Journal of Drone Law & Policy

Volume 2| 2023

THE UNIVERSITY of MISSISSIPPI
SCHOOL OF LAW

AIR AND SPACE LAW PROGRAM
P.O. Box 1848
University, MS 38677-1848
airandspacelaw.olemiss.edu

DEALING WITH DEADLY DRONES: STATES HAVE RIGHTS TOO

Manny Psihountas[*]

ABSTRACT

Over the last decade, the FAA has passed regulations intending to safely integrate drone technology into the United States economy. The effect on today is that companies like Amazon are working to integrate this technology into their practice, but the impact of drone technology is likely to impact more industries than logistical ones: agriculture, construction, insurance, and infrastructure inspection are all areas expected to benefit. In passing these regulations, the FAA ensured safe usage by imposing various operational restrictions, proper licensing, and drone registration. However, there is one aspect that is lacking in this integration: the preventative measures against bad actors. Right now, the only way to report a bad actor is to call a federal agency. In order for drones to become as common as the FAA desires, the manner of addressing conflict must progress with drone use itself. If a criminal uses a drone to commit crimes in a way that poses a threat, local law enforcement must be capable of acting in a swift and decisive manner, as they are the first to respond in many situations. In order to successfully integrate this technology into the public in the long term, there must be ways to prevent bad actors from using drones as a way to shield their malfeasance. Otherwise, this progression will not be sustained.

---

[*] Manny Psihountas graduated magna cum laude from both Wichita State University, where he received a B.S. in Aerospace Engineering, and the University of Mississippi, where he received a J.D. As a registered patent agent, Manny is set to begin as an associate at Sughrue Mion in Washington, D.C., where he will specialize in patent prosecution and litigation.

I. INTRODUCTION

In the late 1990s, unmanned aerial vehicles (UAVs) started to become commonplace among the United States (U.S.) military.[1] Successes from the Israeli Forces made it apparent that drone technology offered a newfound tactical advantage. In the early 2000s, the U.S. military discovered the benefits associated with reducing the size of UAVs;[2] such systems allowed for "quick launch and recovery, which provided real-time observational intelligence to gain a tactical advantage over an enemy."[3] Over time, the systems for these small UAVs became more sophisticated and proven, prompting the interest of civilian innovators.[4]

In the late 2000s, the spark of this new technology invigorated Congress to begin investigating the benefits this technology could have on the economy, and specifically on the commercial industry.[5] Soon after, Congress gave the Federal Aviation Administration (FAA) direct orders to begin the integration of drones into the national airspace.[6] Since receiving the go-ahead, recreational and commercial communities have adopted drone technology at an unprecedented rate.[7] Today, an array of drones are more widely available than ever at affordable price points.[8] While the impact of this technology appears propitious, as with any new technology, a new possibility of benefits accompanies a new possibility of malicious conduct.[9]

Accordingly, it is the job of Congress to ensure that the numerous administrative agencies develop reliable procedures to prevent malicious drone operation. Currently, these procedures

---

[1] *See* BRET TERWILLIGER ET AL., SMALL UNMANNED AIRCRAFT SYSTEMS GUIDE: EXPLORING DESIGNS, OPERATIONS, REGULATIONS, AND ECONOMICS 16 (2017).

[2] *Id.* at 19.

[3] *Id.* at 16.

[4] *Id.* at 21.

[5] *Timeline of UAS Integration*, FED. AVIATION ADMIN., https://www.faa.gov/uas/resources/timeline/ (last updated June 2, 2022) [hereinafter *FAA Timeline*].

[6] FAA Modernization and Reform Act of 2012, Pub. L. No. 112-95, § 332 126 Stat. 73 (2012).

[7] *FAA Aerospace Forecast: Fiscal Years 2021-2041*, FED. AVIATION ADMIN. (2020), https://www.faa.gov/sites/faa.gov/files/data_research/aviation/aerospace_forecasts/FAA_Aerospace_Forecasts_FY_2021-2041.pdf [hereinafter *FAA Forecast*].

[8] TERWILLIGER, *supra* note 1, at 21.

[9] *See* Feynman, *infra* note 40.

are centralized around federal agencies, which are preempting any ability for local law enforcement to rectify a troubled situation.[10] As local law enforcement officers are the first to respond to distress,[11] the federal regulations largely preempt any action that would provide redress. This is problematic when the unlawful drone operation is of minor character;* but when a drone poses an imminent threat, the legal blockade preventing a first responder from efficiently mitigating a threat is unsustainable and must be fixed.

This article will provide an overview of the current state of drone technology and where the future is headed, then will highlight the diverse applications of drone technology by reviewing the beneficial impacts brought to society. After portraying this technology's ability to benefit society, the paper will reveal how that same ability can be manipulated for malicious purposes. Once the array of unlawful conduct is established, the discussion introduces the rules prohibiting such conduct, defense mechanisms to counter unlawful operation, and the laws preventing use of such defense mechanisms. The analysis concludes by illustrating the crippling effect these laws have on the ability of law enforcement to mitigate unlawful drone operation, and the changes that must be made to reinstate local law enforcement's ability to address this evolving threat to public safety. In this way, an efficient protocol will effectuate public acceptance, leading to long-term sustainable growth.

II. DRONE TECHNOLOGY

The impact of drone technology is becoming more apparent as the public continues to adopt it. Generally speaking, while new technologies bring many positive impacts to society, often overlooked is the possibility of abuse and how to deal with such newfound vulnerabilities. With this new drone technology, the down-

---

[10] *See Drones: A Report on the Use of Drones by Public Safety Agencies – And a Wake-Up Call about the Threat of Malicious Drone Attacks*, OFF. CMTY. ORIENTED POLICING SERVS. (2020), https://cops.usdoj.gov/RIC/Publications/cops-w0894-pub.pdf [hereinafter Police Procedures].

