

## U.S. Domestic Regulation of National Airspace: An Evolution and Suggested Way Ahead

Colonel Dawn M.K. Zoldi and First Lieutenant Gregory R. Speirs, United States Air Force\*

### I. INTRODUCTION

The Federal Aviation Administration (FAA) Modernization and Reform Act of 2012 mandates the “safe integration of civil unmanned aircraft systems” (UAS) into the national airspace system by the end of 2015. However, the FAA’s progress has been slow. The vast majority of states have attempted to fill this void. In the past two years, all fifty states have proposed a combined total of 168 UAS bills. Almost half of the states entertained multiple bills simultaneously. Thirteen states have passed UAS legislation. Federal UAS legislation has also been introduced, which largely tracks state initiatives in scope and purpose.

The generalized goal of all of almost all of these proposals is to “protect citizens’ privacy” or free them from “unwarranted” surveillance. Although each state takes a different path, across both years, most of these bills apply to local law enforcement agencies and prohibit them from using UAS to gather information or evidence, with various exceptions. Many also contain procedural hurdles, operational constraints, detailed reporting and oversight

regimes, and significant ramifications for violations.

This article reviews and analyzes these legislative proposals and identifies “best practices” as a means to suggest a reasonable way ahead for future UAS legislation.

### II. 2013 LEGISLATION

In 2013, the overwhelming majority of states proposed legislation to prohibit domestic UAS use by government actors. There were exceptions, the most common being the requirement for a judicial warrant. The bills also contained operational restrictions, and violation ramifications. The 2013 federal UAS proposals largely tracked state requirements.

#### A. State Legislation

- Applicability. Fifty-eight percent of 2013 UAS bills applied to state and local government actors, primarily to law enforcement agencies (LEA). Sixty-eight percent extended their applicability to federal government employees. While even fewer, ten percent, of state bills directly addressed the military, many were written broadly enough to apply to military operators.

- Prohibitions and Exceptions. The majority of states precluded government officials from using UAS to collect information or evidence, with limited exceptions. The most common exception was the requirement to obtain a judicial warrant or order. Other exceptions, in order of prevalence, included: imminent danger and the protection of life; individual consent; credible risk of terrorist attack; protection of property; to catch a “fleeing

\* The views expressed herein are those of the author and do not represent those of the U.S. Air Force or the Department of Defense.

Colonel Dawn M.K. Zoldi, USAF (B.A. History and Philosophy, University of Scranton (1989); M.A. History University of Scranton (1989); J.D. Villanova University School of Law (1992); M.S. Military Strategic Studies, Air War College, Air University with Distinction (2010)) is currently the Staff Judge Advocate, United States Air Force Academy (USAF), CO, 80840 (719-333-3920; fax: 719-333-3644; e-mail: dawn.zoldi@us.af.mil).

First Lieutenant Gregory Speirs, USAF (B.A. International Relations with a concentration in National Security, Pennsylvania State University (2009); J.D. North Carolina Central University School of Law (2014)) is currently stationed at Lackland AFB, TX. (e-mail: gregoryspeirs@gmail.com).

felon” or prevent the destruction of evidence; disaster response; Search and Rescue (SAR); higher education, training, research, or recreation; operations on or over public lands; in support of national security or organized crime conspiracies; crime scene investigations; aerial inspections; “Amber” or missing person alerts; other judicially recognized exceptions to the warrant requirement; border monitoring; and in support of controlled substance crimes investigations.

•Operational Constraints. The 2013 UAS bills also contained operational restrictions. Although the stated purpose of state UAS bills was to protect privacy, very few of them addressed how information collected would be used, disseminated, or retained. Those that did prohibited the use of facial recognition or other biometric matching technology, primarily on non-targets. Rarely did bills address dissemination of information, other than in the form of notice to the subject of UAS monitoring. Retention was a more common theme, specifically the requirement to delete information collected unlawfully or on non-targets shortly after collection. Some bills also included retention limits on target information, unless needed for a criminal investigation or prosecution.

Weapons restrictions were a more common thread across 2013 UAS bills. Almost a third of the states would have restricted operators from carrying lethal or non-lethal weapons on, or employing weapons from, UAS.

The 2013 bills also contained time, place, and manner restrictions, most notably the forty-eight hour mission execution window. States with place restrictions focused primarily on the home and areas surrounding it, places of worship, as well as farms and agricultural areas. Most states that included manner restrictions generally required users to collect information only on the target and to avoid or minimize data collection on others.

