SIAGOVSUMMIT

Connecting Government, Security and Technology

June 27 – 28, 2018 | Washington, D.C. | #siagov18

SIAGOVSUMMIT

UAS/Counter-UAS Policy: Path Forward for Government and Private Security

Lisa Ellman
Hogan Lovells
Commercial Drone Alliance

Mark McCourt
Cobalt Robotics

Tom McMahon
AUVSI

Gilad Sahar
Convexum

FAA Reauthorization

House
Develop a rulemaking process to certify UAS Traffic Management services
Deploy UTM in low-risk areas, away from congested airspace
GAO report on roles of federal, state, and local governments concerning UAS
Study on financing UAS services by the FAA and how to sustain them
DOT, DOD and DHS to coordinate policy for counter-UAS technology
Establish sUAS air carrier certificate
BVLOS and sense-and-avoid at test sites

Senate
Report on spectrum coordination across government stakeholders
Study on government jurisdiction of UAS
FAA to publish procedures for emergency operations by civil operators
Review House-passed bill
Counter-UAS for DHS, DOJ agencies

UAS Integration Pilot Program

Choctaw Nation of Oklahoma
Mobile ground-based detect & avoid radars, advanced weather infrastructure

City of San Diego, California
ID & tracking systems
for UAS airspace integration

Innovation and Entrepreneurship Investment Authority, Herndon, Virginia
Detect & avoid, ID & tracking, radar systems, and mapping tools

Kansas Department of Transportation, Topeka, Kansas
Detect & avoid, ADS-B, satellite communications and geofencing

City of Reno, Nevada
Radar & weather data to expand UAS capability

University of Alaska-Fairbanks
Collision avoidance, detect & avoid day & night, ADS-B, differential GPS, satellite services, infrared imaging, and UTM

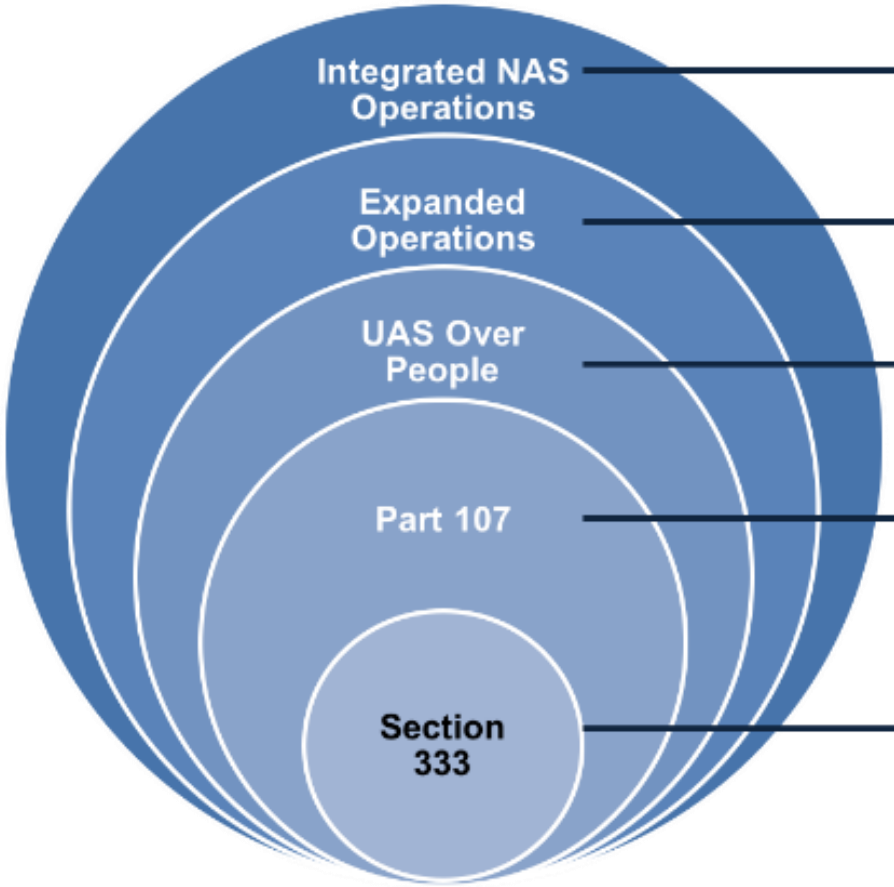
Memphis-Shelby County Airport Authority, Tennessee
Autonomous operations to support airport operations, perimeter security surveillance

