Chapter 10 UV, Social Networks & Covid-19 Defense [Shay]

Student Learning Objectives

The student will obtain an understanding of how the federal regulation of UAS operations by the FAA, are affected by current Fourth Amendment, privacy laws and their interpretation at national, state, and local levels. Earn an understanding of how privacy laws have been applied to UAS and the common technologies they carry in their payloads. Develop an understanding of layered system of FAA regulation, matched with state and local level UAS legislation.

Key Concepts

1. Understanding the creation and evolution of the UAS legislative and regulatory operating environment, both federally and locally.
2. Understand the relationship between the CoViD-19 pandemic and UAS systems, their diverse technical payload and freight carrying abilities.
3. The ability for UAS to enable a “Surveillance State”, facilitating fear and the potential ‘over-regulation’ which could hinder and undermine continued UAS industry growth in America.
4. Application and interpretation of the Fourth Amendment, privacy laws, and why they matter to UAS operators and industry.
5. FAA Regulations v. State Laws: Which is better for the continued growth and progression of the UAS industry and public privacy rights as a whole.
A Recent Rise in UAS Operations, Privacy Concerns and A Pandemic

The recent novel coronavirus (CoViD-19) pandemic has been a black swan event which has brought many modifications to our local, national, and global societies and norms. (Taleb, 2007) Many of these required changes, such as those related to the desire for increased usage and relaxed regulation of unmanned aerial systems (UAS) will likely have the intended effect of increasing UAS usage but may the unintended consequence of affecting the interpretation and application of constitutional law.

The UAS industry with the rapidly evolving technologies it employs, is by definition a disruptive technology. According to Margaret Rouse on WhatIs.com, “A disruptive technology is one that displaces an established technology and shakes up the industry or a ground-breaking product that creates a completely new industry.” (Rouse, 2016) This disruption of legacy industry will continue and gain momentum, as UASs increasingly make their way into the average American experience.

These flying robots are natural candidates to perform pandemic related tasks categorized into the “three Ds”: dull, dirty, or dangerous. (Diab, 2014) Until recently, the Federal Aviation Administration’s (FAA) regulatory framework governing UAS and their industry was evolving at a slow, methodical pace. With the onset of the pandemic, UAS regulation has loosened to allow more industry partners to help the government combat the disease. Due to the ever-growing list of payloads and tasks UAS can and do perform, their new uses have made some citizens nervous and rightfully concerned about their privacy. As with all innovation and change, the UAS disruptions will have pros and cons. UAS sensors and payloads have the potential to capture, record, and upload huge amounts of data to their corporate owners and sponsors in near real time. Whether you are a willing part to this collection or not, there are privacy concerns regarding the collected data and for what it
can and will potentially be used. The Fourth Amendment protects citizens from unreasonable searches and seizures of individuals and their property. (Smentkowski, 2020) Whether or not the data collected and used by UAS, that pertains to individuals and their activities in both public and private locations, is protected by our Fourth Amendment rights or not is a brewing debate and one that could delay this disruptive technology’s contributions to our society and economy.

As UAS use continues to grow without specific legislation or regulation protecting privacy, a legal conflict will likely ensue. This conflict and its outcome will undoubtedly affect the interpretation and application of constitutional law. We will look at the changes in the FAA’s regulatory environment applicable to UAS, the court cases most likely to be referred to as precedence when UAS operation affects privacy concerns, any current cases in the federal system with potential to become or change the legal precedence for UAS' impact on Fourth Amendment rights[1], and the pros/cons of UAS v. ‘Public Privacy’ being regulated at the national level by the FAA or by a more Federalist approach at the local and state levels.

**Background to the FAA’s Regulatory Environment**

To examine an environment and the effects a new technology has on that environment, we first need to understand how the environment was created and existed prior to the new technology. It is important to understand why the FAA and not the legislative bodies, have the authority to regulate private and commercial UAS operations within the national airspace (NAS). Congress grants this regulatory authority to ensure experts with aerospace experience are making the decisions concerning the safety and accessibility of the NAS. When Congress mandated the FAA establish rules for the regulation of UASs, they started with drafting new rules for private and commercial operators to establish CFR Title 14, Part 107. Commercial operators who wanted to carry freight via UAS would
also be regulated by meeting the applicable requirements in CFR Title 14, Part 135, which all air carriers must comply with.