[11] *See* FBI, *infra* note 104 ("local and state law enforcement agencies are virtually always the first ones on the scene").

* By minor, the author is referring to conduct that is not imminently threatening life or property, such as trespass or breach of privacy.

side must be understood and addressed before it can be prevented. In this way, society will be able to reap only the positive fruits of this new technology. To fully understand the impact of drone technology, it is important to understand what exactly a drone is and where this technology came from.

A drone is an unpiloted aircraft referred to as an "unmanned aircraft system" (UAS).[12] This paper specifically addresses drones that are less than 55 lbs, classified as "small unmanned aircraft."[13] These aircraft are often powered by electricity ranging from batteries or solar cells; however, more expensive models are capable of being powered by small gas fueled engines.[14] Drones come in many shapes and sizes, and can be manipulated to accomplish many tasks. For instance, a readily available quadcopter drone can fly up to 45 mph, carry a payload of over 1 kg, and last 30 minutes in the air.[15] With these abilities, this drone could be used as a flying camera, to deliver a package, or many other possibilities.

Drones can change the way businesses operate and the way hobbyists enjoy technology, enabling them to see the world from a bird's-eye view. Hobbyists and commercial operators often use drones for aerial photography purposes. Photography can range from families taking overhead pictures of a backyard barbeque, to real estate agents taking pictures for a home listing, to professional videographers filming a documentary, and to anything in between.[16]

As is common with the advancement of technology, the development of the law tends to lag behind.[17] Noticing this trend in the area of drone technology, in 2008 Congress recommended the for-

---

[12] Nanci K. Carr, *Look! It's A Bird! It's A Plane! No, It's a Trespassing Drone*, 23 J. TECH. L. & POL'Y 147, 150 (2019).

[13] 14 C.F.R. § 107.3 (2021) (last amended June 16, 2023). Unmanned aircrafts heavier than 55 lbs. are registered in the same manner as manned aircraft, calling for different operating regulations. David Sella-Villa, *Drones and Data: A Limited Impact on Privacy*, 55 U. RICH. L. REV. 991, 1000 (2021).

[14] *See* Carr, *supra* note 12.

[15] Matthew J. Cronin, *Crime in the Sky – Prosecuting Drone Offenses*, 69 DOJ J. FED. L. & PRAC. 255, 259-60 (2021).

[16] Carr, *supra* note 12, at 151.

[17] Rachel G. McConoughey & W. Eric Richey, *Advice for When the Lone Ranger Shoots Down Your Client's Rogue Drone: Plus, Where to Not Fly Your Drone in 2019*, 30 S.C. LAW. 28, 29 (2019).

mation of an executive committee between the FAA and Department of Defense to resolve a range of issues accompanying the integration of drones into society.[18] Evidently, Congress was satisfied with the committee's findings, because in 2012, the FAA received official orders to "safely accelerate the integration of civil unmanned aircraft systems into the national airspace system."[19] After being extended in 2016 and reauthorized in 2018,[20] Congress is currently set to fund these prerogatives until 2023.[21]

Congress's desire to integrate this technology into the economy is making a noticeable impact on the drone population. Among the commercial sector, the registered drone population increased from about 12,000 in 2015 to nearly 500,000 in 2020, with the population expected to reach over 1,140,000 by 2025.[22] Recreational users have seen a similar increase in the adoption of drones: from 2015 to 2020, the recreational population increased from about 130,000 to over 1,130,000.[23] Experts predict this number may exceed 1,630,000 by 2025.[24] Early restrictions on commercial use caused drones to be more prevalent among recreational users,[25] but with the versatility of this new technology, this gap will only decrease as more commercial entities find uses for this new technology.[26] The expected impact from widespread drone adoption is truly put into perspective when understanding how they can benefit the populace.

A. Positive Societal Impact

For instance, one sector poised to prosper from integrating drone technology is agriculture.[27] The average Texas farmer owns

---

[18] *FAA Timeline*, *supra* note 5.

[19] FAA Modernization and Reform Act of 2012, *supra* note 6.

[20] *See* FAA Reauthorization Act of 2018, Pub. L. No. 115-254, H.R. 302.

[21] *FAA Timeline*, *supra* note 5.

[22] *FAA Forecast*, *supra* note 7.

[23] *Id.*

[24] *Id.*

[25] *See* James L. Cresswell Jr., *Who Controls the Airspace? Issues Increase as Unmanned Aerial Systems – Drones – Fill Tennessee's Skies*, 56 TENN. B.J. 12, 13 (2020).

[26] *See FAA Forecast*, *supra* note 7.

[27] *See generally* Andy Linn, Comment, *Agriculture Sector Poised to Soar with Drone Integration, But Federal Regulation May Ground the Industry Before it Can Take Off*, 48 TEX. TECH L. REV. 975 (2016); *see also Seeing is Believing: Drones – What Are They*

roughly 500 acres of land, with the largest reaching 500,000.[28] When cultivating crops, each acre requires just as much care as the next. Before drone technology, farmers were required to walk through each acre of their harvest in order to monitor crop health – an inefficient process with high rates of error.[29] Using a drone, however, eliminates the need to walk the fields, provides better and more reliable data to the farmer, and allows for more efficient coverage of larger areas.[30] All of these factors contribute to lower cost, higher crop yield, and ultimately more profit for farmers who already work on a slim profit-margin.[31] Similarly, this process can also be used to monitor pollution among lakes, thus lowering the environmental impacts of farming.[32] While agriculture is poised to see a noticeable impact from drones, other sectors expected to benefit similarly are construction, insurance, and infrastructure inspection.[33]

At the moment, drones are primarily used as flying cameras,[34] but various other applications are continuing to evolve as the technology becomes more widespread. One alternative function is seen in the field of logistics. In the mid-2010s, drone performance was tested by delivering medical supplies to hard-to-reach areas and delivering food to a community in North Carolina,[35] foreshadowing what was to come on a larger scale over the next decade. Today, big companies like Amazon.com, Alphabet, UPS, and Domino's are investing in the future of drone delivery, and this is just the tip of the iceberg.[36] In a society that thrives on competition,[37]

Good For?, ECONOMIST (June 8, 2017), https://www.economist.com/technology-quarterly/2017/06/08/drones-what-are-they-good-for [hereinafter *Seeing is Believing*].