North Carolina Department of Transportation, Raleigh
ADS-B, detect & avoid technologies, UTM & radar technologies

North Dakota Department of Transportation, Bismarck
Diverse operations that incorporate advanced technologies to expand nighttime and Beyond Visual Line of Sight operations

Lee County Mosquito Control District, Ft. Myers, Florida
Ground-based detect &avoid radar systems w/ADS-B, infrared imaging & satellite technology

FAA UAS Regulation Roadmap



- Interaction with ATC
- Safety achieved via compliance to conventional aircraft operating principles

- Expand part 107 to facilitate low altitude operations through Airworthiness certification
- Enables Pathfinder 2 and 3 operations

- Expand part 107 to incorporate standards for flight over non-participating people
- Enables Pathfinder 1 operations
- Remote Identification*

- Regulatory framework for small UAS operations
- Safety achieved through VLOS and operating limitations

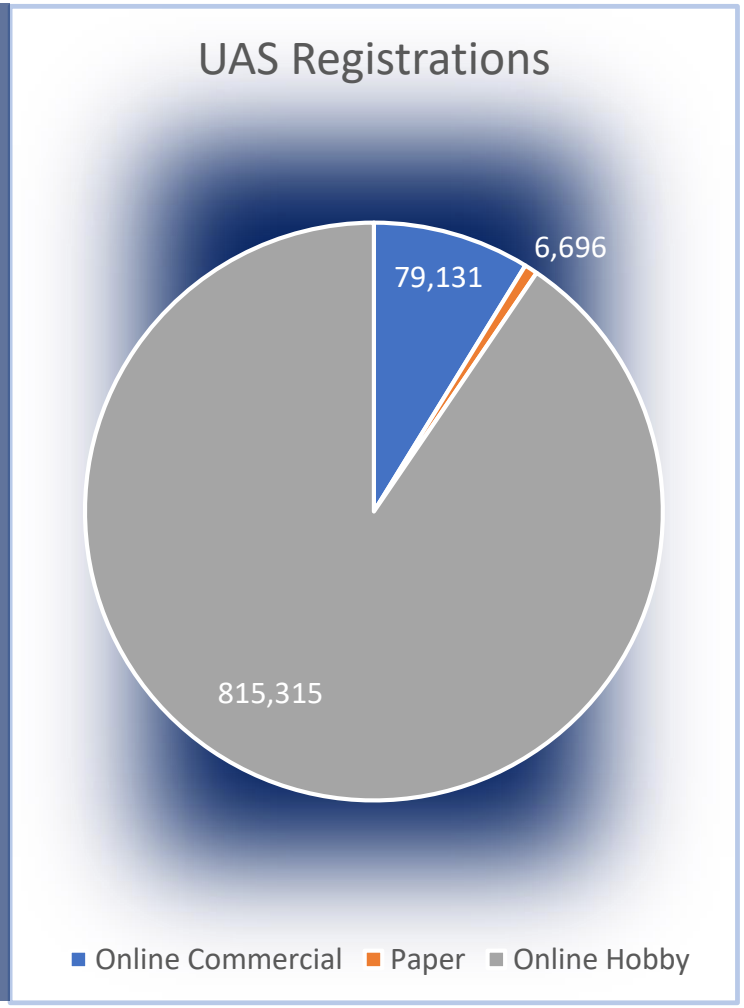
- Case-by-case exemptions granted to existing regulations
- Enables non-recreational UAS operations before final part 107 rulemaking
- Safety achieved with operating conditions and limitations