To appreciate the different roles of the FAA and state legislations, as they pertain to UAS, and their effects on public privacy, it helps to review an online press release dated 20 July 2018, from the FAA. The title of the web page is, “Press Release – FAA Statement–Federal vs. Local Drone Authority.” (FAA, 2018) The primary purpose of the press release is to remind readers what gives the FAA its authority over the entire NAS, and allows it to preempt state and local governments from legislating UAS operations; EXCEPT for areas traditionally governed by state or local legislation i.e. land use, zoning, privacy, trespass[2], and law enforcement usages. (FAA, 2015)

There are two congressional laws which encompass most of the federal legislation pertaining to UAS; the FAA Extension, Safety, and Security Act (FESSA) of 2016, and the FAA Reauthorization Act of 2018 (H.R. 302). There are others, such as the National Defense Authorization Act of 2017, which makes it legal for the Department of Defense to shoot down UAS over certain areas, but these only have small or single sections pertaining to UAS. (Rupprecht J.) The FESSA provided one key article of particular importance to this chapter; the article which streamlined the FAA process for approval of interagency teams to use UAS in emergency situations. (U.S. Senate, 2016) We’ve included a summary of the Part 107 and 135 changes made by the FAA to address the CoViD-19 pandemic in Appendix C. In short, the FESSA was exactly what the FAA used when it issued the emergency changes at the beginning of the pandemic to rules established under the direction of H.R. 302. (FAA, 2020)

As stated, most of the relevant legislation Congress has passed pertaining to UAS was included in H.R. 302. For reference, we’ve included a summary in Appendix A. The primary UAS result of
H.R. 302 was the FAA’s establishment the regulations in the Code of Federal Regulations (CFR) Title 14, Part 107 requirements. The operating environment created by H.R. 302 can be summarized by the following: operators of UAS must obtain a certification from the FAA, must be operated below 400', must be operated within visual sight of pilot, a pilot can only operate one UAS at a time, cannot be operated over people, and cannot be operated at nighttime. For reference, a summary of the complete set of CFR 14, Part 107 rules pilots or UAS operators must follow is located in Appendix B. Since the establishment of the Part 107 rules, any operators who wish to deviate outside these rules is required to request a waiver through the FAA.

To review the legal operating environment created by the H.R. 302, and its impacts on privacy, a few sections of the law, and the deliverables required by those sections, are of particular importance to this study. The first of these is Section 357, titled “UNMANNED AIRCRAFT SYSTEMS PRIVACY POLICY UAS.” The summary of this section is quite brief but clear, “UAS operations shall be carried out in a manner that respects and protects personal privacy consistent with the United States Constitution and federal, state, and local law.” Although this statement in the law appears to be quite vague, it ensures the state and local authorities will have a say in how UAS operations and their effects on privacy will be litigated.

The next applicable area of H.R. 302, Section 358, and titled “UAS Privacy Review” mandates a deliverable from the Comptroller General of the United States National Telecommunication and Information Administration. The deliverable is a report to congress from the Comptroller General because this is the office of government that has been working on a review of federal, state, and local statutes, meant to address UAS impacts on personal privacy. The Comptroller General’s office was originally tasked with this review by President Obama in his Presidential memorandum “Promoting Economic Competitiveness While Safeguarding Privacy,
Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems,” dated February 15, 2015. (Obama, 2015) This report was originally due to Congress 180 days after the signing of the law, around April 2019, and has not been produced or delivered according to the authors’ research.

The final section of H.R. 302 pertaining to this study is Section 378, titled “Sense of Congress.” The purpose of this section is to require anyone who operates UAS for hire, except the media, to have a written privacy policy which must be made available to customers and the public. This policy is required to disclose the collection, storage, use(s), destruction, and sharing of any data collected during the UAS operations. (Zoldi, 2020)

It should be pointed out concerns over the changes made to UAS regulation by the FAA have not created a wild west free for all of UAS activity in the U.S. The changes made to the FAA’s regulations were largely administrative. (FAA, 2020) There is an increasing amount of UAS operating companies working to get into the CoViD-19 fight. Here are examples of newly approved applications for waivers to operate UAS during the pandemic:

- March, Wing begins making home deliveries of dry goods and medicines to homes in Virginia during CoViD-19 induced lockdown, through FAA approved trial (Summers, 2020)
- April 27, UPS and Matternet get approval to support a quarantined retirement community with UAS deliveries from a local CVS pharmacy (Bonifacic, 2020)
- May 27, the FAA granted Zipline an emergency BVLOS waiver to fly medical supplies in North Carolina. The flights will cover 20-30 miles and carry up to 4 lbs of medical personal protective gear and supplies (de León, 2020)
- July 14, UPS and Matternet approved to deliver time and temperature critical medicines and PPE to medical facilities in N.C. (McNabb, Matternet and UPS Expand Hospital Delivery
July 28, Cotton Bowl is first outdoor stadium to use UASs spraying disinfectant in an effort to combat CoViD-19 and support sporting events. (Davis, 2020)

How Previous Case Law Concerning UASs or the Technology They Carry, Has Been Applied Toward Privacy and Fourth Amendment

To begin the examination of cases involving UASs, privacy concerns and the Fourth Amendment; we will start with a relatively recent case, Brossart v. North Dakota (2015)[4]. The following is a summary of the case and its related features to our study. The case involved local law enforcement requesting a UAS from the U.S. Customs and Border Patrol to take photographic evidence when local authorities were confronting Brossart over allegations of cattle theft. This is the first known incidence in the U.S. where evidence, collected by a UAS, without a warrant, was used against an American citizen. Brossart looked to dismiss the charges due to his belief his Fourth Amendment rights were violated by the UAS invading his privacy.