[28] Linn, *supra* note 27, at 978.

[29] *Id.*

[30] *Id.*

[31] *See Id.*

[32] *Id.* at 981.

[33] *Commercial Drones Are the Fastest-Growing Part of the Market*, ECONOMIST (June 8, 2017), https://www.economist.com/technology-quarterly/2017-06-08/civilian-drones.

[34] *Seeing is Believing*, supra note 27.

[35] *FAA Timeline*, *supra* note 5.

[36] *Why Amazon, UPS, and Even Domino's Is Investing in Drone Delivery Services*, INSIDER INTEL. (Jan. 1, 2023), https://www.insiderintelligence.com/insights/drone-delivery-services/.

[37] *See generally* Heather Boushey & Helen Knudsen, *The Importance of Competition for the American Economy*, WHITE HOUSE (July 9, 2021),

as more big companies adopt this technology, it will only induce others to do the same.

The widespread adoption is expected to positively impact the economy as a whole. Comprehensively, integration of drone technology is expected to produce an increase of $82 billion in gross domestic product and nearly 100,000 new jobs.[38] The increased efficiency is likely to result in total savings of over $100 billion.[39] With such incredible impacts on the economy, it seems like nothing could go wrong … until it does.

B. Bad Actors & Drone Technology

Richard Feynman, infamous theoretical physicist from the California Institute of Technology, once quoted a Buddhist Proverb, "[t]o every man is given the key to the gates of heaven; the same key opens the gates of hell."[40] Feynman, who spent time working on the Manhattan Project,[41] was speaking to the belief that scientific progress can produce great horror in the world, while simultaneously producing incredible benefits.[42] The same is true for the progress of engineering,[43] and specifically, the widespread adoption of drone technology. The many positives brought to society also coincide with much potential for abuse by bad actors. "Just as an entrepreneur can use a drone to provide security,

---

https://www.whitehouse.gov/cea/written-materials/2021/07/09/the-importance-of-competition-for-the-american-economy/.

[38] ASS'N UNMANNED VEHICLE SYS. INT'L, THE ECONOMIC IMPACT OF UNMANNED AIRCRAFT SYSTEMS INTEGRATION IN THE UNITED STATES, (2013), https://robohub.org/_uploads/AUVSI_New_Economic_Report_2013_Full.pdf.

[39] U.S. DEP'T. OF TRANSP., INTEGRATION OF CIVIL UNMANNED AIRCRAFT SYSTEMS (UAS) IN THE NATIONAL AIRSPACE SYSTEM (NAS) ROADMAP (1st ed., 2013), https://www.faa.gov/uas/resources/policy_library/media/uas_roadmap_2013.pdf.

[40] Richard Feynman, *The Value of Science*, 19 ENG'G & SCI. 13 (1955), https://calteches.library.caltech.edu/1575/1/Science.pdf.

[41] After the start of the Second World War, Feynman was recruited to the Manhattan Project where he contributed to the development of the atomic bomb – scientific development which clearly produced great horror but also furthered science in many ways. *See Richard Feynman*, WIKIPEDIA, https://en.wikipedia.org/wiki/Richard_Feynman (last visited June 24, 2023).

[42] *See* Feynman, *supra* note 40.

[43] Any new technology can be used for both good and bad purposes. Using the realm of computer science as an example, Facebook was created as a social media platform to connect people, and now it has the power to sway elections. *See generally* Seth Fiegerman, *Facebook Is Well Aware That It Can Influence Elections,* CNN (Nov. 17, 2016), https://money.cnn.com/2016/11/17/technology/facebook-election-influence/.

deliver goods, and assist in life-saving emergency services, so too can an enterprising criminal use it to terrorize airports and public venues, smuggle contraband, and create a mass-casualty event."[44] With drone operations, these potential abuses come in the form of a shield – an extra layer of protection making it more difficult to locate and identify a perpetrator. The various transgressions capable of being committed by a drone fall into two categories: logical attacks or physical attacks.[45]

Logical attacks include instances of a drone attacking the network of a given location.[46] In this way, drones can be manipulated to capture passwords, credit card numbers, and other sensitive data.[47] Researchers in Singapore displayed this ability by attaching a cell-phone to a drone in order to set up an open Wi-Fi network; they flew the drone up the side of a building to the thirtieth floor next to where a printer was located, and proceeded to intercept confidential documents that were being sent to print.[48] Cyberespionage is already a frightening reality,[49] as the victim rarely knows of the damage taking place; the use of drones adds another dimension to this silent battle for electronic privacy.

Physical attacks cover those abuses that do not attack one's network, relying more on the kinetic aspect of drone operation.[50] This is most commonly seen in the form of physical privacy invasion[51] – using a drone camera to spy on someone or something:

> [T]he incredibly accurate, detailed imagery and other remotely sensed data obtainable by small drones poses an additional risk to critical infrastructure. The unique per-

---

[44] Cronin, *supra* note 15, at 271.