•Procedural Requirements. Exhaustive documentation, oversight, and reporting requirements were commonplace in 2013. In particular, most states proposed reporting rules that would have required LEA, the Attorney General, the judiciary and court administrators, to file reports on UAS activities annually. Many states also would have, with regard to emergency UAS operations, required responders to document the grounds for such use within 24 to 48 hours. Of these, a minority of states required public notice of UAS operations, images, and government reports. Other than these examples, few states required specific record-keeping on UAS operations.

•Violation Ramifications. UAS proposals in 2013 contained exclusionary rules, personal liability provisions, and preventive measures to address violations of their standards. In order of prevalence, evidence exclusions applied to: criminal cases (more than half); civil or administrative hearings (more than a third); and derivative evidence.

Civil liability provisions were commonplace and included equitable relief, such as injunctions to preclude UAS use or to prevent the use of information collected. Many bills contained a broad spectrum of civil penalties. Twenty-two percent of 2013 bills made violating their provisions a crime. A few provided for administrative discipline.

## *B. Federal Legislation*

•Applicability. Federal law applies to federal actors, but some of 2013 federal proposals also expanded their reach to state actors as well as private actors.

•Prohibitions and Exceptions. As with the majority of state bills, the key 2013 federal bills forbade collection of information without a warrant or other valid exception. They contained similar exceptions as well, including for: danger to life; terrorist attacks; patrol of borders; “exigent circumstances;” pursuit of fleeing felons; to prevent destruction of

evidence; consent; in emergency situations; and for conspiratorial activities threatening the national security interest or characteristic of organized crime.

- Operational Constraints. Most federal bills in 2013 focused on operational constraints, especially with regards to weaponized UAS. Three bills were introduced to specifically prohibit the use of UAS to use lethal force against a person in the U.S. except where the person posed a threat to life. Minimization was also a common theme.

- Procedural Requirements. The procedural requirements contained in 2013 federal UAS bills were consistent with those found in their state counterparts. Common provisions included: 10-day notice to the subject of an investigation; extensive reporting rules; and requirements to obtain a warrant after an emergency use of a UAS.

- Violation Ramifications. Many federal bills also copied state efforts to exclude UAS-collected data from criminal, civil and administrative hearings if obtained in violation of their outlined restrictions. Some also contained civil causes of action, triggered administrative or other discipline for violators, and included license revocation for non-compliance.

### III. 2014 LEGISLATION

Legislative UAS efforts in 2014 built on the 2013 state and federal templates, but with a slightly more nuanced approach. These bills trended towards extending coverage more broadly to government actors beyond those in LEA. Prohibitions expanded beyond collection and included retention and dissemination of UAS-collected data. Exceptions to those prohibitions were more detailed than previously seen. Operational constraints more frequently included directives for UAS program rule-making. Finally, the number of procedural requirements for UAS operations greatly expanded.

#### A. State Legislation

- Applicability. 2014 UAS bills trended towards broader coverage, using general terms such as “state agency,” “local entities,” “any individual,” or “any person,” instead of maintaining a primary focus on state or local LEA. More states also directly addressed military UAS operations, in contrast to 2013 UAS bills.

- Prohibitions and Exceptions. Whereas 2013 UAS bills focused on prohibiting the use of UAS to obtain information or evidence, 2014 bills took a more expansive approach by also prohibiting disclosure and receipt of UAS-collected information. One-third of 2014 bills took a similar tact as 2013 by placing primary emphasis on UAS “use.” Twenty-one percent additionally included disclosure and receipt prohibitions in their UAS prohibitions.

The warrant exception remained a popular provision, but not nearly as prevalent as in the past year. Of note, the exception that allowed UAS to protect life in emergency situations was significantly lower than in 2013. Likewise, other exceptions found in 2013 bills appeared less frequently, including: protection of property; to counter a high risk of terrorist attack; in support of disaster response; to pursue a fleeing felon; to prevent the destruction of evidence; “Amber” or missing persons alerts; public land operations; and in support of crime scene investigations.

In contrast, several of the 2013 exceptions were included more frequently in 2014, including: consent; judicially recognized exceptions to the warrant requirement; aerial inspections and allowances for higher education, training, research and recreation.