Source: FAA

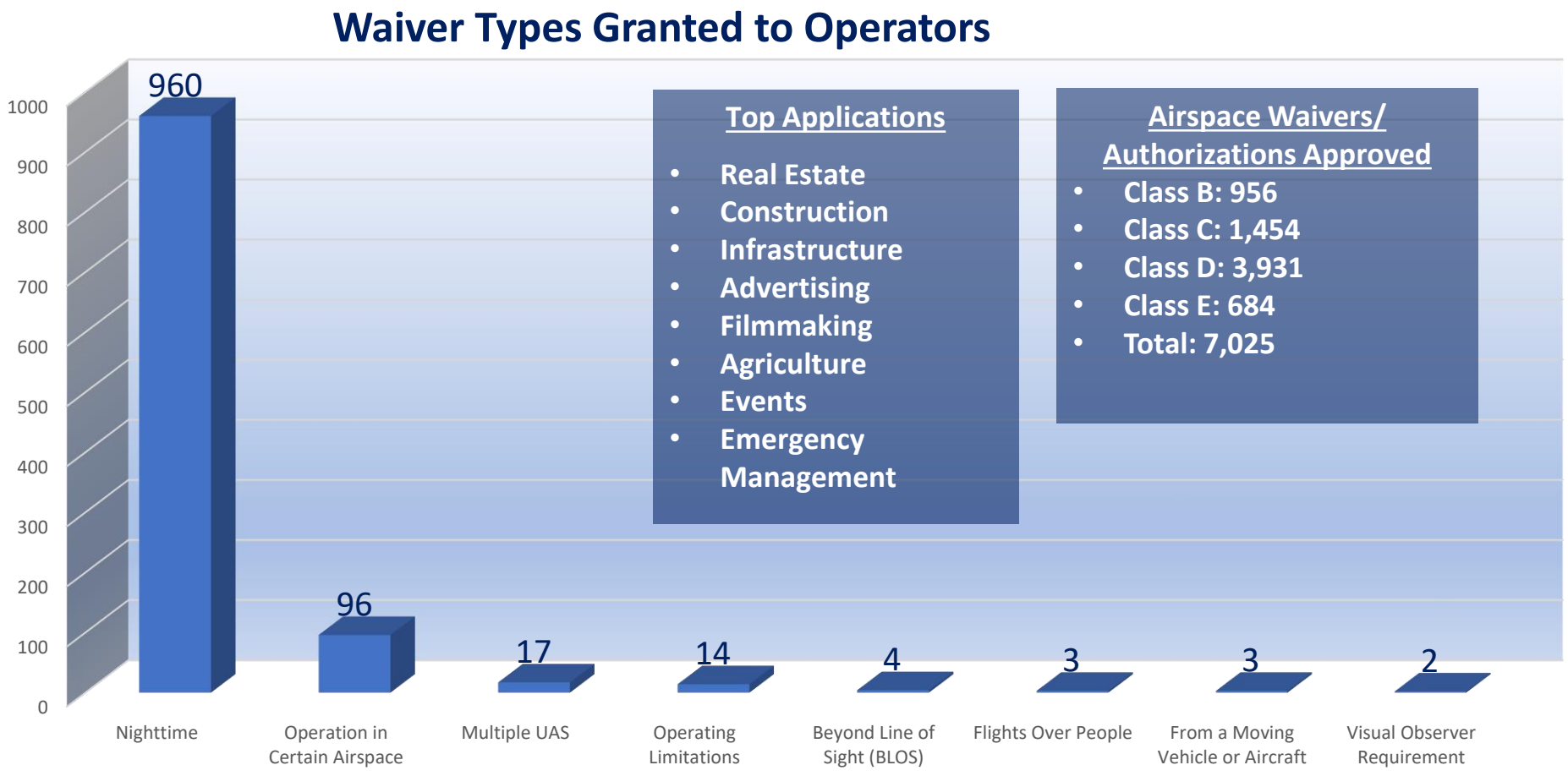
sUAS Rule (Part 107)