[45] Jean-Paul Yaacoub et al., *Security Analysis of Drones Systems: Attacks, Limitations, and Recommendations,* NAT'L CTR. FOR BIOTECH. INFO. (May 8, 2020), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7206421/ [hereinafter Yaacoub et al., *Security Analysis*].

[46] *Id.*

[47] *Id.*

[48] Joseph J. Vacek, *Counter-UAS Applications Illegal Under 18 U.S.C. § 32 Are Justified When Using a Reasonably Defensible Counter-UAS Strategy That Incorporates Risk and Compliance Categorizations*, 93 N.D. L. REV. 499 (2018).

[49] *See Google v. Joffe*, 746 F.3d 920 (9th Cir. 2013) (finding Google liable for using its automated street cars, which collect data and take imagery for Google Earth "Street View," to simultaneously collect data from any unencrypted Wi-Fi networks with which the car would come in contact).

[50] Yaacoub et al., *Security Analysis*, *supra* note 45, at 504.

[51] *Id.*

> spective offered by a drone operating at up to several hundred feet, coupled with high-resolution stabilized cameras, allows anyone to obtain detailed data for critical infrastructure, such as dams, electrical transmission systems, power generation facilities, airports, public safety agencies and assets, and military hardware locations.[52]

Drones can be "whisper quiet," and when high enough, are "undetectable to the human eye."[53] Therefore, as with logical attacks, victims may similarly be unaware of the damage being done. Another form of physical attack and an "increasingly common tactic" is using drones to smuggle and distribute contraband, whether that be across the U.S. border or over a guarded fence into prisons.[54] However, perhaps the most severe type of physical attack derives from the integration of drone technology and serious weaponry. For instance, in *Huerta v. Haughwout*, the FAA investigated a father and a son who posted YouTube videos of their drone-weapon creation: one drone attached to a handgun and the other to a flamethrower.[55] The mere ability to manipulate drone technology in such a manner illustrates the magnitude of damage that can be done by someone with bad intentions.

All in all, drones clearly have plenty of positive aspects, but they also carry potential for problems. It is the job of Congress and such authorized agencies to ensure that the integration of this technology is not manipulated into being a Trojan horse for lawlessness. Congress must ensure that the first responders to a drone-related incident are not crippled by needless legal restrictions.

III. LEGAL FRAMEWORK OF DRONE INTEGRATION – OPERATIONAL REGULATIONS

With the downside of drone use established, it is important to understand the rules governing operation to better visualize how this technology is being integrated into society. Once it is established what the law allows, then it is easier to understand where

---

[52] Vacek, *supra* note 48, at 504.

[53] Cronin, *supra* note 15, at 271.

[54] *Id.*

[55] *Huerta v. Haughwout*, No. 3:16-cv-358, 2016 WL 3919799 (D. Conn. July 7, 2016).

the law fails. The FAA heavily regulates the operation and registration of drones. Before flying, every drone must be registered in the FAA's database.[56] Following this process, the FAA will then issue a registration number that must be displayed on the outside of the drone.[57] Further, when flying the drone, every operator must have proof of registration available at all times.[58] In 2023, an FAA regulation will become effective which mandates every drone to be remotely identifiable, so innocent bystanders can distinguish good-faith operators from the mischievous.[59] This information will provide bystanders with a drone's identity, location, altitude, and its control station or take-off location.[60]

As far as operating a drone, the broadest rules governing operation require the operator to not use the drone in a "careless or reckless manner so as to endanger the life or property of another," and to not "allow an object to drop from the aircraft in a way that creates undue hazard to persons or property."[61] In practice, this essentially obligates the operator to act reasonably. More specific requirements bind an operator to only controlling one drone at a time,[62] prohibit operation while under the influence of drugs or alcohol,[63] and obligate "the person manipulating the flight controls" to maintain the drone within his or her line of sight.[64]

The regulations passed by the FAA sufficiently prohibit the possibilities for wrongdoings. The operational requirements limit operation in situations that may cause an accident, and the registration requirements aid to document every entity operating in the sky. On one hand, this may progress toward more efficient law enforcement and create better acceptance from the public. On the other hand, a sad truth of today is that any number of laws only

---

[56] 14 C.F.R. § 107.13.

[57] *Id*.

[58] 14 C.F.R. § 107.7.

[59] *Remote Identification*, FED. AVIATION ADMIN., https://www.faa.gov/uas/getting_started/remote_id (last updated June 29, 2023).

[60] *Id*.

[61] 47 C.F.R. § 107.23.

[62] 47 CFR § 107.35.

[63] 47 CFR § 107.27.

[64] 47 CFR § 107.31.

stop the rule-followers,[65] and those law-abiding individuals are unlikely to perform the bad acts that are possible with drone technology. While this is true for all bad acts, outside of drone technology, police are in a position to prevent the malfeasance – like an officer patrolling a mall to dissuade theft. In this scenario, theft is dissuaded because people know that an officer is capable of addressing the thief if he or she were to act. However, when the bad act is committed via a drone, police are preempted from addressing the transgression in an efficient manner; therefore, no bad act is dissuaded. To dissuade bad actors from performance, there must be more than the threat of retribution from breaking the law – there must be preventative measures available to stop them from doing it in the first place.

IV. DRONE DEFENSE

If one witnesses a drone being operated in an unlawful manner, it is pertinent to understand what options are available to rectify the situation. One would assume that the best recourse is to notify local law enforcement; however, when it comes to drone operation, local law enforcement is preempted from action in many ways.[66] With a public that is largely reliant on local law enforcement to aid in troubled situations,[67] this causes problems. This section delves into the various technological resources to detect and mitigate drone technology, and the legal regime's inimical effect on law enforcement's ability to provide redress.