A few exceptions common to both years’ UAS legislative proposals remained unchanged in frequency of appearance, such as those relating to search and rescue operations as well as national security and organized crime conspiracies.

A host of new exceptions arose in 2014 to address a broad range of public and private activities. Some states introduced public safety exceptions that would allow UAS operations for: hostage situations; to handle explosive ordinances or hazardous materials; monitoring plants and animals; fire suppression; utilities inspection, maintenance or repair; port authority surveillance and security; and atmospheric testing and monitoring. With respect to LEA, unlike 2013, some states explicitly included a “plain view” exception. Some states included a “catch all” provision to permit state actors to operate UAS, so long as the information collected would not be used for law enforcement or intelligence purposes.

With regards to private actors, a number of states contained exceptions for farming and agricultural use, and for inspection of one’s own land and infrastructure. A number of business-related exceptions appeared in 2014, including for UAS manufacturers; the media; realtors; FAA test site operators; and business owners generally.

• Operational Constraints. 2014 UAS legislative filings contained constraints on operations similar to those in 2013 including: prohibitions on facial recognition technology and use of biometrics; requirements for notice to the subject of data collection; distribution limitations; retention limits; mission execution windows; weapons prohibitions; minimization requirements with regards to non-targets and other unique provisions. The quality and quantity of such provisions varied widely, depending on the topic.

Legislators decreased emphasis on retention rules by a ten percent margin. Likewise, both weapons and location restrictions showed an eight percent decrease. Subject notification provisions also appeared slightly less in 2014.

On the other hand, provisions addressing dissemination appeared seventeen percent

more frequently. Mission execution windows and collection minimization requirements were slightly more prevalent as well. Prohibitions on use of facial recognition or biometric technologies increased by one percent.

Given the FAA’s 2015 UAS integration deadline, a provision to comply with FAA requirements and guidelines, not previously seen in 2013, appeared in several 2014 bills.

Some of the more rare but interesting manner restrictions and constraints that appeared in 2014 UAS bills included: requiring contact information to be marked on a UAS; procedural rules for firefighters; hunting provisions; licensure requirements; and a prohibition on the use of Chinese lanterns.

• Procedural Requirements. Reporting and oversight clauses took a slight downturn in 2014. However, the reporting requirements appear to have evolved, placing extensive procedural burdens on government agencies. Legislators continued to require approval before a governmental organization could purchase an UAS. A similar trend appeared with regards to requiring first responders file a public report after emergency UAS use; for other public notifications of UAS operations; and for UAS-related record-keeping.

2014 UAS legislation contained a four percent uptick in procedural requirements, with noteworthy informational reporting burdens. Many such provisions would require either LEA, attorneys general, the judiciary or all three to report to the legislature or other governing body information such as the number of times UAS were used by date, time, location, the types of incidents and justifications; the number of criminal investigations aided and in what manner.

A new development in the 2014 proposals included that procedures be adopted to address approval authorities, licensure, and training,

such as those proposed by the International Association of Chiefs of Police Aviation Committee.

- Violation Ramifications. Ramifications for violating UAS laws evidenced a slight decrease in 2014, with one exception, the criminalization of UAS activity.

Exclusionary provisions, for criminal, civil or administrative hearings and derivative evidence were down by a small margin. Likewise, civil liability, penalties and equitable relief did not get as much attention.

In contrast, increased emphasis was placed on the criminalization of UAS activities, from UAS weaponization, to use for hunting or tracking, to creation of specific privacy offenses punishable as crimes, ranging from misdemeanors to serious felonies.

#### *A. Federal Legislation*

2014 marked a quiet year in federal legislation. In 2013, a total of 13 bills were introduced; only five were introduced in 2014. These bills demonstrated competing viewpoints toward UAS. On one hand, three bills prevented acquisition of UAS' by LEA. On the other hand, lawmakers recognized and proposed specific roles in which the platform could enhance LEA's capabilities.

As in the state arena, 2014 bills contained similar language to that found in 2013, with additional nuance. Emphasis expanded beyond LEA to other government actors; prohibitions were broadened to address the retention and dissemination of UAS collected data; directives for UAS program rule-making abounded as did the number of operational procedures. Exceptions were also similar to those previously seen.