- Mandated by 2012 FAA Reauthorization Act
- Took effect on Aug. 29, 2016
- First clear regulatory framework on civil and commercial UAS operations
- Established a flexible, risk-based approach to regulating UAS
- Requires knowledge test, background check
- Certain operations allowed by waivers

- Approved operations:
  - Only during daylight hours
  - One aircraft, one pilot
  - Within visual line of sight, <400 feet
- Certain operations allowed by waivers
- Remote Pilot Certificates
  - Total Certificates Issued: 85,910
  - Total Knowledge Exam Passed: 59,391 Exam Training Course (ALC-451) – 26,519

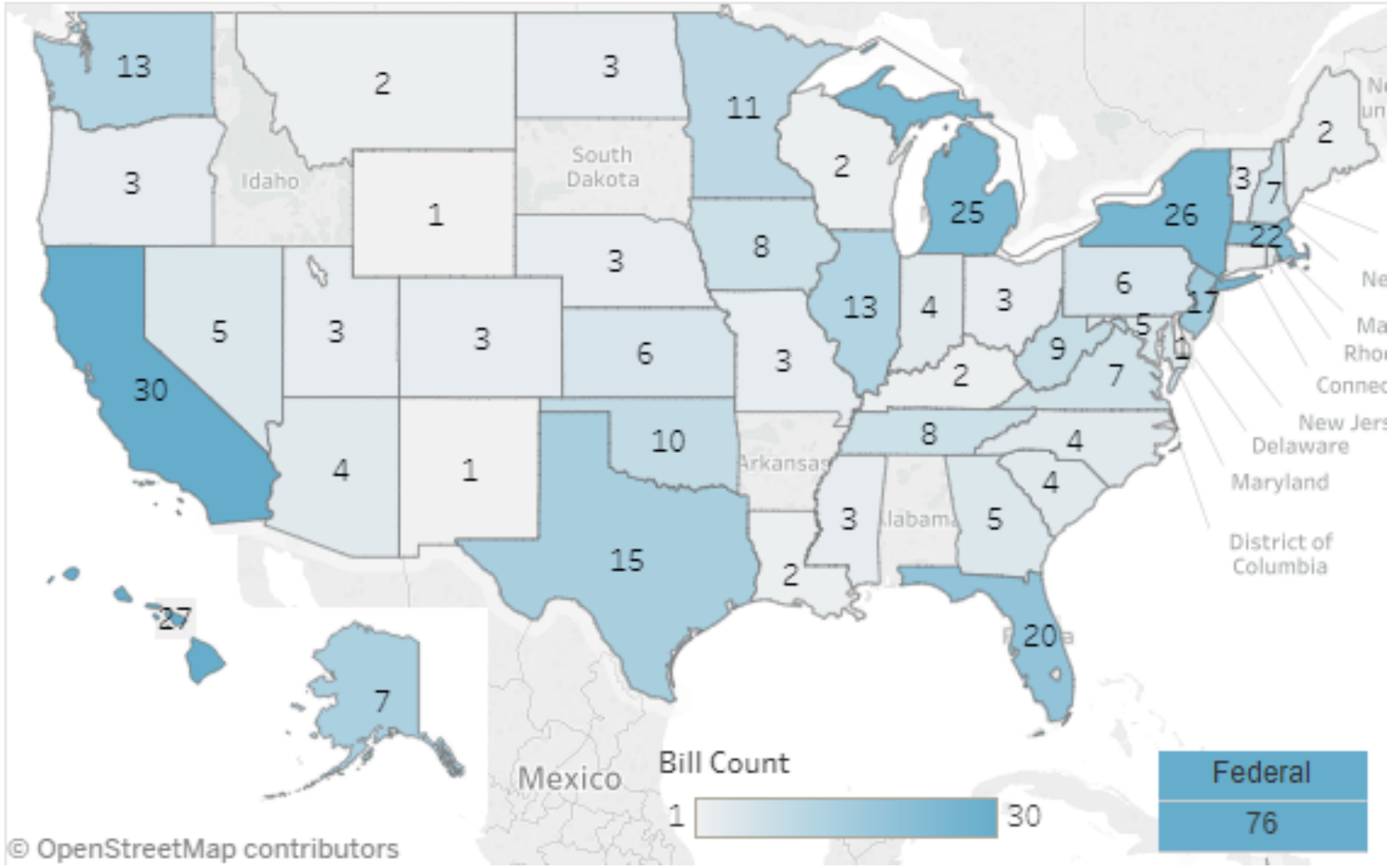


sUAS Rule (Part 107 FAR)