A. Technological Possibilities

Technology is a two-way street: just as technology may allow a criminal to perform a bad act through a drone, technology also may find a way to prevent a criminal from committing such acts. This article will refer to preventative technology and other counter-drone methods as 'defense techniques.' The effects of the various techniques are further divided into two categories: detection

---

[65] *See* Cronin, *supra* note 15, at 257 ("drone misuse has also 'increased dramatically over the past two years,' with the FAA receiving over 100 reports of errant drones [per] month").

[66] *See generally* Police Procedures, *supra* note 10.

[67] *See generally* Heather Mac Donald, *Why We Need the Police*, CITY J. (June 8, 2020), https://www.city-journal.org/why-we-need-the-police.

and mitigation. Detection works to identify and communicate the location of a drone when intruding into a particular vicinity, while mitigation works to actively interrupt the operation of the drone.

i. Detection Techniques

Drone detection comes in two forms: radiofrequency and non-radiofrequency. Non-radiofrequency systems detect the physical presence of a drone or the signals being sent from the drone, but do not "record" the signals detected.[68] These systems come in the form of radar-based systems, acoustic systems that "hear the drone," and also thermal imaging cameras.[69] Radiofrequency systems identify the radio signals from the drone, and proceeds to "record" the signals to calculate the location of the controller.[70] Non-frequency systems are legal and available to the public; however, the use of radiofrequency systems to locate the controller is prohibited.[71] Such systems violate the Pen/Trap Statute and Wiretap Act for capturing and recording electronic communications.[72] There is no exception for private actors; thus, law enforcement may use such devices only with a court order.[73] This is only given if necessary for the furtherance of an ongoing criminal investigation.[74]

Detection techniques may be useful for citizens who desire to know when a drone is intruding on their property; however, to prevent a drone from intruding in the first place requires use of a mitigation technique.

ii. Mitigation Techniques

There are four realistic methods to mitigating drone technology, most of which are frowned upon by the law because drones

---

[68] FED. COMMC'NS COMM'N ET AL., ADVISORY ON THE APPLICATION OF FEDERAL LAWS TO THE ACQUISITION AND USE OF TECHNOLOGY TO DETECT AND MITIGATE UNMANNED AIRCRAFT SYSTEMS (2020), https://docs.fcc.gov/public/attachments/DOC-366222A1.pdf [hereinafter INTERAGENCY ADVISORY NOTICE].

[69] Police Procedures, *supra* note 10.

[70] *See Id.*; *see also* INTERAGENCY ADVISORY NOTICE, *supra* note 68.

[71] Police Procedures, *supra* note 10.

[72] INTERAGENCY ADVISORY NOTICE, *supra* note 68.

[73] *Id.* (citing 18 U.S.C. §§3122(b)(2) & 3121(c)).

[74] *Id.*

are entitled to fly in national airspace.[75] The four categories are spoofers, hackers, jammers, and destroyers.[76] Each works in a distinct way to interrupt the operation of the drone.

Spoofers work by manipulating and altering the signals between the remote operator and the drone itself.[77] This can be done by interfering with the sensor measurements of position, time, or velocity; ultimately causing the controller to lose control of the drone.[78] Hacking a drone is similar to spoofing, but taken to a further extent – interfering with the position, time, and velocity signals in such a way as to completely hijack operation away from the controller.[79] Alternatively, frequency jamming works to send a stronger signal on the same radio frequency as the one used between the controller and the drone, which overpowers and disrupts the incoming signal[80] – essentially causing the drone to fall out of the sky. Lastly, a destroyer is the category representing the "old fashioned" approach to drone mitigation: physical destruction by force, such as using a baseball bat or a firearm.[81]

Broadly speaking, local authorities* are outlawed from taking such action under 18 U.S.C. § 32: prohibiting the destruction, damage, or disabling of any aircraft within the jurisdiction of the United States.[82] Moreover, the technological responses are outlawed by 18 U.S.C. § 1030: prohibiting instances of "accessing a protected computer without authorization and thereby obtaining information, or intentionally damaging a protected computer without authorization, including by transmitting a program, in-

---

[75] *See* 18 U.S.C. § 32 (1999) (destruction of aircraft or aircraft facilities).

[76] *See* Jonathan Rupprecht, *Big Problems with Counter Drone Technology (Anti Drone Guns, Drone Jammers, Etc.)*, RUPPRECHT L. P.A. (May 21, 2023), https://jrupprechtlaw.com/drone-jammer-gun-defender-legal-problems/.

[77] *Id*.

[78] Yaacoub et al., *Security Analysis*, *supra* note 45; *see also* Shah Zahid Khan et al., *On GPS Spoofing of Aerial Platforms: A Review of Threats, Challenges, Methodologies, and Future Research Directions*, PEERJ COMP. SCI. (May 6, 2021), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8114815/.

[79] *Id*.

[80] Vacek, *supra* note 48, at 513.

[81] *See* Rupprecht, *supra* note 76.

* An exception carved out in 6 U.S.C. § 124n allows the Secretary of State and Attorney General to authorize personnel to destroy aircraft, notwithstanding 18 U.S.C. § 32. This exception has been granted to few federal agencies but is not extended to state law enforcement.