### IV. CRITICAL ANALYSIS & RECOMMENDATIONS

In this section, we take a critical look at all of these proposals, with an eye towards

proposing an actionable roadmap for developing this critical area of the law.

#### *A. Applicability*

Over the last two years, virtually all state and federal UAS proposals target government actors, primarily LEA; yet existing law and policy, including the Fourth Amendment, already applies to governmental action as it relates to privacy.

What should be more concerning, and worthy of increased regulatory attention, are private individuals' use of UAS. This includes those who might choose to use UAS technology for good as well as nefarious purposes. Very few bills provide affirmative guidance on private UAS operations, such as requiring training or licensure. A positive example worth emulating can be found in North Carolina Senate Bill 744, which requires a skills and knowledge test to be administered before anyone can fly a UAS. On the other hand, other than criminalizing violations of UAS regulatory procedures, no bills have attempted to address the potential threat that privately operated UAS pose to our nation's critical infrastructure, including to our military installations.

Also rare, but increasing in emphasis, are codified military exemptions and authorities. A 2013 bill from the State of Washington serves as a model example. The bill exempts from its provisions the military, including the National Guard, conducting training operations on a military base. With the increased role UAS systems have played on the battlefield, the military must maintain readiness through continual training.

Recommendations: Regulators should provide additional focus on private actors. In addition to criminalizing privacy violations, create laws prohibiting the use of UAS in

furtherance of criminal activity (e.g., delivery vehicle for improvised explosive devices). Finally, carve out exceptions for military UAS use, including National Guard in state status.

### *B. Prohibitions and Exceptions*

Prohibitions primarily against governmental actors relating to UAS use and collection remain consistently overbroad, with random exceptions. These continue to proliferate, despite the fact that there is applicable Fourth Amendment precedence already in place. Instead, legislators continue to take a buffet-style approach to UAS use and permissions. Keeping the Fourth Amendment intact should be a non-negotiable component to any UAS legislative proposal.

For example, the requirement for law enforcement to obtain a judicial warrant remains the most common exception found in UAS bills, yet this is already well entrenched in U.S. law as is the exception which enables law enforcement to gather information or evidence in exigent circumstances; with individual consent; in plain view; to pursue a fleeing felon or prevent the destruction of evidence. The Supreme Court of the United States has already endorsed these concepts, yet most UAS bills fail to include them. Legislators cannot continue to abandon established precedence for a “pick and choose” approach to the Fourth Amendment.

It remains encouraging that some proposed UAS laws would permit use without a warrant in emergency circumstances to save lives, akin to the “exigent circumstances” exception in Fourth Amendment law. Unfortunately, however, these provisions dropped by forty-eight percent in 2014 from the previous year. Danger to property clauses were only included in ten of the 2014 bills. Where such provisions are included, legislators have added more steps for LEA to respond to an

emergency. The absence of these provisions, or the presence of the provisions with additional procedural caveats, not only marks a significant departure from Supreme Court jurisprudence, it impedes LEA’s ability to timely respond to citizens in dire need.

On the other hand, some UAS proposals contain such broad provisions they completely gut the Fourth Amendment. “Catch-all” provisions, such as those found in seven states, lay out a “have at it” approach, as long as the gathered information is not used. For example, proposals in Iowa and Kansas allow for use of a UAS “if the agency does not use the information or derivative evidence in any proceeding... or for any intelligence purpose.” Such provisions would threaten the individual privacy these bills were meant to protect and simultaneously render the Constitution meaningless.

Constitutional provisions aside, very few state or federal bills contain explicit exceptions that would facilitate public safety or security, such as SAR, disaster response or damage assessment. Those bills that include these also require a warrant be obtained after-the-fact, even though there is no similar requirement in existing law.

Several state bills contain identically worded “terror attack” and “national security conspiracy” exceptions that would allow UAS use, “To counter a high risk of a terrorist attack by a specific individual or organization if the United States Secretary of Homeland Security...determines that credible intelligence indicates that there is such a risk.” These could benefit from revision. For example, the term “credible intelligence” is undefined. Similarly, the “national security conspiracy” exceptions found in many bills, addressing emergencies involving “conspiratorial activities threatening

the national security interest.” fails to define what these terms mean.

Another example of lack of clarity, one bill provides for an exception for “lawful business use.” Does *Amazon.com* need an approval process? Could pizza delivery qualify? Or can UPS fly gasoline to customers’ homes? The bill neither define the term “business use” nor provides the requisite framework for certification or licensing before a person may fly and safely claim it is a legitimate business purpose.