His defense cited support from a SCOTUS decision in Kyllo v. U.S. (2001)[5]. In this case SCOTUS ruled to throw out evidence obtained by infrared technology without a warrant. The North Dakota Supreme Court ruled the evidence from the UAS was admissible due to the precedence set by SCOTUS in the ruling of California v. Ciaraolo (1986)[6]. In this case SCOTUS ruled an individual's privacy and Fourth Amendment rights are not violated when their actions can be observed from an aircraft in navigable airspace, in this case, from 1000 feet above ground level (AGL). With these decisions by the North Dakota Supreme Court, Brossart was the first American citizen to serve federal prison time, due to evidence obtained with a UAS. (Bomboy, 2014)
To further examine the issue of UASs and privacy, it is sometimes necessary to form a scenario using a very particular set of assumptions. This was precisely the case made by David Sella-Villa in his work, *Drones and Data: A Limited Impact on Privacy*. We will look at just how a UAS would affect privacy within the set of assumptions he describes in his paper, and what happens when you alter the assumptions. Let us start with a UAS being operated with a simple visual light spectrum camera. The visible light spectrum simply put is light or images visible to the naked eye. Further we are only looking at scenarios where the UAS are being operated and piloted legally. Finally, it is important to know the author’s definition of privacy, which is “privacy simply means freedom from unwanted visual observations in and about the home.” (Sella-Villa, *Drones and Data: A Limited Impact on Privacy*, 2020)

Another key condition to be noted concerning this paper and the author’s view point is the statement and reference that UAS flights beyond visual line of sight (BVLOS), “have been reserved exclusively for military and search-and-rescue operators.” Although this may have been true at the time of his writing and publishing, the UAS industry has been moving towards BVLOS flights as being absolutely necessary for UAS delivery and other commercial uses. (Seeking Alpha, 2019) Within these viewpoints and assumptions, the author examines and makes a convincing argument that UASs outfitted only with visual light spectrum cameras do not significantly challenge the jurisprudence of privacy law in the U.S. However, the author does concur that UASs are significantly able to exploit traditional assumptions about privacy and trespass as defined in our legal system. (Sella-Villa, *Drones and Data: A Limited Impact on Privacy*, 2020)

The most significant contribution of Mr. Sella-Villa’s paper to this chapter’s study is his break-down of why UASs outfitted with visual light spectrum data collection devices alone, will not challenge our
Fourth Amendment rights, as the laws are currently written. Much of his legal reasoning for this has to do with the precedence of “Third Party Doctrine”. The basis of this concept has been established through several cases heard and decided by the SCOTUS, and “maintains that one cannot assert a privacy interest over something that has been knowingly shared with a third party.”[11] The two primary ideas behind this premise according to the author’s listed assumptions, are; the UAS is operated legally, without trespass and the UAS’ image capture software stores images remotely. This is almost always true because of the how UASs share what they are ‘seeing’ in near real time with their operators. (Sella-Villa, Drones and Data: A Limited Impact on Privacy, 2020)

Additional examples of how UAS and their technologies potentially impact privacy concerns can be found in products of the Congressional Research Service, which prepares and drafts reports for Congress[12]. One particular we will examine is titled, Drones in Domestic Surveillance Operations: Fourth Amendment Implications and Legislative Responses, by Richard M. Thompson II, a Legislative Attorney. His report specifically looks at and addresses the use of UAS by law enforcement to conduct surveillance both with a warrant and without one. Key points highlighted in this report are how a UAS is essentially a data collection device, and that without its high technology payloads, should not be considered a threat to Fourth Amendment rights or privacy laws. The author suggests that many of the known high-tech payload capabilities of UAS (keep in mind this article was written in 2013) have been addressed sufficiently in federal or state laws. In the conclusion however, the author concedes that where the capabilities of a UAS and its payload is headed, could be a place that will stretch our current privacy and Fourth Amendment protections to their limits. (Thompson II, Drones in Domestic Surveillance Operations: Fourth Amendment Implications and Legislative Responses, 2013)