[82] 18 U.S.C. § 32.

formation, code, or command that causes such damage."[83] With jammer technology it is not just illegal to possess[84] – it is also illegal to manufacture, import, market, or sell the operation of an unlicensed jammer in the United States, thus making its use further from becoming a realistic possibility.[85]

B. Dealing with Unlawful Drones – Minor Threats

With the amalgam of legal barriers preventing disarming action on a drone, what is one to do if one comes in contact with a bad actor? The law allows for use of a mitigation technique by providing justifications for either defense of property or self-defense.[86] To be justified, the actions of defense must be reasonable in scope to the threat posed.[87] When dealing with minor infractions,[*] this poses the problem of knowing what exactly constitutes unlawful conduct so as to know what is threatening. However, when the rules forbidding certain conduct are ambiguous, this places a substantial burden on everyday laypersons. For instance, in the scenario of a simple trespass with a drone, the "threat posed" may be mitigated by a request to the operator to desist from entering one's property.[88] If the trespasser persists, use of a counter-drone technique may be justified. In any trespass scenario, however, the landowner must be aware of the airspace delineations to know whether the drone was trespassing in the first place.

---

[83] INTERAGENCY ADVISORY NOTICE, *supra* note 68 (citing 18 U.S.C. § 1030). There are additional statutes that may prohibit such conduct, but these are the primary focal points listed in the Interagency Advisory Notice.

[84] *Jammer Enforcement*, FED. COMMC'NS COMM'N (April 2020), https://www.fcc.gov/general/jammer-enforcement [hereinafter *Jammer Enforcement*].

[85] 47 U.S.C. § 302(b). It is worth noting that these techniques are not prohibited against the public needlessly and many of them cause unintended consequences. For instance, use of a frequency jammer is only legal when given a license from the FCC because use of such may interfere with other devices reliant on radio waves like cell phones. *See Id*.

[86] Vacek, *supra* note 48, at 507.

[87] *Id*.

[*] Referring to the unlawful use of drones that do not pose an imminent threat to life or property.

[88] *Id*. at 514.

i. Airspace

According to the U.S. Congress, the federal government has "exclusive sovereignty of the airspace in the United States."[89] This authority was then delegated to the FAA to "develop plans and policy for the use of the navigable airspace…"[90] In using this power to regulate, the FAA clearly established a ceiling for permissible drone travel in 14 C.F.R. § 107.51, which mandates that a small unmanned aircraft must not exceed "400 feet above the ground."[91] However, when dealing with the minimum altitude over private property, the lines are not quite as clear.

In the common law, delineation of airspace followed the ancient doctrine of *cujus est solum ejus esque ad coelom* – "whoever owns the soil, it is theirs up to Heaven."[92] In the wake of technological progress, lawmakers deviated from this idea – seeing it as incompatible with modern airplane travel.[93] When faced with the revolutionary issue of airspace delineation in the wake of technology, the United States Supreme Court held in *Causby* that landowners have "exclusive control of the immediate reaches of the enveloping atmosphere" and "the landowner owns at least as much of the space above the ground as he can occupy or use."[94] Further, in *Singer*, the District Court of Massachusetts invalidated a law that prohibited unauthorized drone use up to 400 feet above private property, finding that it was preempted by Congress's intent to regulate the airspace.[95]

Synthesizing these two holdings: a drone cannot be prevented from flying 400 feet above private property,[*] but can only go low enough as to not interfere with the landowner's enjoyment and

---

[89] 49 U.S.C. § 40103(a)(1).

[90] 49 U.S.C. § 40103(b)(1).

[91] 14 C.F.R. § 107.51 (2016).

[92] TIMOTHY M. RAVICH, INTRODUCTION TO AVIATION LAW 62 (2020).

[93] *Id*.

[94] Carr, *supra* note 12, at 158 (citing *United States v. Causby*, 328 U.S. 256, 258 (1946)).

[95] *Singer v. City of Newton*, 284 F.Supp.3d 125, 131 (D.Mass. 2017).

[*] This assumes that other jurisdictions fall in line with the Court in *Singer*. It is certainly possible that other jurisdictions differ on finding conflict or field preemption with regards to federal airspace laws. A finding of conflict preemption would permit airspace regulations from the states so long as it does not conflict with the federal regulations, while a finding of field preemption would not allow any state regulations regarding airspace.

use. In the scenario of a distressed landowner contemplating proper recourse, these lines are as fuzzy as lines can be. In *Boggs*, a district court in Kentucky was faced with this exact dilemma: a trespassing drone and a civilian who took matters into his own hands by shooting it down with a shotgun.[96] The plaintiff argued that he was in navigable airspace, but the defendant claimed the drone was on his property.[97] The federal court ended up dismissing the case for lack of subject matter jurisdiction, ruling that the FAA had not sought to enforce such regulations in this case, but left the door open for a cause of action in State court.[98] However, in *Commonwealth v. Merideth*, the Kentucky State Judge ruled that the defendant had the right to shoot down the drone.[99] Despite the *Boggs* and *Merideth* holdings in favor of landowners' rights, the outcome was not clear-cut and could have ended poorly for the defendant.

ii. Recourse

To avoid the risk of unlawful action against a drone in a trespass situation, one typically notifies local law enforcement.[100] However, the ability for law enforcement to rectify the situation is crippled. The Preventing Emerging Threats Act of 2018, a subsection of the FAA Reauthorization Act of 2018, only gives certain authorized personnel the power to disable a drone, ultimately preempting local law enforcement from taking such action.[101] On the flipside, when merely locating an operator, law enforcement is prohibited from using radiofrequency detection systems that would efficiently gather such information.[102] This means that local

---

[96] *See Boggs v. Merideth*, No. 3:16-CV-00006-TBR, 2017 WL 1088093 (W.D. Kent.).

[97] *Id.*

[98] *Id.*

[99] *Judge Dismisses Charges for Man Who Shot Down Drone*, WRDB.COM (Oct. 26, 2015), https://www.wdrb.com/news/judge-dismisses-charges-for-man-who-shot-down-drone/article_b52eff9b-0c87-53ce-ad68-38806c7c9288.html (updated June 7, 2023).