Recommendations: Legislators should: place a renewed emphasis on the Fourth Amendment by including all of its judicially recognized exceptions and conversely not condoning wide-open “catch all” exceptions; add provisions to facilitate humanitarian missions; and define key terms in any novel provisions.

### *C. Operational Constraints*

Most UAS proposals fail to address the issues that most directly impact privacy: use, dissemination, and retention. To the extent that existing privacy laws insufficiently guide the proper handling of UAS-collected information, such issues require legislative attention.

Many bills prohibit use of facial recognition or other biometric matching technology on non-target information. What if the non-target has committed a crime? Prohibiting LEA or intelligence personnel from using this invaluable tool creates an unnecessary legal safe-haven in incidentally-collected imagery for terrorists and criminals.

Prohibitions on weaponized UAS, as discussed above, are relatively commonplace in UAS legislative proposals. Yet, a UAS may

prove to be the best asset for a particular situation, such as high risk tactical situations. Weapons prohibitions could also impact critical training for the military and its partners.

One positive development in UAS proposals, over time, has been increased attention to the distribution and use of information collected with a UAS. To protect privacy, some states would designate UAS-collected images as “confidential,” and outside the scope of public records. Even so, some bills continue to forbid use or disclosure of incidentally collected information in any proceeding or require such information be deleted shortly after collection. Recognizing that these types of provisions are unduly restrictive, some drafters adjusted course and would allow non-target information to be retained if necessary to a criminal investigation, prosecution or, in some cases, for training. These are worth emulating.

Recommendations: Maintain an increased emphasis on what to do with UAS-collected information through procedures on proper use, dissemination and retention. Regulators should reconsider weapons prohibitions for public actors. All of this must be done in a manner that balances privacy and individual rights against the need for effective operational missions. For the weapons dilemma, one way to do this is to build in high-level approval authorities, such as the Governor, upon advice from the State Attorney General, before such force could be used.

### *D. Procedural Requirements*

The two-year survey of state and federal bills above showed an increase in additional and burdensome governmental reporting requirements. However, positive developments were also ushered in, in the

form of safety requirements for training and certification.

In concept, specific departmental record-keeping procedures seem to be a reasonable requirement for use of UAS technology. However, some bills took this too far. For example, in New Jersey, multiple bills would require a law enforcement entity that uses UAS to “retain fuel receipts for the previous two years.” There are simpler means to institute a check and balance to prevent excessive flight hours, such as those states which would require a year end annual report on usage.

Perhaps the strangest addition to some bills is a post-emergency search warrant provision. These require law enforcement agencies to document the emergency and file the report to the court within 48 hours. A few go even further. A bill in Hawaii requires an emergency situation to be in existence, meaning imminent danger to life or safety, but requires grounds for probable cause and warrant to be obtained within 48 hours after the use. As discussed above, the Fourth Amendment does not require this. Why should we do so merely because the means to assist those endangered was a UAS?

For the first time in 2014, many state bills included a requirement for UAS operators to, “fully comply with all FAA regulations and guidelines.” Although the FAA has released guidance regarding certificates to be obtained for non-governmental use of UAS, notice of public rule-making for small UAS is just underway. In the meantime, only twelve exemptions have been granted, all of which were to private companies. The lack of FAA guidance will result in patch-work state action to continue filling this void.

One positive development in 2014, as opposed to 2013, are the bills that seek to establish training and certification systems for UAS use. One North Carolina bill delegates proper authorities to the state Division of Aviation and Department of Transportation, including oversight of the program. The lawmakers in this instance should be applauded taking a proactive and practical approach, by using agency personnel already in place to develop a system that is the first of its kind for UAS operation.

**Recommendations:** The addition of procedural requirements could greatly aid the safe use of UAS’ consistent with privacy interests. If the FAA adopts procedures including sound skills, training and certification programs, states should focus on additional safety issues, such as requirements that aircraft be easily identifiable and that actions be attributable. Reasonable record-keeping provisions for all UAS users would assist with this accountability.

