Id.

with another government agency only when the information contains evidence of criminal activity or is relevant to an ongoing investigation or criminal trial.[22]

Information obtained by law enforcement use of UAS/UAV in violation of the Act is inadmissible in judicial and administrative proceeding.[23]

III. ILLUSTRATIVE TECHNOLOGY-USE GUIDELINES: PLATE READERS AND BIOMETRIC ID

A. Automatic License Plate Recognition (ALPR) Technology

The privacy and data retention concerns raised by ALPR technology are similar to those raised by UAS/UAV surveillance, particularly with respect to the specter of indiscriminate collection and limitless retention of data pose by both technologies. Law enforcement agencies are increasingly utilizing ALPR systems to track vehicle movements. ALPRs can be mounted on patrol cars, toll booths, and along access roads, and the systems are capable of rapidly recording vast amounts of data about the movements of both criminal and innocent citizens.[24] Despite the apparently widespread use of ALPRs and the potential for limitless data retention and aggregation, this technology is largely unregulated. Self-imposed data retention policies vary widely. For example, the Drug Enforcement Agency (DEA) retains ALPR-collected data for up to two years and shares this information with other federal agencies and local police.[25] The New York State Police retains ALPR-collected data indefinitely.[26]

In 2009, the International Association of Chiefs of Police (IACP) published its Privacy Impact Assessment Report for the Utilization of License Plate Readers.[27] The report recognized the lack of uniform rules or guidelines governing the appropriate use and sharing of ALPR data and noted that "potential misuse of LPR data may expose agencies operating such systems to civil liability and negative public perceptions."[28] In light of these concerns, IACP's goal for the report was to identify "the impact LPR systems can have on the public's privacy interests and to make recommendations for the development of information management policies intended to

[22] Id.
[23] Id.
[24] Hilary Hylton, License-Plate Scanners: Fighting Crime or Invading Privacy?, TIME (July 30, 2009), available at http://content.time.com/time/nation/article/0,8599,1913258,00.html.
[25] G. W. Schulz, "DEA Installs License-plate Recognition Devices Near Southwest Border," Ars Technica, July 11, 2012, available at http://arstechnica.com/tech-policy/2012/07/dea-installs-license-plate-recognition-devices-near-southwest-border/.
[26] Cyrus Farivar, "Your Car, Tracked: The Rapid Rise of License Plate Readers," Ars Technica, September 27, 2012, available at http://arstechnica.com/tech-policy/2012/09/your-car-tracked-the-rapid-rise-of-license-plate-readers/.
[27] International Association of Chiefs of Police, Privacy impact assessment report for the utilization of license plate readers (2009), available at http://www.theiacp.org/Portals/0/pdfs/LPR_Privacy_Impact_Assessment.pdf (hereafter IACP Report).
[28] IACP Report at 1.

govern an agency's operation of a LPR system."[29] The report suggested that LPR data can be appropriately accessed to conduct crime analysis, to alert officers of the location of a license plate that has been included on a "hot list," and to detect criminal conduct.[30] Sharing of LPR data may be appropriate among law enforcement agencies; other, non-law enforcement government entities; and with the public in specific, limited circumstances.[31] IACP recommends that data retention policies should consider issues including:

- Statutes of limitation
- Potential future usefulness of the data
- Sensitivity of the data
- The system's technologically implemented policy controls.[32]

The IACP report emphasizes that, while there is no standard formula for determining retention policies, it is critical that a standard policy is established and followed.[33]

Undersigned counsel recommends that data retention policies also specify:

- Retention period: Length of data retention
- Data storage: how data is stored, secured and protected
- Access: who may access the retained data and under what circumstances
- Use: for what purposes may the data lawfully be used
- Disclosure: to what other persons or agencies may the data be disclosed

B. Biometric Identification Technology

Recommendations for police use of biometric identification technology are instructive for UAS/UAV use, particularly because UAS/UAV can be equipped with biometric identification technology, including facial recognition technology. A prominent example of this technology is the Mobile Offender Recognition and Information System ("MORIS"). MORIS is a smartphone-based mobile device capable of identifying individuals via facial recognition technology, iris scans, and fingerprints.[34] When used with an iPhone, the device can photograph an individual's face and check the image against a criminal records database maintained by the device's manufacturer.[35] MORIS does not presently store these images, but there is nothing preventing

[29] IACP Report at 1.
[30] Id at 3.
[31] Id.
[32] Id at 4.
[33] Id.
[34] See Sabrina A. Lochner, Saving Face: Regulating Law Enforcement's Use of Mobile Facial Recognition Technology & Iris Scans, 55 Ariz. L. Rev. 201, 202 (2013).
[35] Zach Howard, Police to Begin iPhone Iris Scans Amid Privacy Concerns, Reuters (July 20, 2011, 2:59 PM).

this in the future.[36] MORIS is reportedly employed by more than 50 law enforcement agencies nationwide, but there is a concerning lack of regulation regarding how officers should collect, retain, use and disclose data with this device.[37]

One law review article identifies a troubling distinction between stationary surveillance devices, such as ALPR and video cameras attached to fixed locations, and mobile surveillance devices, such as MORIS or UAVs. The mobility of a surveillance device permits police discretion in whom to scan or record, which can produce discriminatory surveillance results.[38]

IV. DATA COLLECTION VIA UAS/UAV

Law enforcement collection[39] of electronic data via surveillance devices deployed on UAS/UAV must address four principal concerns:

(1) where the data collection takes place;

(2) what kind of data is being collected;

(3) how much data is collected; and

(4) from whom is the data being collected.