[100] *See How to Charge Someone With Trespassing*, FAIR PUNISHMENT, https://fairpunishment.org/how-to-charge-someone-with-trespassing/ (last visited June 25, 2023) ("The first step is to contact the police. A trespasser is in violation of the law and should be reported to the police immediately").

[101] *See* 6 U.S.C. 124n – Protection of certain facilities and assets from unmanned aircraft.

[102] *See Id.*; *see also* INTERAGENCY ADVISORY NOTICE, *supra* note 68.

law enforcement could find itself powerless to counter the whims of an anonymous drone operator.

Imagine a scenario where a citizen continually bothered by a drone does the right thing and calls law enforcement. If the police walk around the vicinity and cannot physically locate the operator, there is no *immediate* assistance that the officer can give; the officer cannot disable or interfere with the operation of the drone, and the officer cannot use radiofrequency technology to locate the perpetrator. The only recourse is to get a court order to detect the operator, or call a federal agency to disable the drone. This is not efficient and will lead more citizens to take matters into their own hands – perhaps in an unsafe way as seen in the *Boggs* case.

C. Dealing with Imminent Threats

The handicapping of local law enforcement is more worrisome when such unlawful conduct poses an imminent threat. An example of a drone posing as an "imminent threat" is seen in the hit television show "Criminal Minds," wherein the perpetrator attaches an automatic firearm to a drone, and proceeds to commit atrocities at mass gatherings.[103] If a civilian comes across this type of conduct, typically the first reaction is to call 911, which initially summons local and state law enforcement officials.[104] However, what are the first responders going to do? This is the crux of the issue. When the threat posed is imminent, action from a first responder to neutralize the threat likely falls under the self-defense exception.[105] When evaluating the readily available methods of recourse, presumably, a first responder's instinct

---

[103] *Criminal Minds: Killer App* (CBS television broadcast Oct. 18, 2017).

[104] *See First Responder Toolbox: Malicious Modification of UAS*, OFF. DIR. NAT'L INTEL. (Sept. 16, 2020), https://www.dni.gov/files/NCTC/documents/jcat/firstresponderstoolbox/First_Responders_Toolbox_-_Unmanned_Aircraft_System_UAS-_Recognizing_Malicious_Modification-survey.pdf (recommending to "call 911 for observed UAS activity placing individuals or facilities in immediate danger"); *see also Active Shooter Resources*, FED. BUREAU INVESTIGATION, https://www.fbi.gov/about/partnerships/office-of-partner-engagement/active-shooter-resources (last visited June 24, 2023) ("local and state law enforcement agencies are virtually always the first ones on the scene") [hereinafter FBI].

[105] Vacek, *supra* note 48, at 507.

would be to try and shoot it down.* This is not an efficient response, especially in a setting where misfires can increase injuries. An efficient response would be for the first responders to arrive with jamming technology to immediately interrupt the radio communications between the controller and the drone. This would cause the drone to fall out of the sky instantaneously and would be more effective than attempting to shoot it down. However, just as the technology is outlawed in the general public, it is similarly outlawed in the hands of the first responders – law enforcement is just as handicapped as civilians.[106]

If this scenario came to fruition, the only response from law enforcement is to call a federal agency, likely the FAA or Department of Homeland Security.[107] An imminent threat requires a timely response, which is unlikely to come from a federal agency.[108] Additionally, if the first responders are unable to mitigate the threat, then there is no barrier preventing malicious drone use from affecting the public. Mandating this response is inefficacious and will eventually cripple the growth of drone technology.

In order for drone technology to thrive, it must be accepted by the public. Public acceptance is more likely when the downside of drone technology is actively prevented, allowing the public to reap only the positive effects of this technology. The public traditionally relies on local law enforcement to prevent malicious acts and to assure its safety.[109] This feeling of safety derives from the presumption that law enforcement officials are actually capable of mitigating the various threats that may be posed. For instance, if a criminal breaks into a house and the homeowner calls the police, this is likely a result of believing that the police are capable of

---

* Out of all of the possible mitigation techniques available to a first responder, the author assumes that use of the firearm would be the most readily available option.

[106] Jamming technology is only permitted when granted a license by the FCC prior to use. This technology is rarely even attempted to be marketed to law enforcement because sellers know that officers are prohibited from obtaining such technology in majority of cases. *See* Police Procedures, *supra* note 10.

[107] *See* Police Procedures, *supra* note 10; *See generally Protecting Against the Threat of Unmanned Aircraft Systems*, INTERAGENCY ADVISORY COMM. (Nov. 2020), https://www.cisa.gov/sites/default/files/publications/Protecting%20Against%20the%20Threat%20of%20Unmanned%20Aircraft%20Systems%20November%202020_508c.pdf.

[108] *See* FBI, *supra* note 104 ("local and state law enforcement agencies are virtually always the first ones on the scene").

[109] *See* Mac Donald, *supra* note 67.

neutralizing the threat. However, in the integration of this new technology, the threats facing the public are evolving, while the legal regime preempts the backbone of public safety from evolving to stop them.

The FAA is doing a sufficient job of integrating drones into society with proper regulations and rules, but this has little effect on the criminals within society. In order to deal with the evolving methods of committing crimes, threat prevention responsibilities cannot be centralized to federal agencies. Local law enforcement is the best equipped to respond to imminent threats, and there must be efficient procedures set in stone before one actually takes place.

V. SOLVING THE DRONE DILEMMA

The flaws associated with drone integration can be fixed with just a few modifications to the laws currently standing in the way. The problem, in essence, is that Congress began integrating drone technology into society for the numerous economic and societal benefits, all while not properly acknowledging the new dimension of possible misconduct. This is acknowledged on the federal level, but essentially preempts any acknowledgement from the states.[110] Law enforcement at the local and state level is the backbone that public safety relies upon to guard against bad actors.[111] However, law enforcement is preempted from taking effective action against unlawful conduct that materializes through drone operation.[112] This is neither efficient nor likely to lead to the prosperous integration of drone technology. Rectifying this situation lies in expanding exceptions within the legal barriers preempting defense techniques.