A second report from the Congressional Research Service, also
written by Thompson, but slightly later in 2015, is titled Domestic Drones and Privacy: A Primer. This report, its cited sources, and the author’s legal perspective provide a comprehensive understanding of the complexities surrounding UAS and our current legal framework’s ability to contain the privacy invasion concerns and unlawful search threat posed by the potential of UAS payloads. (Thompson II, Domestic Drones and Privacy: A Primer, 2015)

Technologies of the Digital Age and the Fourth Amendment

Further study of the existing legal and regulatory landscape and the dangers of its lack of specific privacy protections, can be found in The Sky Police: Drones and the Fourth Amendment, by Jessica Dwyer-Moss. Her work is a fairly comprehensive examination of the wide array of technologies UASs can bring to domestic authorities’ surveillance methods. Applicable legal cases, pertaining to the individual technologies and their impact on the Fourth Amendment are also reviewed. This work uses many of the case studies we have discussed previously to show how dated these references are compared to the twenty first century technologies UASs will present to test them. An important case she brings to the discussion is Carpenter v. United States[13]. This case was not decided by the time of her publishing, but she correctly included it due to its topic being cell phone location records being used without a warrant, in the conviction of a robbery suspect. Shortly after she published her article, SCOTUS decided the case. In their decision it was determined that cell phone location data is constant and should be considered from the legal standpoint like GPS data, as protected by the Fourth Amendment, requiring law enforcement to obtain a warrant for its sharing and use as evidence. This is seen as a win for privacy advocates and a blow to the Third-Party Doctrine’s coverage of modern electronic data. (Dwyer-Moss, The Sky Police: Drones and the Fourth Amendment, 2018)

Another case highlighted by this work is Riley v. California[14]. In
this case SCOTUS had to decide if law enforcement could search an individual’s cell phone upon arrest. The court in its decision made particular note that the main reason an officer is allowed to search an individual under arrest is to preserve evidence and ensure safety of the officer and person under arrest. SCOTUS concluded digital data could not harm an officer or help the individual escape, a warrant was required in order to search a cell phone. (Dwyer-Moss, The Sky Police: Drones and the Fourth Amendment, 2018) This ruling could be immensely important to UAS operators and companies, since the primary thing UASs will “deliver” in the near future is data.

Dwyer-Moss also examines the rulings in cases where aerial observation was a key component, although Brossart v. North Dakota was not among them. Dwyer-Moss is an Assistant General Counsel at the Department of Defense whose extensive areas of practice include but are not limited to, Privacy Act, Privacy and Civil Liberties, and Intelligence Oversight. (Dwyer-Moss, Jessica Dwyer-Moss’ Profile, 2020) Her knowledge, opinions, and expertise in subjects discussed in this chapter has been immensely helpful in establishing the current environment and upon where it can be improved.

An important legal construct to understand when we look at how UASs and the data they can collect effect privacy and the Fourth Amendment is known as the Miller Doctrine or Third-Party Doctrine. This extremely important concept in Fourth Amendment law came from two decisions, Smith v. Maryland[15] and United States v. Miller[16], by SCOTUS in the 1970s. These two decisions both referenced SCOTUS's decision in Katz v. United States[17]. In the Katz decision SCOTUS ruled that Fourth Amendment protections not only applied to an individual’s tangible things but also to an individual’s reasonable expectation of privacy. United State v. Miller’s decision helped to frame and contain this expectation by establishing that no reasonable expectation of
privacy can be expected when one uses the services of a third party, in this case the phone company, to contact (dial numbers) another party. The conversation between yourself and the party you contact is protected and would require a warrant for authorities to access[18], but the number you dialed, the time you dialed it, and the connection made, were ruled to be business records of the third party, and therefore could be subpoenaed[19]. In Smith v. Maryland, a similar decision was handed down stating that records such as deposit slips, and checks used by an individual to perform business with the bank were not protected by the “reasonable expectation of privacy”[20] outlined in Katz because the customer was voluntarily sharing and disclosing their business with a third party[21]. All these decisions taken together have come to be known as the Third-Party Doctrine. This doctrine and its application to twenty-first century technology is highly applicable to the subject matter of this chapter. (Thompson II, The Fourth Amendment Third-Party Doctrine, 2014)