The following subsections address each of these concerns.

A. Where UAS/UAV Data Collection Takes Place

As discussed in Legal Memo #1, the Fourth Amendment does not require law enforcement to obtain a search warrant before installing and utilizing video equipment and cameras to record activities exposed to the public and visible to the naked eye.[40] The area under

[36] Sabrina A. Lochner, Saving Face: Regulating Law Enforcement's Use of Mobile Facial Recognition Technology & Iris Scans, 55 Ariz. L. Rev. 201, 225 (2013).
[37] Sabrina A. Lochner, Saving Face: Regulating Law Enforcement's Use of Mobile Facial Recognition Technology & Iris Scans, 55 Ariz. L. Rev. 201, 202 (2013)
[38] Sabrina A. Lochner, Saving Face: Regulating Law Enforcement's Use of Mobile Facial Recognition Technology & Iris Scans, 55 Ariz. L. Rev. 201, 218-19 (2013).
[39] This section addresses only *data collection* issues. Data retention is addressed in Section III and Section V. Data use is addressed in Section V as well.
[40] *See, Dow Chem. Co. v. United States*, 476 U.S. 227, 239, 106 S. Ct. 1819, 1827, 90 L. Ed. 2d 226 (1986) (holding that aerial surveillance from navigable airspace does not violate the Fourth Amendment); *California v. Ciraolo*, 476 U.S. 207, 213, 106 S.Ct. 1809, 90 L.Ed.2d 210 (1986) ("The Fourth Amendment protection of the home has never extended to require law enforcement officers to shield their eyes when passing by a home on public thoroughfares.").

surveillance must be visible from a lawful vantage point,[41] and the surveillance must record only what passersby could otherwise observe.[42]

B. What Kind of Data is Collected by UAS/UAV Surveillance

Law enforcement surveillance operations that employ UAS/UAV equipped with audio- or video-recording capabilities may be subjected to regulation by Title III of the Wiretap Act if the data collected includes wire or oral communications protected by that Act. Determining whether UAS/UAV surveillance falls within the scope of Title III requires a two-step inquiry. First, the agency must determine whether the surveillance technology is capable of intercepting wire, oral or electronic communications. Section 2510 defines "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device."[43] Second, the agency must determine whether the surveillance technology may intercept communications protected by Title III. An "oral communication" within the scope of Title III is defined as a communication "uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectations."[44] In other words, the speaker must have a "reasonable expectation of privacy" in the conversation in order to constitute an "oral communication" protected by Title III.[45] Thus, UAS/UAV surveillance equipped with technology capable of audio-recording private conversations is subject to Title III.

Where UAS/UAV surveillance intercepts and records protected wire or oral communications, officers must obtain surveillance authorization pursuant to Title III. Unauthorized collection of such protected data is a violation of Title III, for which exclusionary sanctions and other penalties may result.[46]

It is important to note that law enforcement use of video surveillance is not, to date, explicitly regulated by federal statute. Courts have suggested that Title III of the Wiretap Act may nevertheless be implicated in such activity, specifically due to audio-recording capabilities of video surveillance and generally in light of underlying public policy of the Act.[47] Title III

---

[41] *California v. Ciraolo*, 476 U.S. 207, 213, 106 S.Ct. 1809, 90 L.Ed.2d 210 (1986).
[42] *United States v. Jackson*, 213 F.3d 1269, 1281 (10th Cir. 2000) cert. granted, judgment vacated on other grounds, 531 U.S. 1033, 121 S. Ct. 621, 148 L. Ed. 2d 531 (2000) (noting that video cameras installed on public telephone poles "were incapable of viewing inside the houses, and were capable of observing only what any passerby would easily have been able to observe.").
[43] 18 U.S.C. § 2510(4).
[44] 18 U.S.C. § 2510(2).
[45] *United States v. Harrelson*, 754 F.2d 1153, 1170 (5th Cir. 1985)
[46] 18 U.S.C. § 2511
[47] *See United States v. Nerber*, 222 F.3d 597, 604-05 (9th Cir. 2000) ("Although no federal statute regulates the government's use of video surveillance, the existence of a law which prohibits the warrantless use of audio surveillance on a citizen alone in another person's hotel room is strong evidence that society is not prepared to accept the warrantless use of an even more intrusive investigative tool in the same situation.").

likely does not govern silent video camera surveillance.[48] However, where video camera surveillance collects both visual and audio data, the audio portion of the surveillance may constitute interception of wire and oral communications under Title III.[49] Courts have suggested that, as long as officers conduct video surveillance in conformity with Title III requirements, they have complied with the Fourth Amendment warrant clause as well.[50]

C. How Much Data is Collected by UAS/UAV

Law enforcement should ensure that UAS/UAV data collection is sufficiently limited in scope. The Supreme Court has suggested that the Fourth Amendment universally requires a reasonably limited scope for surveillance activity.[51] Pervasive and limitless UAV/UAS surveillance and data collection thus may violate the Fourth Amendment due to its unreasonably broad scope.