The broadest law preempting action lies in 18 U.S.C. § 32, prohibiting the destruction, damage, or disabling of any aircraft.[113] Notwithstanding, federal agencies are given the power to mitigate threatening drones under the Preventing Emerging Threats Act of 2018.[114] Accordingly, preemption must first be nul-

---

[110] *See* INTERAGENCY ADVISORY NOTICE, *supra* note 68 (referencing the Preventing Emerging Threats Act, 6 U.S.C. § 124n (2018)).

[111] *See Id.*; *see also* FBI, *supra* note 104.

[112] INTERAGENCY ADVISORY NOTICE, *supra* note 68.

[113] 18 U.S.C. § 32.

[114] Preventing Emerging Threats Act, 6 U.S.C. § 124 (2018).

lified by expanding the Preventing Emerging Threat Act to include state law enforcement officials. Federal agencies are incredibly busy and only have a certain amount of bandwidth. Alternatively, rather than extending the exception, a similar outcome can be reached by excluding small unmanned drone technology from the definition of an aircraft, thus removing it from the whims of 18 U.S.C. § 32. Regardless of how the ultimate goal is reached, the burden of dealing with numerous trivial matters from across the country is decreased by giving local law enforcement the ability to take the proper action. Allocating authority to state officials will increase faith in law enforcement to remedy a situation, which in turn disincentivizes citizens from taking actions in unsafe ways.[115]

The next law preempting meaningful action can be avoided by expanding the law enforcement exception within the Pen/Trap Statute. Currently, if law enforcement cannot physically locate the drone operator, it must retain a court order to use the radiofrequency detection system that would reveal such location. This is too high of a burden to bear and will chip away at citizens' confidence in law enforcement to address unlawful conduct. Rather, if a local law enforcement official *reasonably believes* a drone to be operating unlawfully, then use of radiofrequency detection systems should be permitted. This will be most impactful in 2023, after the remote identification mandates go into effect.[116] Then, if local enforcement finds that an operator is unable to be identified,[117] that would reveal *prima facie* evidence of unlawful conduct, and radiofrequency detection systems should be readily available to locate the operator.*

---

[115] See the discussion about *Boggs v. Merideth* in section IV(b)(ii).

[116] This remote identification requirement would give law enforcement and federal agencies instant access *supra* note 59.

[117] Any wireless communications device that is within range will be able to detect the serial number of the drone, but the registration corresponding to the serial number is kept by the FAA. This information is given to law enforcement after a formal request. *See Executive Summary: Final Rule on Remote Identification of Unmanned Aircraft*, FED. AVIATION. ADMIN. (Dec. 28, 2020), https://www.faa.gov/sites/faa.gov/files/2021-08/RemoteID_Executive_Summary.pdf. If law enforcement is unable to detect a serial number, then the operator cannot be identified.

* Especially in the early years, the penalties for such conduct should be incredibly trivial, if at all. The goal should be to merely create awareness of this law so good faith operators achieve compliance, and those bad faith operators can be located.

Detection systems will greatly aid in the minor infractions posed by drones; however, the major threats possible with drone technology require ensuring that first responders have access to a mitigation technique to efficiently disable any threat. The readily available defense to an imminent threat should be proportionate to the severity of the threat posed. However, currently "[l]ocal law enforcement agencies do not have independent authority to use jamming equipment,"[118] so the threat can surpass any defense available. In the event of a major threat, time is of the essence;[119] allowing for limited use of frequency jammers only in these severe situations will allow for an efficient response. This ability can be given to local law enforcement by conditionally expanding the license for legal jammer use, the condition providing for use only in severe situations. Regarding a state law enforcement's right to use jammers: it is better to have this technology and to not use it, than to be preempted from efficiently protecting its community if the time comes.

VI. CONCLUDING REMARKS

Drones are becoming more widespread, but they are not near the peak of public adoption.[120] The impact of this new technology is poised to bring considerable positive impacts to society, and this should be cherished. However, in order to preserve the benefits, Congress must properly address the new possibility for unlawful conduct. This is done by giving the heroes who preserve public safety the power to sufficiently address a drone-related incident. In any community, the authorities relied on are almost always state and local officials—as they are the first to respond to a cry

---

[118] *Jammer Enforcement*, *supra* note 84.

[119] A short response and engagement time leads to less casualties in an active shooter situation. *See* Keily Linger, Honors Thesis, *Analysis of the Police Response to Mass Shootings in the United States Between 1966 and 2016*, UNIV. AT ALB.: EMERGENCY PREPAREDNESS, HOMELAND SEC., AND CYBERSEC. (May 4, 2018), https://scholarsarchive.library.albany.edu/cgi/viewcontent.cgi?article=1000&context=honorscollege_ehc ("the relationship between the shooting duration and the total number of casualties … was considered statistically significant").

[120] *See Drone Market Outlook in 2022: Industry Growth Trends, Market Stats and Forecast*, BUS. INSIDER (Jan. 7, 2023), https://www.businessinsider.com/drone-industry-analysis-market-trends-growth-forecasts. The market for drone technology passed $1.25 billion in 2020, and Goldman Sachs forecasts it to eventually be worth $100 billion.

for help.[121] By having adequate procedures in place before a drone-related incident occurs, Congress can preserve and maintain a positive public perception of this new technology, allowing such benefits to flourish in society for many years to come.

[121] FBI, *supra* note 104.