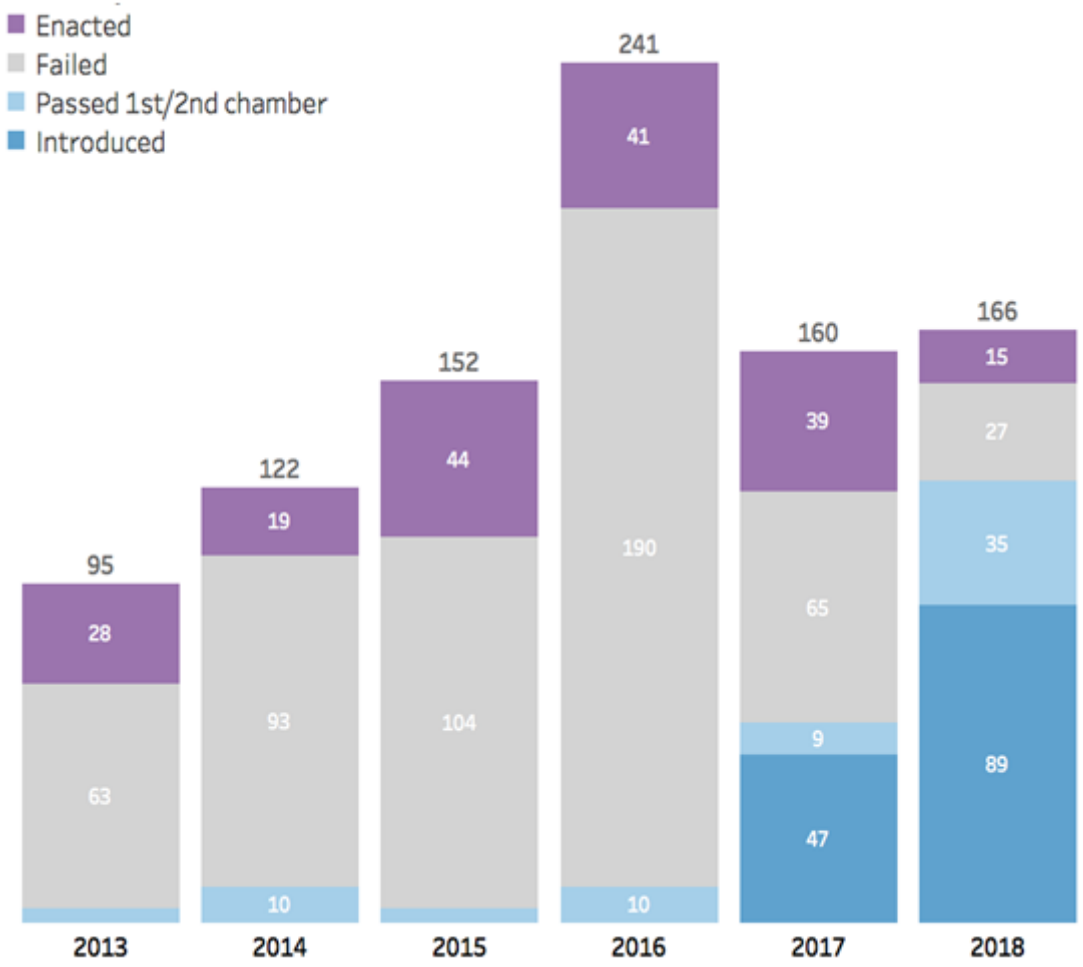
Source: FAA

State UAS Legislation in 2018

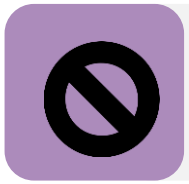


State UAS Legislation in 2013-18

- About 40 UAS bills enacted per year
- A handful of 2017 were carried over
- Decline in state bills since Part 107
- Statewide preemption:
  - Arizona
  - Connecticut
  - Florida
  - Georgia
  - Maryland
  - Rhode Island
  - Virginia
  - Utah



State UAS Legislation in 2013-18



Unlawful Acts
Use of drones to commit existing criminal acts (harassment, trespassing, etc.)