Title III of the Wiretap Act explicitly requires surveillance to be limited in scope. Where Title III regulates UAS/UAV surveillance, law enforcement must "minimize the interception of communications not otherwise subject to interception" or otherwise outside of the scope of authorization.[52] The American Bar Association's Standards on Technologically-Assisted Physical Surveillance also indicates that the "scope of the surveillance should be limited to its authorized objectives and be terminated when those objectives are achieved."[53]

D. From Whom is Data Collected by UAS/UAV

Law enforcement must avoid discriminatory collection of data by UAS/UAV. Searches and seizures based on racial discrimination may violate the Equal Protection Clause of the Fourteenth Amendment.[54] The ABA Standards also indicates that "subjects of the surveillance should not be selected in an arbitrary or discriminatory manner."[55] Research on the United Kingdom's video surveillance system revealed bias against minorities and "massively disproportionate targeting of young males, particularly if they are black or visibly identifiable as having subcultural

[48] *U.S. v. Larios*, 593 F.3d 82, 90 (1st Cir. 2010); *U.S. v. Jackson*, 213 F.3d 1269, 1280 (10th Cir. 2000), cert. granted, judgment vacated on other grounds, 531 U.S. 1033, 121 S. Ct. 621, 148 L. Ed. 2d 531 (2000); *U.S. v. Taketa*, 923 F.2d 665, 675 (9th Cir. 1991)
[49] *United States v. Torres*, 751 F.2d 875, 885 (7th Cir. 1984).
[50] *United States v. Torres*, 751 F.2d 875, 885 (7th Cir. 1984) ("If the government conducts television surveillance in conformity with the requirements of particularity that Title III imposes on electronic eavesdropping (not literal conformity, of course, since words such as "communications" and "intercept" in Title III do not fit television surveillance), the government has also conformed to the requirement of particularity in the Fourth Amendment's warrant clause.").
[51] *Terry v. Ohio*, 392 U.S. 1, 17-19, 88 S. Ct. 1868, 1878, 20 L. Ed. 2d 889 (1968) ("This Court has held in the past that a search which is reasonable at its inception may violate the Fourth Amendment by virtue of its intolerable intensity and scope.").
[52] 18 U.S.C. § 2518(5)
[53] ABA Standards, supra note 5.
[54] *Whren v. United States*, 517 U.S. 806, 813, 116 S. Ct. 1769, 1774, 135 L. Ed. 2d 89 (1996)
[55] ABA Standards, supra note 5.

affiliations."[56] The potential for discriminatory targeting may be inherent to such large-scale public surveillance operations, and law enforcement must take proper steps to prevent such unlawful conduct.

V. UAS/UAV DATA PRACTICES: NOTICE; RETENTION; AND USE

A. Notice of Surveillance

Law enforcement conducting surveillance via UAS/UAV may also be required to provide notice of the surveillance. Where surveillance is conducted pursuant to judicial authorization, both Title III of the Wiretap Act and the ABA Standards indicate that post-surveillance notification must be given to all individuals listed on the warrant application for communication surveillance.[57] Where crime deterrence is the primary goal, pre-surveillance notification will not only help further that goal but also minimize potential unexpected intrusions on privacy.[58] The ABA Standards also recommend giving such pre-surveillance notice.[59]

B. Data Retention

In light of technological advances that have facilitated low-cost, high-volume storage data, both courts and legal commentators have expressed concern over the lack of regulations on surveillance data retention.[60] A federal judge for the Ninth Circuit Court warned of GPS tracking capability to "create a permanent electronic record that can be compared, contrasted and coordinated to deduce all manner of private information about individuals. By holding that this kind of surveillance doesn't impair an individual's reasonable expectation of privacy, the panel hands the government the power to track the movements of every one of us, every day of our lives."[61]

As one commentator has noted, in the absence of meaningful regulation "law enforcement is arguably incentivized to take advantage of the declining costs of storage by creating 'digital dossiers' to aid in future investigations."[62] The D.C. Circuit Court recognized that "[a] reasonable person does not expect anyone to monitor and retain a record of every time he drives

---

[56] Clive Norris & Gary Armstrong, *The Maximum Surveillance Society: The Rise of CCTV* 212-14 (1999), at 50; Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 Miss. L.J. 213, 298-99 (2002).
[57] 18 U.S.C. § 2518(8)(d); ABA Standards, supra note 18.
[58] Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 Miss. L.J. 213, 297-98 (2002).
[59] ABA Standards, supra note 5.
[60] Stephen Rushin, *The Judicial Response to Mass Police Surveillance*, U. Ill. J.L. Tech. & Pol'y, Fall 2011, at 281, 291.
[61] *United States v. Pineda–Moreno*, 617 F.3d 1120, 1125 (C.A.9 2010) (Kozinski, C.J., dissenting from denial of rehearing en banc).
[62] Stephen Rushin, *The Judicial Response to Mass Police Surveillance*, U. Ill. J.L. Tech. & Pol'y, Fall 2011, at 281, 291.

his car, including his origin, route, destination, and each place he stops and how long he stays there; rather, he expects each of those movements to remain 'disconnected and anonymous.'"[63]

Notably, one manufacturer of facial recognition technology recommended "reasonable uses principles" for its systems, which included a "No Match-No Memory" practice "to ensure that no audit trail is kept of faces that do not match a known criminal or a person under active police investigation." The manufacturer further advised that "[n]on-matches should be purged instantly."[64]

The Freedom from Drone Surveillance Act, passed by the Illinois state legislature in 2013, provides an example of recommended data retention and data use practices.[65] As discussed in Section II of this memo, the Act prohibits retention of information gathered by law enforcement via UAS/UAV beyond 30 days, unless the information contains evidence of criminal activity or is relevant to an ongoing criminal investigation or trial.[66] Information gathered by UAS/UAV may not be disclosed under the Act unless it meets the same criteria for retention beyond 30 days.[67]

i. Preservation of evidence

Given the absence of meaningful regulation on the retention of electronic data collected by electronic surveillance, the primary concern for law enforcement in this context is data security and preservation of evidence.