**Examinations of Technologies on UASs due to CoViD-19**

An examination of all the individual technologies UASs are capable of carrying and collecting data with, is beyond the scope of this chapter. In an effort to discuss these technologies in a relevant perspective, we will discuss one cutting edge technology and how it is being used in the CoViD-19 pandemic. This technology was selected to be the example of how new technologies can raise privacy and Fourth Amendment concerns. The technology is a new form of bio-identification. A recent study of this new technology demonstrates just how capable UASs have become at being private data collection devices. The recent research study proved how UASs can pick-up and monitor the cardiorespiratory signals from multiple individuals while flying at 200 feet AGL. (Al-Naji, 2017) This type of progress and advancement in a potential payload’s abilities are the kinds of advancements, once unleashed on society ‘for its own good’, are very difficult to discontinue or legislate after the fact. Although, as we will discuss in a later section, efforts to
Another work to study modern technology and its impact on the Fourth Amendment, is a short but important contributor to this chapter. The article is *Drones and the Fourth Amendment* by Robert E. Smith and published in the May 2017 edition of Privacy Journal. In his work, Smith concentrates on the implications of the government’s use of UAS equipped with surveillance technologies. His first point is how there is an established precedence for the government to use visual camera-based surveillance both with and without warrants. These instances without a warrant require certain circumstances to exist such as “possible destruction of evidence, escape of a suspect, danger to the police or public.” However, any video surveillance that includes audio recordings must have a warrant. This is due to established requirements in the federal electronic surveillance laws. Smith boils down the two most important cases, in his opinion, for UAS surveillance by the government. These are *Kyllo v. U. S.*, due to the use of thermal imaging equipment; and *Jones v. U.S.* and its use of GPS tracking data. The final point to stress from this article is the one Smith makes by including words from the late Associate Justice Anton Scalia, who wrote the majority opinion in both cases. In the majority opinion of *Jones v. U.S.*, Justice Scalia wrote:

“This court has to date not deviated from the understanding that mere visual observation does not constitute a search...It may be that achieving the same result through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy, but the present case does not require us to answer that question. We may have to grapple with these ‘vexing problems’ in some future case where a classic [physical trespass] is not involved.”

*Associate Justice Anton Scalia,* (2012)

In another fairly prophetic portion of the major opinion, Justice Scalia also noted, “the transmission of electronic signals without
trespass” falls under Fourth Amendment restrictions. (United States v. Jones, 2012) (Smith R. E., 2017) To date, from the author’s research, no further decision by the Supreme Court has addressed the potential of electronic signals to be included in or excluded from Fourth Amendment protections.

**Federalism or Federal Regulation of UASs**

To better understand the role of Federalism in UAS and privacy legislation and regulation, we will look at both the pro-Federalism view, and the con-Federalism (or continued FAA regulation) view. Available academic materials were heavily sided toward the pro Federalism argument of UASs and their abilities being regulated at a local level. The con arguments cited are predominately articles from economic advocacy groups.

**Pro Arguments**

To begin the look at the “Pro” side of the argument, an essay by Margot E. Kaminski titled Drone Federalism: Civilian Drones and the Things they Carry, was reviewed. Her essay is rooted in the belief that there are two basic areas of UAS privacy legislation, UAS use by law enforcement, and UAS use by civilians. She notes the FAA’s regulations have specifically allowed law enforcement to use UAS technology since the Congress’s original UAS legislation[22]. A common theme throughout this essay is the regulation and control of UASs and their payloads is best legislated by local authorities because of their “experience regulating other forms of civilian-on-civilian surveillance.” Perhaps the most notable argument for local authorities to regulate the privacy concerns around UASs, is one where she points out that an overarching and preemptive bill by Congress or omnibus privacy regulation by the FAA would, to be effective, be too restrictive in nature and run the real risk of infringing on UAS operators First Amendment rights. The essay also points out the FAA Modernization and Reform Act of 2012 (112 Congress, 2012) does not mandate the FAA take up the issue of privacy, and suggests the reason for this is likely the tradition
of states and local governments enacting privacy controls at their levels. Her conclusion has a focused warning against Congress getting in too big of a hurry to control the budding UAS threat, and to allow the state and local authorities address the issue in their own jurisdictions. (Kaminski, 2013)

The next work doesn’t so much argue for the states to regulate UASs as it assumes their control by local authorities is what is best for the growth potential of the UAS industry as a whole. In their report, Which States Are Prepared For the Drone Industry, Brent Skorup and Connor Haaland from George Mason University study which states have prepared themselves to take advantage of the economic benefits the UAS industry can bring. The basis of their work is the assumption that states can best be ready to reap these benefits by creating “drone highways—aerial corridors directly above public roads.” The authors research which states have the appropriate legislative conditions to enact UAS highways. They do this documenting and grading all 50 states on their preparedness in 5 factors for UASs and enacting UAS highways. The factors are: an airspace lease law on the books, an avigation easement law, a law vesting air rights with landowners, some sort of aviation advisory committee at the state level, and a look at the number of UAS jobs (per 100,000 residents) in each state. Of note, North Dakota was ranked #1, Arkansas #2, Vermont #3, Kansas #32, and S. Carolina #50. The ‘air’ highways described by Skorup & Haaland are one of the concepts proposed that would make the UAS industry more palatable to property owners concerned about their privacy and is a novel way for states to enact similar legislation to maintain an economically even playing field. Whether this legal construct for UASs catches on and is enacted or not remains to be seen. (B. Skorup & Haaland, 2020)