Law Enforcement
Use of drones by law enforcement and military (procurement, warrant requirements, etc.)

Surveillance
Use of drones for filming and photography without prior consent

Security Concerns
Use of drones over critical infrastructure, prisons, hospitals, schools, sports stadiums, and during wildfires

Hunting/Fishing
Use of drones for hunting/fishing, or to prevent hunting/fishing

Study Committees/Education
Legislative tasks forces studying drone technology and impact

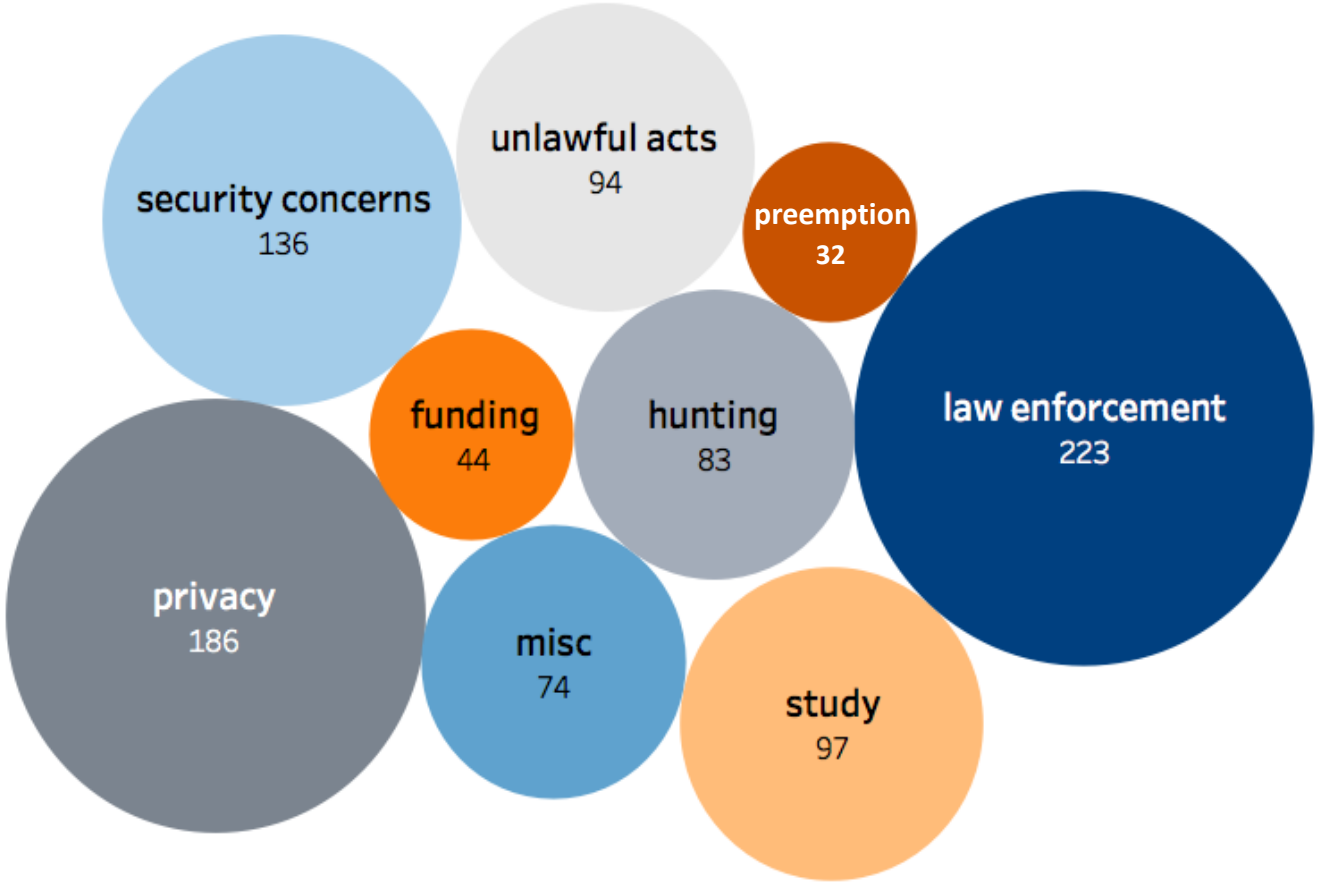
Preemption
Preempting local UAV laws with state laws