Title III of the Wiretap Act requires that authorized recordings of intercepted communications must be protected from editing or alterations and sealed under judicial order.[68] Custody of the recordings is directed by judicial order and the records must be kept for ten years, unless court order directs otherwise.[69]

ii. Data Breach Laws

[63] *United States v. Maynard*, 615 F.3d 544, 563 (D.C. Cir. 2010) (quoting *Nader v. Gen. Motors Corp*., 255 N.E.2d 765, 772 (N.Y. 1970) (Breitel, J., concurring))), cert. granted sub nom. *United States v. Jones*, 131 S. Ct. 3064 (2011) (No. 10-1259).
[64] Marc Jonathan Blitz, *Video Surveillance and the Constitution of Public Space: Fitting the Fourth Amendment to A World That Tracks Image and Identity*, 82 Tex. L. Rev. 1349, 1473 (2004) (citing recommended "reasonable use principles" issued by Visionic, a manufacturer of facial recognition technology).
[65] S.B. 1587 (Ill. 2013). For a more detailed discussion of The Freedom from Drone Surveillance Act, see Section II of this memo.
[66] S.B. 1587.
[67] S.B. 1587 ("[T]he agency shall not disclose any information gathered by the drone, except that a supervisor of that agency may disclose particular information to another government agency, if (1) there is reasonable suspicion that the information contains evidence of criminal activity, or (2) the information is relevant to an ongoing investigation or pending criminal trial.").
[68] 18 U.S.C. § 2518(8)(a).
[69] 18 U.S.C. § 2518(8)(a).

At present, no universally applicable federal law regulates data breach notification. State-level regulation, however, is widespread. Currently, forty-six states and the District of Columbia impose notification requirements for breaches of personal information data.[70] Several of these state laws exempt government agencies from complying with notification requirements, directing application to "businesses" or "persons."[71] Other state laws, importantly California's Security Breach Information Act,[72] *do* apply to "agencies." However, several states that require government agencies to notify individuals of data breaches also specifically exempt these agencies from being punished for non-compliance.[73]

In the absence of a state data breach law that applies to and is enforceable against government agencies, constitutional privacy rights may provide grounds for recovery of damages due to government data breach. The Supreme Court has suggested the possibility of "a threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files."[74] One legal commentator has suggested that a government data breach which violates the right to informational privacy could give rise to a section 1983 claim against the state or a *Bivens* action against the officer.[75] The likelihood of success with either approach is low, however, as the Supreme Court has established several doctrines regarding these claims that create significant obstacles to recovery.[76]

In addition to applicable state law on data breach, three federal statues provide useful guidelines for law enforcement agencies in developing data security and breach notification policies. The Privacy Act of 1974 and the E-Government Act of 2002 require federal agencies to protect and ensure the security of personal information.[77] The Federal Information Security

[70] See Reid J. Schar and Kathleen W. Gibbons, Complicated Compliance: State Data Breach Notification Laws, BLOOMBERG (Aug. 9, 2013), available at http://www.bna.com/complicated-compliance-state-data-breach-notification-laws/.
[71] For example, Connecticut, Georgia, Maryland, Montana, North Dakota, Texas, and Utah's statutes define breach with this language. Conn. Gen. Stat. Ann. §36a-701b(b) (West Supp. 2009); Ga. Code Ann. §10-1-911(2) (2009); Md. Code Ann., Com. Law § 14-3501 (2008); Mont. Code. Ann. §30-14-1704(1) (2009); N.D. Cent. Code. §51-30-02 (2007); Tex. Bus. & Com. Code Ann. §521.053(a) (Vernon Supp. 2009); Utah Code Ann. §13-33-202 (2005). See Jill Joerling, Data Breach Notification Laws: An Argument for A Comprehensive Federal Law to Protect Consumer Data, 32 Wash. U. J.L. & Pol'y 467, 476 (2010).
[72] California Security Breach Information Act §1798.29.
[73] See Jill Joerling, Data Breach Notification Laws: An Argument for A Comprehensive Federal Law to Protect Consumer Data, 32 Wash. U. J.L. & Pol'y 467, 476 (2010) (identifying Florida, Hawaii, Maine, and Tennessee as specifically excluding government agencies from enforcement proceedings).
[74] Whalen v. Roe, 429 U.S. 589, 605, 97 S. Ct. 869, 879, 51 L. Ed. 2d 64 (1977)
[75] A. Michael Froomkin, Government Data Breaches, 24 Berkeley Tech. L.J. 1019, 1054-55 (2009). See Legal Memo #2 for a detailed explanation of section 1983 claims and *Bivens* actions.
[76] A. Michael Froomkin, Government Data Breaches, 24 Berkeley Tech. L.J. 1019, 1052 (2009).
[77] See U.S. Gov't Accountability Office, Information Security: Protecting Personally Identifiable Information, GAO 08-343, at 13 (Jan. 2008), available at http://www.gao.gov/new.items/d08343.pdf.