The final piece of pro-Federalism research comes from a guest article published by Dronelife.com, but written by Jonathan Hayden, Esq. It is titled Why the Drone Community Should Not Embrace
Exclusive FAA Control of Drone Regulations. In this article, Mr. Hayden begins by setting the scene twenty years into the future. He assumes that many of the FAA’s UAS regulatory arm members and experts are former employees from the larger of the companies within the UAS industry. This is not an uncommon or unlikely occurrence since other federal regulatory bodies are currently made up of such professionals. The problem Mr. Hayden foresees with this is if the FAA has complete regulatory control, this can create an environment where the large corporations, who are primarily concerned about profit, will have too large of a voice in the regulatory process. An idea which has been demonstrated in other industries on multiple occasions. This could even create a reality where landowners are prevented from flying UASs over their own property because they may interfere or endanger commercial UAS activity in some scenarios. The best possible answer to this is for the states and local governments to have control over their jurisdictions. (Hayden, 2020)

Con Arguments

The first argument against a federalism approach to UASs, privacy and the Fourth Amendment is a revisiting of The Sky Police: Drones and the Fourth Amendment, by Jessica Dwyer-Moss. As a backdrop to the overall concerns from UASs on privacy in her paper, Ms. Dwyer-Moss opens her work with the following quote, “In the far distance a helicopter skimmed down between the roofs, hovered for an instant like a bluebottle, and darted away again with a curving flight. It was the Police Patrol, snooping into people’s windows.” (Orwell, 1949) The majority of her paper examines a collection of case law which can and will be used as precedence to decide UAS and high technology legal disputes in the near future. The problem, as the Dwyer-Moss sees it, is that precedence can be overturned by a new subjective definition of societies “reasonable expectation of privacy” and regulations can be changed by an agency submitting a proposed change and allowing it to be committed on before changing it. The only sure way for Fourth Amendment protections to be guaranteed is for Congress to take up the matter and legislate
visual and electronic surveillance norms. She sums up her argument by stating that “A national approach is ideal, but in the absence of federal legislation, some states have begun to regulate drones for themselves.” (Dwyer-Moss, The Sky Police: Drones and the Fourth Amendment, 2018)

An additional argument against the state and local governments controlling UASs is presented in States Rush to Regulate Drones Ahead of Federal Guidelines, by Sarah Breitenbach. This article uses what the states have already tried to do in their legislation to make the argument that Congressional law and Federal regulation will be the best way to protect privacy without stifling the natural innovation of this disruptive technology. In 2015 California's Governor vetoed a law that would have made it illegal for any commercial or private UAS to fly less than 350 feet AGL over private property without consent. Had this legislation been enacted, UAS delivery in California would have been severely set back. An interesting point in this article is when the author notes the ACLU has not requested tighter regulation of UASs due to their belief that most privacy concerns posed by UASs are covered by laws already on the books. In a further comment, the ACLU attorney, Chad Marlow suggested state laws limiting UAS activity can actually harm society by preventing the filming of illegal activity. (Breitenbach, 2015)

A Look at UAS Federalism in Action

In order to understand what state legislative responses have been to disruptive UAS and the technologies they carry; we will review state legislation whose primary purpose was to address UAS or their technologies specifically. A comprehensive review of all the state legislation pertaining to our topic is beyond the scope of this textbook. To ensure a more accurate accounting of state UAS laws, two web sites were used to create the collection of laws represented in this chapter. The first was the site of the National
State Legislative Council. (National Conference of State Legislatures, 2020) This site was extremely thorough with its list of UAS impacting legislation and resolutions, up to and through 2019. This sight included laws that addressed newer technology privacy laws in its list, knowing that UAS could or would be outfitted with increasingly sophisticated payloads. The second site was a site dedicated to monitoring state and local governments, called Governing.com, and their adaptation to current events and national cultural trends. One article on this site in particular looked at how state and local governments were using UAS technology as an answer to the CoViD-19 pandemic. (Smith C., 2020) This article and its included database have been kept current through the writing of this chapter.