Funding
Grants and appropriations for drone procurement, education, and test sites

Miscellaneous
Registration/insurance requirements, agricultural uses, etc.

State UAS Legislation in 2013-18

- 24% of UAS bills regulate UAS use by law enforcement, making it the most common type of drone bill
- 85% of UAS bills about security concerns have been introduced between 2016 and 2018
- ~45% of all funding bills were enacted
- ~40% of all preemption bills were enacted



Hogan Lovells

Lisa Ellman

Partner and Chair, Global UAS Practice, Hogan Lovells

Co-Executive Director, Commercial Drone Alliance

SIA Panel

Development of rules and regulations around drone security have fallen behind existing and future technology…

POLICY

INNOVATION

2017-2018: Years of Drone Security

- As emergence of drones has grown, national security agencies raised drone security as important policy issue:
  - Remote ID: Whose drone is that?
  - Counter-drone technology: How to mitigate potential drone threats?
- June/November 2017: First-ever Domestic Drone Security Summits between industry and government
- October 2017: UAS Tracking and ID ARC presented recommendations to FAA; published December 2017

Policymakers worried about:

- *Careless*
- *Clueless*
- *Criminal*

2017-2018: Years of Drone Security

- Counter-drone Enabling Legislation:
  - Various drafts have been introduced; Senator Johnson legislation, incorporating Senator Carper amendments, have passed out of the Senate HSGAC
    - Possibility that this legislation will be passed as part of FAA Reauthorization
  - Legislation is narrow: Enables DHS and DOJ to use counter-drone technology in certain situations
    - Prior versions of legislation had enabled government-wide use of counter-drone technology
    - Includes privacy and civil liberties protections, and requires coordination with Department of Transportation
- Section 336 "fix" and comprehensive remote identification framework also necessary

Policymakers worried about:

- *Careless*
- *Clueless*
- *Criminal*

Examples of a “Rogue UAS”

- UAS operated to harass or stalk individuals
- UAS that are hazardous to people/property on ground
- UAS interfering with manned aircraft
- UAS operations that invade privacy or create nuisance
- UAS operations involving spying on a company or misappropriation of company proprietary information or trade secrets
- UAS operated in an area where it is not supposed to be

Recent High-Profile Incidents Involving Rogue UAS

- UAS crashing on White House lawn
- UAS with radioactive material landing on Japan Prime Minister's rooftop
- UAS flying within 6 feet of German Chancellor
- Smugglers using UAS to fly drugs and other contraband into prisons
- Suspected UAS collision with airliner at Heathrow Airport
- UAS crashing in stands at Petco Park in San Diego during Padres baseball game

Counter-UAS Methods Include:

- Targeting operator and neutralizing operator's ability to operate the UAS
- Targeting the UAS and destroying it or preventing it from operating in inappropriate areas
- Targeting the UAS's command and control links or its navigation technology and flying the UAS away from an inappropriate area