Management Act of 2002 (FISMA) also requires federal agencies to "develop, document, and implement an agencywide information security program."[78]

The Privacy Act, which applies only to federal government agencies, limits agencies' collection, disclosure, and use of personally identifiable information maintained in a record system.[79] Notably, the Privacy Act regulates only intentional disclosure of personal information.

The E-Government Act requires agencies to conduct privacy impact assessments (PIA) to analyze how information technology systems manage and protect personal information.[80]

FISMA directs agencies to conduct a risk-based assessment of information security management and to "cost-effectively reduce information security risks to an acceptable level."[81] Federal agencies are also required to provide security awareness training to personnel, conduct periodic testing of the security measures, and implement "procedures for detecting, reporting, and responding to security incidents."[82] In responding to security incidents, agencies may notify the Federal information security center, law enforcement agencies, national security agencies, or any other designated agency or office.[83] FISMA authorizes the central Federal information center to provide information and technical assistance to operators of agency information systems and to consult with other federal agencies as appropriate.[84]

FISMA does not specifically address notification to members of the public, but the U.S. Office of Management and Budget (OMB) has included this requirement in its directive on "Safeguarding Against and Responding to the Breach of Personally Identifiable Information."[85] As of 2007, federal agencies are required to implement a "breach notification policy" that includes external breach notification. Specifically, OMB requires that "Unless notification to individuals is delayed or barred for law enforcement or national security reasons, once it has been determined to provide notice regarding the breach, affected individuals should receive prompt notification."[86]

C. Use and Disclosure of Collected Data

[78] 44 USC § 3544(b).
[79] See U.S. Gov't Accountability Office, Information Security: Protecting Personally Identifiable Information, GAO 08-343, at 13 (Jan. 2008), available at http://www.gao.gov/new.items/d08343.pdf.
[80] See U.S. Gov't Accountability Office, Information Security: Protecting Personally Identifiable Information, GAO 08-343, at 13 (Jan. 2008), available at http://www.gao.gov/new.items/d08343.pdf.
[81] 44 USC § 3544(b).
[82] 44 USC § 3544(b).
[83] 44 USC § 3544(b)(7).
[84] 44 USC § 3546.
[85] Memorandum from Clay Johnson III, Deputy Dir. For Mgmt., Office of Mgmt. & Budget, on Safeguarding Against and Responding to the **Breach** of Personally Identifiable Information, M-07-16 (May 22, 2007), available at http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf.
[86] Memorandum from Clay Johnson III, Deputy Dir. For Mgmt., Office of Mgmt. & Budget, on Safeguarding Against and Responding to the **Breach** of Personally Identifiable Information, M-07-16, at 19 (May 22, 2007), available at http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf.

Disclosure of information can, in itself, constitute an invasion of privacy.[87] The Supreme Court has further noted "the fact that an event is not wholly 'private' does not mean that an individual has no interest in limiting disclosure or dissemination of the information."[88] In addition to addressing Constitutional concerns, law enforcement's use and disclosure of data gathered by UAS/UAV must also consider Title III of the Wiretap Act, the Privacy Act of 1974, and the Freedom of Information Act exemption 7(c). The following section will first address permissible use and disclosure of UAS/UAV-gathered data in light of existing legal regulations, followed by a discussion of impermissible use and disclosure.

i. Permissible Use and Disclosure

Title III of the Wiretap Act and the ABA Standards suggest general consensus that surveillance data may be used and disclosed exclusively for law enforcement purposes, unless exigent circumstances warrant otherwise.

Where law enforcement officers have intercepted wire, oral, or electronic communications by means authorized by Title III, § 2517(1) of that statute authorizes law enforcement officers to disclose the contents of these communications to other officers to the extent that such disclosure is appropriate to the proper performance of the official duties of the officer making or receiving the disclosure.[89] This provision permits the exchange of information obtained from lawfully intercepted communications among law enforcement officers and between state and federal law enforcement agencies.[90] Such an exchange is permissible only to the extent that it is appropriate to the proper performance of the official duties of both the officer making and the officer receiving the disclosure.[91]

Section 2517(2) of Title III permits law enforcement who have learned of the contents of lawfully intercepted communications to "use such contents to the extent such use is appropriate to the proper performance of his official duties."[92] Appropriate use of intercepted communications may include establishing probable cause for arrest or search warrants and developing additional investigative leads.[93]

Law enforcement conducting surveillance in compliance with Title III may inevitable intercept communications related to offenses outside the scope of the Title III authorization

[87] Martin Marcus, Christopher Slobogin, *ABA Sets Standards for Electronic and Physical Surveillance*, Crim. Just., Fall 2003, at 5, 17
[88] *U.S. Dep't of Justice v. Reporters Comm. For Freedom of Press*, 489 U.S. 749, 770, 109 S. Ct. 1468, 1480, 103 L. Ed. 2d 774 (1989)
[89] 18 USC § 2517(1)
[90] S. Rep. 90-1097, at 2188. See also, *2 Law of Electronic Surveillance* § 7:34
[91] 18 USC § 2517(1)
[92] 18 USC § 2517(2).
[93] S. Rep. 90-1097, at 2188. See also, *2 Law of Electronic Surveillance* § 7:36

order. Section 2517(5) makes clear that the contents of those communications can also be disclosed and used as provided in § 2517(1) and (2).[94]