**State Laws Pertaining to Privacy and UASs Before CoViD-19**

In the effort to understand the different approaches state legislatures took to regulating UAS and their potential to impact privacy, the author first went to the website for the National Conference of State Legislatures[23] (NCSL). This site lists and tracks by each year (from 2013-2019), all state legislatures who introduce UAS law, and each of them that end up enacting UAS laws. A review of all state level UAS laws introduced that pertain to privacy is beyond the scope of this Chapter. Particular attention will be paid to those laws that address privacy concerns in all 50 states. The following is a list of state laws concerning UAS and their impact on privacy or the Fourth Amendment, and their summaries. (National Conference of State Legislatures, 2020)

**Table 1. State Laws and Resolutions pertaining to UASs, their administration and Wildlife (National Conference of State Legislatures, 2020)**
Table Footnote 1—Virginia was the first state to pass a piece of UAS legislation, with the passing of HB2012. This defined what a UAS legally is.

The Table 1 above contains a list of all the state UAS laws and resolutions which pertain to the administration of UASs, with a final column showing the states with laws concerning the use, or prohibition of use, of hunting and fishing with UASs. The inclusion of the laws pertaining to UAS affecting the privacy of hunters/fishers or the rules pertaining to using UAS while hunting and fishing demonstrates a unique look at the priorities of state legislatures as the introduction of UAS technology is growing. The table listed below is a look at which states addressed UAS and their
impacts on personal privacy, either through their physical presence or the data they collect.

Table 2. State Laws and Resolutions pertaining to UAS, their impacts on law enforcement, personal privacy, and wildlife (National Conference of State Legislatures, 2020)

<table>
<thead>
<tr>
<th>Year</th>
<th>Concerning Use by Law Enforcement and Warrant Requirements</th>
<th>Puts a Data Collection, Retention and Destruction Policy in Place</th>
<th>Marx It Illegal To Hack Into or Electronically Disrupt Public Drones</th>
<th>Addresses Landowner Protection</th>
<th>Directly Addresses Privacy Issues and/or Voyeurism Crimes</th>
<th>Addresses Drones in Relation to Hunting and/or Fishing</th>
</tr>
</thead>
<tbody>
<tr>
<td>2013</td>
<td>FL ID IL MT NC OR TN TX VA¹</td>
<td>IL</td>
<td>OR</td>
<td>OR</td>
<td>TX</td>
<td>IL</td>
</tr>
<tr>
<td>2014</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2014 Laws</td>
<td>AK IL IN IA NC UT WI</td>
<td>AK IL UT</td>
<td>LA NC TN UT WI</td>
<td>IN LA NC UT WI</td>
<td>NC TN</td>
<td></td>
</tr>
<tr>
<td>2015</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2015 Laws</td>
<td>MA NV ND UT VA</td>
<td>CA FL</td>
<td>AR CA FL</td>
<td>MI NH OR WV</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2016</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2016 Laws</td>
<td>IN OR VT</td>
<td>CA MI</td>
<td>KS CA MI</td>
<td>IN WI</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2017</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2017 Resolutions</td>
<td>OR UT</td>
<td>UT</td>
<td>IN KY NJ OR SD UT VA WV</td>
<td>IN NJ SD UT VA</td>
<td>MN</td>
<td></td>
</tr>
<tr>
<td>2018</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2018 Laws</td>
<td>KY</td>
<td>DE LA WV WI</td>
<td>DE LA PA WV</td>
<td>WV</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2019</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2019 Laws</td>
<td>VA</td>
<td>IN</td>
<td>DE IN TN</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Due to the ever-changing landscape of laws and resolutions at the
state level, a second source listing these laws was used. Automated Unmanned Vehicle Systems International (AUVSI) maintains a site of state and local laws that affect UASs, autonomous ground vehicles and unmanned maritime vehicles. (AUVSI Advocacy, 2020) The information on the AUVSI website was reviewed and found to be more comprehensive, as in there were UAS and robotic bills found on this site, but all bills found on the NCSL were verified on the AUVSI site.

Federal and State Laws Pertaining to Privacy and UAS After CoViD-19

Since the CoViD-19 pandemic’s dominance of societies attention, the methods and instruments used by society to deal with and attempt to contain the disease have not only been addressed by each citizen, but our federal legislative and regulatory bodies as well. The FAA was quick to realize the constraints their regulations were placing on the UAS industry in the name of safety, were needlessly preventing the potential of UASs to be a key tool in the fight against the virus. With this realization, the FAA was quick to put out extensions on any knowledge requirements with the SFAR. The biggest changes made by the FAA to help get UASs into the fight against CoViD-19 has been an effort to quickly return approved waiver requests for BVLOS flight, night flight, and other requests by UAS operators and pilots.