ANIMALS

Dutch Anti-Drone Police Eagles Ready For Duty

The DJI Phantom menace

By Kelsey D. Atherton *September 13, 2016*

Real Life Example: Boggs v. Meredith

- Case in federal court in the Western District of Kentucky.
- Meredith shot down a UAS flown by Boggs over Meredith's land.
- Boggs sought a monetary recovery for damages to his UAS, and a declaratory judgment that a landowner is not permitted to shoot down a UAS operating in the navigable airspace in the U.S.
- Boggs claimed the U.S. navigable airspace immediately above a landowner's property is not owned by the landowner.
  - *Thus a UAS flight over the land cannot constitute a trespass.*
- U.S. Supreme Court has never addressed this issue, although it did address a related issue in U.S. v. Causby in 1946.
- The Boggs case asked important questions regarding -
  - *Landowner's property rights in the airspace immediately above the land*
  - *UAS operator's right to operate in the navigable airspace immediately above another's land*
  - *FAA's exclusive sovereignty over the navigable airspace in the U.S.*

Legal Issues Raised by Destroying or Disabling a UAS

- Potential criminal liability under Federal Law
  - A UAS is considered an “aircraft” under FMRA of 2012 and the Federal Aviation Regulations
  - Under 18 U.S.C § 32 - Destruction of aircraft or aircraft facilities, destroying or disabling an aircraft is a Federal crime punishable by up to a 20-year prison sentence.

- Potential criminal liability under Virginia state statutes
  - For example, in Virginia, intentionally damaging property is a Class 1 misdemeanor or a Class 6 felony depending on the value of the property (VA. Code Annot. Sec. 18.2-137(A); 18.2-1347(B)).

Legal Issues Raised by Destroying or Disabling a UAS (Cont'd)

- Potential criminal liability under local ordinances
  - For example, under Louisa County, Virginia - Code of Ordinances Sec. 54-9, breaking, injuring, defacing, destroying or preventing the operation a vehicle, aircraft or boat constitutes a Class 1 misdemeanor

- Potential civil liability for damages under Virginia common law
  - For example, civil liability for the tort of conversion of personal property by depriving the owner of his possession or use of his personal property
  - Potential civil liability for personal injury or property damage in the event that someone is injured or property is damaged on account of the counter-UAS activity

Legal Issues Raised by Hacking into, or Interfering with, a UAS's Command and Control Link on Its Navigation System

- Federal law makes it illegal to interfere with wireless communications (47 U.S.C. §§ 301, 302a(b), 333).

- Most counter-UAS technology that involves the use of a radio transmitting device to interfere with the UAS's wireless communications would be illegal under Federal law, and could give rise to civil and criminal liability.

- For example, using a device to interfere with a UAS's radio communications, GPS link, Wi-Fi, or Bluetooth connection would be illegal.

Legal Issues Raised by Hacking into, or Interfering with, the UAS's Command and Control Link on Its Navigation System (Cont')

- In addition to potential violations of Federal law, use of a transmitter jammer might be a felony under Virginia's Computer Crimes Act (Va. Code §18.2-152.1 et al.).
- Potential felonies under the Virginia Computer Crimes Act include:
  - Computer fraud;
  - Computer trespass;
  - Computer invasion of privacy; and
  - Computer as instrument of forgery.

What Are the Risks of Deploying Counter-UAS Technology?

- Possible violation of Federal, state, and local laws and exposure to government prosecution
- Possible exposure to a civil tort action for damages incurred by the UAS operator
- What if the technology does not work?
  - *Possible breach of contract by the designer, manufacturer, or maintainer of the technology*
- What if the technology works, but its use causes an accident injuring persons or property?
  - *Product liability exposure*
  - *Operator negligence liability exposure*
  - *Harm to the facility that was supposed to be protected or persons working at the facility*

How Should the Legal Issues and Risks Be Addressed?

- Laws need to be passed at both the Federal and State level to authorize the appropriate and safe use of Counter-UAS technology in narrowly defined circumstances.
  - *What those circumstances are should be the focus of a healthy public policy debate.*
- Industry "best practices" for use of Counter-UAS technology need to be developed.
- Appropriate insurance products for Counter-UAS technology need to be developed by the insurance industry, and appropriate insurance coverage should be obtained by all operators of the technology.
  - *Users of Counter-UAS technology should consult their insurance broker.*
- Any deployment of Counter-UAS technology should be preceded by a thorough safety and legal review.