Section 2517(3) of Title III permits admission of lawfully intercepted wire, oral, or electronic communications in court proceedings.[95] Privileged communications that are otherwise lawfully intercepted retain their privileged character.[96] Communications intercepted in violation of Title III and any evidence derived therefrom cannot be admitted into evidence at any court proceeding or before any legislative committee or Federal or State government authority.[97] While the language of § 2515 indicates a complete prohibition on any use of unlawfully intercepted communications as evidence, the legislative history of Title III suggests possible Congressional intent that such communications could be used for impeachment purposes.[98]

Law enforcement officers can disclose communications to certain federal government officials "to the extent that such contents include foreign intelligence or counterintelligence" where this information will assist the official in performing official duties.[99] Disclosure can also be made to foreign law enforcement as it relates to the recipient's official duties.[100] Finally, law enforcement may disclose to any appropriate federal, State, local or foreign official communications related to threats of terrorism or hostile acts by a foreign power.[101]

The Privacy Act of 1974 seeks to ensure that individual records are disclosed and used only for a "necessary and lawful purpose."[102] Section 552a(b) of the Privacy Act enumerates a series of specific conditions under which disclosure is permissible.[103] In the absence of consent by the individual, federal agencies cannot disclose an individual's records protected by the Privacy Act to any person or any agency unless one of these specific conditions are met.[104]

ii. Impermissible Use and Disclosure

Both Title III of the Wiretap Act and the ABA Standards indicate that use and disclosure of UAS/UAV-gathered electronic data should be prohibited for any purpose not related to

[94] 18 USC § 2517(5)
[95] 18 USC § 2517(3)
[96] 18 USC § 2517(4)
[97] 18 USC § 2515
[98] S. Rep. 90-1097. See also *2 Law of Electronic Surveillance* § 7:81 (The formal legislative history of Title III, Senate Report 1097, indicates that illegally obtained recordings may be available for impeachment purposes, by stating that the exclusionary provision of § 2515 is not intended "to press the scope of the suppression role beyond present search and seizure law.")
[99] 18 USC § 2517(6).
[100] 18 USC § 2517(7)
[101] 18 USC § 2517(8)
[102] Privacy Act of 1974, Congressional Findings and Statement of Purpose, Act of Dec. 31, 1974, P.L. 93-579, § 2, 88 Stat. 1896.
[103] 5 U.S.C. § 552(a)(b).
[104] 5 U.S.C. § 552(a)(b).

official law enforcement duties.[105] In addition, the Freedom of Information Act (FOIA) exemption 7(c) prohibits federal disclosure of "investigatory records compiled for law enforcement purposes" when such disclosure would "constitute an unwarranted invasion of personal privacy."[106] The Supreme Court has recognized that protecting privacy interests includes "the individual interest in avoiding disclosure of personal matters."[107] The Court determined that this interest was implicated by a FOIA request for a citizen's FBI rap sheet, concluding that disclosure of the rap sheet was protected by FOIA Exemption 7(c). The Court rejected the requesting party's argument that the citizen held no privacy interest in the rap sheet because the events summarized therein had previously been disclosed to the public.[108] Notably, the Court characterized this argument as a "cramped notion of personal privacy."[109]

Unfortunately, abuse of surveillance data captured by UAV is a credible concern. For example,[110] in 2004 a New York City police surveillance video captured the suicide of a twenty-two year old man in the lobby of a public housing unit.[111] After a New York City police officer shared the recording with a friend, the video appeared on an offensive online forum.[112] The tort of public disclosure of private facts is increasingly recognized by state courts and may create liability for officers engaging in such offensive conduct.[113]

iii. Interagency sharing

Officers may be able to share UAS/UAV-gathered data with other federal, state, and local governmental agencies where such data contains foreign intelligence or law enforcement information that is relevant to the receiving agency's official duties. The USA PATRIOT Act includes several provisions to facilitate increased sharing of foreign intelligence and law enforcement information.[114] Section 203 of the PATRIOT Act grants broad authority to share foreign intelligence information gathered during criminal investigations with certain federal

---

[105] 18 U.S.C. § 2517; ABA Standards, supra note 5.
[106] 5 USC § 552(b)(7)(c)
[107] *Whalen v. Roe*, 429 U.S. 589, 598-600, 97 S.Ct. 869, 875-877, 51 L.Ed.2d 64 (1977) (footnotes omitted).
[108] *U.S. Dep't of Justice v. Reporters Comm. For Freedom of Press*, 489 U.S. 749, 762-63, 109 S. Ct. 1468, 1476, 103 L. Ed. 2d 774 (1989).
[109] *U.S. Dep't of Justice v. Reporters Comm. For Freedom of Press*, 489 U.S. 749, 762-63, 109 S. Ct. 1468, 1476, 103 L. Ed. 2d 774 (1989).
[110] Jeremy Brown, *Pan, Tilt, Zoom: Regulating the Use of Video Surveillance of Public Places*, 23 Berkeley Tech. L.J. 755, 763-64 (2008) (discussing the 2004 story of Paris Lane's suicide and police abuse of surveillance recording of that event).
[111] Shaila K. Dewan, *Video of Suicide in Bronx Appears on Shock Web Site*, N.Y. Times, Apr. 1, 2004, at B3.
[112] Murray Weiss, Bx. *Cop Caught in 'Net--Suicide-Video Scandal*, N.Y. Post, June 22, 2004, at 25.
[113] See Restatement (Second) of Torts § 652D (1977).
[114] See Richard A. Best Jr., Sharing Law Enforcement and Intelligence Information: The Congressional Role Summary, Congressional Research Service (Feb. 13, 2007), available at http://www.fas.org/sgp/crs/intel/RL33873.pdf ("Almost all assessments of the attacks of September 11, 2001, have concluded that U.S. intelligence and law enforcement agencies had failed to share information that might have provided advanced warning of the plot.").