#### *D. Violation Ramifications*

The majority of state and federal bills surveyed would also exclude evidence obtained in violation of their procedures at hearings. These provisions are problematic. Bills that fail to include the full spectrum of Fourth Amendment exceptions create unnecessary windfalls for criminal suspects. This windfall is not just limited to criminal suspects. States that preclude admission of UAS information from civil and administrative hearings extend otherwise inapplicable Fourth Amendment’s warrant requirements to civil cases.

Several state and federal UAS bills also create civil, criminal or administrative liability as against LEAs or individuals for failing to abide by their requirements. Interestingly,



legislators while retaining civil and criminal penalties for LEA, they have all but terminated administrative sanctions. The absence of handling a small infraction “in-house,” is detrimental to the efficiency of both agencies and the judicial system. Moreover, these provisions may have a chilling effect on operators who will now have to make life and death decisions under the added threat of personal liability.

In total, very few bills mention equitable relief or provide for an injunction against UAS use. While only a quarter of 2013 bills provided an injunction, 2014 saw a 14% decrease in the provision. What avenue does this leave for an aggrieved party to prevent a possible violation? Injunctive relief would certainly be prevalent if the primary focus of legislation was on private actors.

Legislation seems destined to be reactionary, with a wait for *Amazon.com*, *UPS*, or pizza delivery UAS to clutter the skies first. Certainly thousands of calls from homeowners complaining will then push legislation through.

Recommendations: Liability provisions continue to focus on government actors. Until regulators either revector existing laws, such as land-centric trespass provisions, and otherwise make it potentially painful for private actors to use UAS nefariously, their use to facilitate committing criminal acts will remain our greatest vulnerability.

#### IV. CONCLUSION

- The various state and federal attempts at legislating UAS operations use over the last two years have been inconsistent, albeit with limited threads of similarity. The focus remains on regulating government actors. Legislators continue to take a smorgasbord-

style approach to applying the Fourth Amendment. Helpful clauses that would protect individual privacy in a meaningful way still seem to elude most proposals. Procedural requirements and criminalization of government non-compliant UAS activity are proliferating at a breakneck pace.

Moving forward, legislators must strike a balance. Future efforts must: branch out to more directly and thoroughly address private actors; place a renewed emphasis on the Fourth Amendment and its judicially recognized exceptions for law enforcement; define key terms; and address procedural requirements, such as licensing requirements, and skill tests, in addition to operational constraints.

To date, efforts have been made primarily to restrain the technology. The efforts to confine prove unrealistic, however, because they do not offer solutions for proper development of UAS. A green light and oversight will have many beneficial attributes to society. With the continuing proliferation of UAS technology, the laws promulgated now will have an impact on future commerce, emergency response, and the daily welfare of our citizens. Therefore, the need for insightful UAS regulation requires significant leadership, relentless attention, and swift action in 2015 and beyond.

**Appendix A**  
COMPARATIVE ANALYSIS – STATE UAS BILLS

CLAUSE	2013	2014	DIFFERENTIAL
<b>APPLICABILITY</b>			
STATE/LOCAL APPLICABILITY	14%	35%	Up 21%
LEA APPLICABILITY	43%	46%	Up 3%
ANY PERSON	6%	33%	Up 27%
MILITARY APPLICABILITY	10%	21%	Up 11%
<b>PROHIBITIONS AND EXCEPTIONS</b>			
WARRANT	73%	47%	Down 26%
DANGER TO LIFE	83%	35%	Down 48%
DANGER TO PROPERTY	20%	13%	Down 7%
TERRORIST ATTACK	22%	13%	Down 9%
DISASTER RESPONSE	17%	15%	Down 2%
CONSENT	23%	26%	Up 3%
FLEEING FELON	18%	14%	Down 4%
DESTRUCTION OF EVIDENCE	11%	9%	Down 3%
SEARCH & RESCUE	16%	17%	Up 1%
AERIAL INSPECTIONS	6%	17%	Up 11%