There have been 58 State Law concerning UASs proposed so far this year with only one of them being directly contributed to the CoViD-19 pandemic. (National Conference of State Legislatures, 2020) The number of UAS laws to actually be enacted by states so far this year is only 6. Below is a chart to show the status and topics of state UAS laws pertaining to privacy. For consistency of method, the author made note of how many states continue to address UASs being used in hunting or fishing.

Table 3. Status of 2020 State UAS Legislation (Governing.com, 2020)
Conclusions

UASs are becoming more prevalent in American society and the industry is expected to grow exponentially once BVLOS commercial flights become a reality. In July 2020, it was reported the use of the Low Altitude Authorization and Notification Capability (LAANC) has significantly increased in so far in 2020. In the first 6 months of 2020, a third of the 320,000 LAANC authorizations (it’s been operating since Oct 2017) were submitted by UAS operators and granted by the FAA. (McNabb, LAANC Use Accelerates: Kittyhawk Reports All-Time Record Levels of Activity, 2020) Further evidence of increased UAS activity during the pandemic, the numbers of FAA registered UASs and certified pilots continues to grow. On 10 March 2020 we checked the numbers on the FAA’s “UAS By the Numbers”
website. We checked the site again on 28 July 2020. Only 138 days have passed.

<table>
<thead>
<tr>
<th>FAA.GOV</th>
<th>Drones by the #s</th>
<th>Drones by the #s</th>
<th>Δ</th>
</tr>
</thead>
<tbody>
<tr>
<td>Drones Registered</td>
<td>1,563,263</td>
<td>1,668,243</td>
<td>104,980</td>
</tr>
<tr>
<td>Commercial Drones</td>
<td>441,709</td>
<td>479,902</td>
<td>38,193</td>
</tr>
<tr>
<td>Recreational Drones</td>
<td>1,117,900</td>
<td>1,184,839</td>
<td>66,939</td>
</tr>
<tr>
<td>Remote Pilots Certified</td>
<td>171,744</td>
<td>186,292</td>
<td>14,548</td>
</tr>
</tbody>
</table>

**Table 4. Registered UAS & Certified Pilot growth during the 2nd quarter of 2020 Invalid source specified. Invalid source specified.**

With healthy growth of the UAS industry even during the CoViD-19 pandemic, the importance of understanding how UASs will affect the Fourth Amendment and the privacy rights attached to it are even more important. Since the beginning of the pandemic there have been multiple nations around the world using UASs in their fight against the CoViD-19 virus. (Chen, 2020) Some appear to be using the pandemic to push forward their own desires to increase their surveillance state. (Maynes, 2020) Americans see these situations and naturally fear UASs and their capabilities will facilitate a similar environment here. (Tuccille, 2020) During the chapter, we have reviewed an immense amount of material to study concerns about UAS and their effects on our privacy laws. Many of these references have shared deep concerns UASs will impact our privacy and Fourth Amendment protections. Dissenting views were more difficult to come by but made strong focused arguments our current laws are sufficient for the current level of technology used by UAS. (Sella-Villa, Drones and Data: A Limited Impact on Privacy, 2020)

As pointed out previously, the changes to UAS laws so far during the pandemic have largely been administrative. Without the blanket approval of BVLOS flights, night flights, or commercial freight licenses, there hasn't been an overwhelming number of UAS taking
to the sky and therefore there has been no need for knee-jerk reactions by the Congress or the state legislatures.

The slow and fairly methodical spread and management of UAS delivery introduction appears to be exactly what is necessary for the current environment. The FAA’s focus on safety and free efficient economic mobility in the U.S. NAS, while leaving the issues of law enforcement use, zoning, and privacy to be governed by that state and local authorities (FAA, 2018) appears to be the best mix of Federal oversight and Federalist control for the UAS industry, at the moment. This patchwork approach has been proven for other transportation focused industries such as the automobile industry and maritime industry. We shall see if this remains true for UAS.

**Student Questions**

1. What has been the impact, if any at all, of the CoViD-19 pandemic related regulatory changes to increase UAS use during the U.S.’s pandemic response?
2. Do these changes create an environment where UAS and their payloads can further infringe upon or hamper individuals Fourth Amendment rights?
3. Can you name benchmarked and precedence establishing court cases concerning UAS and the technologies used in their payloads?
4. What situations can you see where privacy and Fourth Amendment rights can be endangered or negated by UAS and their payloads?
5. When it pertains to privacy and UAS, do you think a national approach to regulation, or a Federalist approach is better for the UAS industry? For public privacy protections? For advancing and protecting both?
6. Were your answers to the previous question different? Why?
References


https://www.behorizon.org/russian-a2ad-strategy-and-its-implications-for-nato/


de León, R. (2020, May 27). Zipline, Novant Health launch the


274 | Chapter 10 UV, Social Networks & Covid-19 Defense [Shay]