officials. Specifically, subsection 203(b) of the PATRIOT Act amended Title III of the Wiretap Act to authorize law enforcement officers and Government attorneys to share "foreign intelligence" information obtained by Title III-authorized wiretap with any other federal law enforcement, intelligence, protective, immigration, national defense, or national security official."[115] Subsection 203(d) authorizes sharing of foreign intelligence information gathered during federal criminal investigations with the same types of federal officials.[116] Section 504 of the PATRIOT Act permits federal intelligence officers to consult with Federal and State law enforcement "to coordinate efforts to investigate or protect against" threats to national security.[117]

Sharing of foreign intelligence information among federal, state, and local law enforcement is also facilitated through state-run "fusions centers."[118] In 2003, the U.S. Department of Justice (DOJ) issued the National Criminal Intelligence Sharing Plan to emphasize the increased role of state and local law enforcement in domestic intelligence.[119] Based on this plan, DOJ and the U.S. Department of Homeland Security (DHS) issued federal guidelines for the establishment and operation of fusion centers in 2006.[120] The federal guidelines described "a collaborative environment for the sharing of intelligence and information among local, state, tribal, and federal law enforcement agencies, public safety agencies, and the private sector."[121] Law enforcement agencies located in jurisdictions that currently operate fusion centers should follow existing protocol on information sharing with respect to UAS/UAV-gathered electronic data.

While some of the barriers separating the foreign intelligence and law enforcement communities have been torn down in recent years, the separation between domestic law enforcement and U.S. military operations remains strong. The Posse Comitatus Act outlaws the willful use of any part of the Armed Forces to execute the law unless expressly authorized by the Constitution or by an act of Congress.[122] Specifically, the Act provides:

---

[115] 18 USC § 2517(6).
[116] 50 USC § 3365
[117] 50 USC § 1806(k)(1)
[118] See Michael Price, National Security and Local Police, Brennan Center for Justice, available at http://www.brennancenter.org/sites/default/files/publications/NationalSecurity_LocalPolice_web.pdf.
[119] Global Info. Sharing Initiative, U.S. Dep't of Justice, The National Criminal Intelligence Sharing Plan (2003), available at http://www.au.af.mil/au/awc/awcgate/doj/nat_crim_intel_share_plan2003.pdf.
[120] Global Justice Info. Sharing Initiative, U.S. Dep't of Justice, et al., Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era 2 (2006) [hereinafter Fusion Center Guidelines], available at http://www.it.ojp.gov/documents/fusion_center_guidelines_law_enforcement.pdf.
[121] Fusion Center Guidelines, at 29.
[122] *See* Charles Doyle & Jennifer K. Elsea, *The Posse Comitatus Act and Related Matters: The Use of the Military to Execute Civilian Law* Summary, Congressional Research Service (Aug. 16, 2012) (hereinafter, the "CRS Report"), *available at* http://www.fas.org/sgp/crs/natsec/R42659.pdf.

> Whoever, except in cases and under circumstances expressly authorized by the Constitution or Act of Congress, willfully uses any part of the Army or the Air Force as a posse comitatus or otherwise to execute the laws shall be fined under this title or imprisoned not more than two years, or both.[123]

Though the particular language of the Act mentions only the Army and the Air Force, Department of Defense policy has extended its application to all branches of the U.S. military.[124]

Questions concerning the Act's application arise most often in the context of assistance to civilian police.[125] At least in this context, the courts have held that, absent a recognized exception, the Posse Comitatus Act is violated when (1) civilian law enforcement officials make "direct active use" of military investigators; or (2) the use of the military "pervades the activities" of the civilian officials; or (3) the military is used so as to subject "citizens to the exercise of military power which was regulatory, prescriptive, or compulsory in nature."[126] It is important to note that the Act is not violated when the Armed Forces conduct activities for a military purpose.[127]

One important exception relating specifically to information sharing was carved out by Congress in 1981. The 1981 exception, designed to promote military cooperation with criminal investigations of narcotics trafficking in the Caribbean,[128] provides that "[t]he Secretary of Defense may . . . provide . . . civilian law enforcement officials any information collected during the normal course of military training or operations."[129] Thus, Armed Forces can legally share information with domestic law enforcement if they just so happen to come across it in the ordinary course of business, by they *cannot* share information/intelligence they have deliberately set out to collect on law enforcement's behalf.[130]

---

123 18 U.S.C. § 1385.

124 See Daniel Gonzalez et al, Improving Interagency Information Sharing Using Technology Demonstrations, The RAND Corporation (2014), available at https://www.rand.org/content/dam/rand/pubs/research_reports/RR500/RR551/RAND_RR551.pdf.

125 *See* Charles Doyle & Jennifer K. Elsea, *The Posse Comitatus Act and Related Matters: The Use of the Military to Execute Civilian Law* Summary, Congressional Research Service (Aug. 16, 2012) (hereinafter, the "CRS Report"), *available at* http://www.fas.org/sgp/crs/natsec/R42659.pdf.

126 *Id.* at 54 and n.322. For an in depth discussion of exceptions, see the CRS Report at 29-51.

127 *See id.* at 46-51.