OPS OVER PUBLIC LANDS	9%	6%	DOWN 3%
BORDER MONITORING	2%	0	DOWN 2%
JUDICIALLY RECOGNIZED EXCEPTIONS TO THE WARRANT REQUIREMENT	3%	9%	UP 6%
NATIONAL SECURITY CONSPIRACIES	7%	3%	DOWN 4%
ORGANIZED CRIME CONSPIRACIES	7%	3%	DOWN 4%
CRIME SCENE INVESTIGATIONS	6%	3%	DOWN 3%
AMBER/SIMILAR ALERTS	4%	1%	DOWN 3%
CONTROLLED SUBSTANCE INVESTIGATIONS	1%	0	DOWN 1%
HIGHER EDUCATION, TRAINING, RESEARCH AND RECREATION	10%	15%	UP 5%
<b>OPERATIONAL CONSTRAINTS</b>			
FACIAL RECOGNITION/BIOMETRICS	13%	14%	UP 1%
NOTICE TO SUBJECT	11%	10%	DOWN 1%
DISSEMINATION / RECEIPT	9%	29%	UP 20%
RETENTION	22%	12%	DOWN 10%
WEAPONS RESTRICTIONS	31%	23%	DOWN 8%
MISSION EXECUTION WINDOW	10%	12%	UP 2%
COLLECTION/MINIMIZATION	17%	22%	UP 5%
<b>PROCEDURAL REQUIREMENTS</b>			
ACQUISITION APPROVAL	17%	13%	DOWN 4%
REPORTING REQUIREMENTS	22%	24%	UP 2%
DOCUMENTATION AFTER EMERGENCY USE	19%	11%	DOWN 8%
PUBLIC NOTICE OF OPS	10%	5%	DOWN 5%
RECORD KEEPING	4%	5%	UP 1%
FULLY COMPLY WITH FAA GUIDELINES	N/A	26%	UP 26%
REQUIREMENTS TO ADOPT NEW PROCEDURES	N/A	24%	UP 24%
<b>VIOLATION RAMIFICATIONS</b>			
CRIMINAL EXCLUSION	54%	50%	DOWN 4%
CIVIL / ADMIN EXCLUSION	38%	31%	DOWN 7%
DERIVATIVE EVIDENCE	16%	5%	DOWN 11%
CIVIL LIABILITY	34%	33%	DOWN 1%
EQUITABLE RELIEF	24%	10%	DOWN 14%
CIVIL PENALTIES	43%	37%	DOWN 6%
CRIMINAL PROVISIONS	22%	24%	UP 2%
ADMIN DISCIPLINE	2%	1%	DOWN 1%

#### FEDERAL BILLS

CLAUSE	2013	2014	TOTAL
LOCAL APPLICABILITY	31%	75%	41%
FEDERAL APPLICABILITY	62%	75%	65%
MILITARY EXPLICITLY EXEMPT	8%	100%	29%
MILITARY NOT EXEMPT	69%	0	53%
GUARD AND RESERVE EXPLICITLY EXEMPT	0	25%	6%
PROHIBIT RPA USE	77%	50%	71%
STATES THAT FOLLOW 4 <sup>TH</sup> AGNOSTICALLY	0	0	0
STATES WITH DATA-COLLECTION AND RETENTION LIKE LANGUAGE	0	25%	6%
STATE CRIMINAL EXCLUSIONARY RULE	23%	50%	29%
CIVIL AND ADMINISTRATIVE EXCLUSIONARY RULE	23%	50%	29%
WARRANT EXCLUSION	31%	50%	35%

TERROR ATTACK EXCLUSION	31%	25%	29%
DANGER TO LIFE EXCLUSION	62%	25%	53%
DANGER TO PROPERTY EXCLUSION	8%	0	6%
FEELING FELON EXCLUSION	0	0	0
PUBLIC LAND MONITOR EXCLUSION	0	0	0
BORDER MONITOR EXCLUSION	0	0	0
CONSENT EXCLUSION	0	0	0
CIVIL INJUNCTION	0	0	0
CIVIL LIABILITY	0	0	0
CRIMINAL LIABILITY	0	0	0
WEAPON RESTRICTION	0	25%	6%
ANNUAL REPORTING REQUIREMENT	0	25%	6%
SEARCH AND RESCUE EXCEPTION	0	0	0
EVANESCENT EVIDENCE/DESTRUCTION OF EVIDENCE EXCEPTION	0	0	0
TEST SITE ESTABLISHMENT	0	0	0
STUDY COMMITTEE/TASK FORCE	0	0	0

## Appendix B – References

### STATE AND FEDERAL UAS BILLS 2013 & 2014

**References for 2013 legislation:** Ala. SB 317; Alaska HB 159a; Alaska Enrolled HCR 6; Ariz. HB 2574; Ariz. HB 2269; Ark. HB 1904; Ark. SB 1109; Cal. AB 1327; Cal. AJR 6; Cal. SB 15; Fla. SB 92; Ga. SB 200; Ga. HB 560; Haw. SB 783; Idaho SB 1134; Ill. SB 1587; Ill. SR 217; Ill. HB 1652; Ind. SB 20; Ind. SR 27; Iowa SF 276; Iowa HF 410; Iowa HF 427; Kan. 2394; Ky. HB 454; Ky. RS BR 1; Me. SP 72; Md. HB 1233; Mass. SB 1664; Mass. HB 1357; Mich. HB 4455; Mich. HB 3157; Minn. HF 612; Minn. SF 485; Minn. HF 1620; Minn. HF 1706; Minn. SF 1506; Minn. HF 990; Mo. HB 46; Mont. SB 196; Neb. LB 412; Nev. SB 385; Nev. AB 507; N.H. HB 619; N.J. AB 3157; N.J. AB 3929; N.M. SB 556; N.Y. AO 6370; N.Y. SO 4537; N.Y. AO 6244; N.Y. AO 8091; N.Y. AO 654; N.C. HB 312; N.C. SB 402; N.D. HB 1373; N.D. HB 1372; N.D. HB 2018; Ohio HB 207; Okla. HB 1556; Okla. HB 1795; Or. HB 2710; Or. SB 524; Or. SB 71; Or. SB 853; Pa. HB 961; Pa. SB 875; R.I. 28 Feb 2013 Act (Title 12 Ch. 5.3); R.I. LC00564; S.C. H3415; S.C. GB 395; Tenn. HB 591; Tenn. SB 796; Tex. HB 912; Vt. HB 540; Vt. SB 169; Va. HB 2012; Va. SB 954; Va. Charlottesville Drone Ordinance; Wash. HB 1771; Wash. SB 5782; W. Va. HB 2732; W. Va. HB 2948; W. Va. HCR 101; W. Va. HB 2997; Wis. SB 196; Wis. AB 203; Wyo. HB 242.

**References for 2014 legislation:** Ala. SB 240; Alaska HCR 15; Alaska HB 209; Alaska HB 209; Alaska HB 255; Alaska SB 136; Alaska SCR 11; Ariz. HB 2538; Ariz. HB 2334; Cal. AB 1524; Conn. HB 5217; Fla. SB 92; Haw. HB 1561; Haw. HB 1657; Haw. HB 1691; Haw. HB 1775; Haw. HB 1827; Haw. HB 2421; Haw. HB 2627; Haw. HB 2152; Haw. SB 2582; Haw. SB 2608; Haw. SB 3058; Ill. SB 2937 Ind. SB 336; Iowa HF 2289; Iowa SF 2314; Iowa SF 2157; Iowa SSB 3145; Kan. HB 2683; Kan. HB 2240; Kan. SB 409; Ky. RS BR 1328; Ky. HB 11; La. SCR 124; La. SB 330; La. SB 356; Md. SB 926; Md. HB 847; Md. HB 785; Mich. SB 926; Mich. HB 5631; Mich. SB 927; Mich. HCR 16; Mich. HR 280; Mich. SR 107; Mich. HCR 17; Mich. HR 279; Minn. HF 1994; Minn. HF 2553; Minn. HF 2552; Minn. SF 2687; Minn. SF 2037; Mo. HB 1204; Nev. SCR 7; N.H. HB 1307; N.J. S. 2310; N.J. AB 534; N.J. AB 4073; N.J. S. 2702; N.J. AB 4381; N.J. AB 4091; N.Y. S. 7639; N.Y. A. 9697; N.Y. S. 7479; N.Y. S. 6412; N.Y. A. 6541; N.Y. A. 4839; N.C. SB 402; N.C. HB 1099; N.C. HB 1208; Ohio HCR 45; Ohio HB 364; Ohio SB 189; Okla. HB 3055; Okla. HB 3039; Pa. SB 1334; Pa. SB 1332; P.R. SR 483; R.I. HB 7170; R.I. SB 2362; Tenn. HB 591; Tenn. HB 1779; Tenn. SB 1892; Tenn. HB 1669; Tenn. SB 1752; Tex. HR 866; Utah SB 167; Wash. HB 2789; Wash. HB 2178; Wash. SB 6172; Wis. SB 196; Wis. AB 203; Wyo. HB 105.