128 *See* Nathan Alexander Sales, Mending Walls: Information Sharing After the USA PATRIOT Act, 88 Tex. L. Rev. 1795, 1827 (2010) (citing Roger Blake Hohnsbeen, *Fourth Amendment and Posse Comitatus Act Restrictions on Military Involvement in Civil Law Enforcement*, 54 Geo. Wash. L. Rev. 404, 416-19 (1986)).

129 10 U.S.C. § 371(a).

130 *See Sales* at 1827 and n. 210.

The 1981 exception does not directly address whether domestic law enforcement can legally share collected information with the Armed Forces. Therefore, the question becomes whether, in Posse Comitatus terms, the Armed Forces "execute the laws" when they use in military operations data that was gathered *via* UAV or UAS by domestic law enforcement for policing purposes. This kind of exchange is not clearly unlawful.[131] But while police may risk little harm from sharing UAV/UAS-gathered electronic data with Armed Forces, such a practice may make citizens uncomfortable.

A second important provision of federal law that restricts the use of U.S. military for law enforcement activities is found at Title 10, Section 375 of the U.S. Code:

> The Secretary of Defense shall prescribe such regulations as may be necessary to ensure that any activity (including the provision of any equipment or facility or the assignment or detail of any personnel) under this chapter does not include or permit direct participation by a member of the Army, Navy, Air Force, or Marine Corps in a search, seizure, arrest, or other similar activity unless participation in such activity by such member is otherwise authorized by law.[132]

This provision generally prohibits members of the U.S. military from directly participating in the search, seizure or arrest of a U.S. citizen or other person on U.S. territory unless specifically authorized by law.[133] Nevertheless, certain forms of indirect assistant from the U.S. military to domestic law enforcement may be permissible. Section 371 notably permits the military to share information collected during military operations and training with law enforcement when such information "may be relevant to a violation of any Federal or State law."[134]

VI. RECOMMENDED PRACTICES

As repeated throughout, no federal legislation explicitly regulates UAS/UAV-gathered electronic data and little in the way of state law exists on the topic. Existing federal legislation and legal principles can be used, by analogy, to create a piecemeal legal framework. Although this framework fails to provide truly meaningful or cohesive regulation, it does highlight a basic set of issues and concerns that law enforcement must address with respect to UAS/UAV data. The following guidelines are recommended practices for law enforcement to avoid legal pitfalls in UAS/UAS electronic data collection and use:

---

[131] Sales reaches the same conclusion. *See id.*

[132] 10 USC § 375.

[133] 10 USC § 375.

[134] 10 USC § 371.

First, law enforcement must ensure that the collection of electronic data by UAS/UAV is conducted in a non-discriminatory manner and is reasonably limited in its scope. UAS/UAV must be lawfully present at the vantage point from which data is collected. Where the data collected includes audio-recordings of protected communications, officers must comply with Title III of the Wiretap Act regarding authorization, minimization, and providing notice of surveillance.

Second, law enforcement agencies that plan to retain any UAS/UAV-gathered electronic data must implement sufficient security and access controls. When necessary, officers must also comply with Title III requirements regarding sealing and storage of surveillance records.

Third, UAS/UAV-gathered data should be used and disclosed exclusively for law enforcement purposes, unless exigent circumstances warrant otherwise. Officers must recognize that disclosure of personal information can result in unlawful invasion of privacy and exercise significant care when accessing and sharing such data.

Fourth, to further transparency and public engagement, officials should disclose by way of publically-available, published guidelines specifically what happens to information once it is collected by UAS/UAV as well as how the collected information may or will be used.[135] Officials should specifically address:

- whether captured data is retained or discarded;
- if data is retained, officials should specify for how long data is retained and where it is retained, i.e., is a separate database maintained; is the data incorporated into other government databases?;
- what other government-controlled electronic databases the law enforcement agency compares captured data with (sex offenders, suspects wanted by police, etc.);
- and what actions the law enforcement agency takes when it detects a match.[136]

Fifth, law enforcement agencies must ensure that UAS/UAV surveillance policies are written and that they include sufficient accountability and transparency. The ABA Standards suggests that law enforcement officials should be held accountable for the use of physical surveillance technology by periodic review of the scope and effectiveness of the surveillance program.[137] The ABA Standards also suggest that accountability can be furthered by "[m]aintaining and making

[135] Max Guirguis, *Electronic Visual Surveillance and the Reasonable Expectation of Privacy*, 9 J. Tech. L. & Pol'y 143, 171 (2004)
[136] Max Guirguis, Electronic Visual Surveillance and the Reasonable Expectation of Privacy, 9 J. Tech. L. & Pol'y 143, 171 (2004).
[137] ABA Standards, supra note 5.

available to the public general information about the type or types of surveillance being used and the frequency of their use."[138]

Public concern over potentially limitless surveillance capabilities of sophisticated UAS/UAV technology may stem from fear that officers will be watching and recording their every move. As noted by the International Association of Chiefs of Police (IACP) in the 2014 "IACP Technology Policy Framework", a "principal tenet of policing is the trust citizens grant police."[139] Law enforcement should take reasonable steps to dispel concerns and foster public trust in UAS/UAV programs in order to maximize the potential utility and public benefit offered by these emerging technologies.

[138] ABA Standards, supra note 5.
[139] *See* International Association of Chiefs of Police Aviation Committee, *Recommended Guidelines for the use of Unmanned Aircraft* (Aug. 2012), *available at* http://www.theiacp.org/portals/0/pdfs/iacp_uaguidelines.pdf.