# Commercial Drone Activity: Security, Privacy, and Legislation Issues

Sandra A. Vannoy
vannoysa@appstate.edu

B. Dawn Medlin
medlinbd@appstate.edu

Department of Computer Information Systems & Supply Chain Management
Appalachian State University
Boone, North Carolina 28684, USA

## Abstract

As consumers increasingly demand quick delivery of products to their homes, the drone has emerged as a viable solution. However, the use of drones as transport vehicles has outpaced resolutions to privacy and security concerns, as well as the creation of appropriate legislation and regulation. In this paper, we discuss the issues of privacy and security related to the use of the drone as delivery vehicles, as well as the unique challenges drones present to our current legislative and federal agencies charged with oversight of airspace and well-being of our citizens.

**Keywords:** Commercial Drones, Security, Privacy, Legislation

### 1. INTRODUCTION

New technology developments have historically outpaced our understanding of their associated issues, such as privacy, security, and legislation, as their futures are unstable and unknown. Therefore, it is not surprising that there is little to be found in current academic or contemporary literature investigating these matters in the context of the drone.

Drones are receiving increased attention around the globe. There has been a recent emphasis upon unmanned flying vehicles for commercial use, particularly in the area of consumer product delivery; however, little is known about the impacts of this commercial application on the world as we know it. Existing research suggests that while safety has been considered in various governmental rulings, little thought has been given to issues such as privacy and security (Dorr & Duquette, 2016). This paper is intended to provide some insight into issues around the commercial use of drones, with particular emphasis upon privacy, security, legislation, and regulation.

### 2. BACKGROUND

Drones are essentially flying robots that can be controlled remotely or fly autonomously through embedded software and sensors that interface with global positioning systems. These unmanned flying robots are classified according to their size, intended use, flight range, speed, power system, among other traits (Hassanalian & Abdelkefi, 2017). Across the globe, there has been a loosening of restrictions around the use of drones in commercial airspace, with the global market projected to surpass $120 billion by 2021 (Joshi, 2017).

To understand the use of drones in general, it is helpful to look at the historical use of drones

 

(originally known as unmanned aerial vehicles or UAVs). In 1918, the United States army used unmanned aerial vehicles, which were known as "flying bombs" that could hit a target up to 64 kilometers. The functions of drones were later enhanced by the military in their use as weapons carriers. Governments in general have found that drones can be used to prevent casualties of war as they can provide accurate surveillance information and precise strike zones. Additionally, they have the abilities to discern between intended and unintended targets (Rao, Goutham, Maione, 2016).

Several industries have expanded upon the military's use including agriculture, energy, deliveries, rapid response and emergency services, real estate, photography and others. According to Peter Diamandis (2018) in his article "Top 10 Reasons Drones Are Disruptive" between the years 1980 and 2010 there was major growth in the drone industry by both consumers and businesses in the four following areas:

**1. GPS:** In 1981, the first commercial GPS receiver weighed 50 pounds and cost over $100K. Today, GPS comes on a 0.3 gram chip for less than $5.
**2. IMU:** An Inertial Measurement Unit (IMU) measures a drone's velocity, orientation and accelerations. In the 1960s an IMU (think Apollo program) weighed over 50 lbs. and cost millions. Today it's a couple of chips for $1 on your phone.
**3. Digital Cameras:** In 1976, Kodak's first digital camera shot at 0.1 megapixels, weighed 3.75 pounds and cost over $10,000. Today's digital cameras are a billion-fold better (1000x resolution, 1000x smaller and 100x cheaper).
**4. Computers & Wireless Communication (Wi-Fi, Bluetooth):** No question here. Computers and wireless price-performance have gotten a billion times better between 1980 and today.

UAVs have been employed in a wide variety of civilian, law enforcement and military applications, the overwhelming majority of them beneficial. They can be used, for example, to deliver much needed medicines to remote areas, help rescuers identify people in need of assistance following a natural disaster, or to provide vital overhead imagery to police officers attempting to defuse a hostage standoff. In the commercial world, UAVs can be employed for a multitude of tasks as diverse as surveying, crop spraying, and traffic congestion monitoring. Scientific applications include air quality assessment, wildlife tracking, and measuring the internal dynamics of violent storms (Kwon, Kim, and Park, 2017).

UAVs also generate a number of economic benefits, with the potential to create thousands of jobs around the world that involve the design and production of UAVs as well as and spurring advances in robotics that will apply well beyond aviation, in fields ranging from manufacturing to surgery (Chamata, 2017).

## 3. COMMERCIAL DRONE USE

According to E-Marketer (2016), worldwide retail sales is approximately $26.6 trillion with online retail sales expected to grow to around $4 trillion by 2020. This means that e-commerce sales will account for almost 15% of the total retail market. The upward tick in e-commerce also means that fewer consumers are going into brick and mortar stores, and it is expected that they will receive their packages at the office or at their home. Accordingly, there may be increasing opportunities for companies to use drones for the delivery of packages.

Major online research firm Skylark Services suggests that in any given day 110 million online orders are placed, with 100 million of the products ordered weighing under five pounds. This evidence suggests that there is huge economic potential for drone delivery, and in fact, Skylark predicts a major disruption of the delivery world as we know it (Jenkins, Vasigh, Oster & Larson, 2017). Furthermore, drone delivery offers an interesting solution to the "last mile" problem faced by e-commerce companies wishing to reduce delivery times, reduce costs, and improve customer satisfaction (Murray & Chu, 2015).

In late 2013, Amazon announced its intention to implement a global drone-enabled delivery system, Prime Air. Since that time, a number of companies in the United States have expended a tremendous effort in developing a safe and reliable drone delivery system. Drone delivery company Flirtey has completed a number of FAA-approved drone deliveries, including medical supplies to the Remote Area Medical health clinic in Wise, Virginia in 2015, a delivery to a customer home in collaboration with 7-Eleven in 2016, and most recently has been engaged in delivery of pizzas with the Domino's Pizza company (Flirtey Continues to Lead Drone Delivery Industry, 2017). With each of these expansions of drone usage, additional benefits can occur that include the economic benefits such as the creation of new

job titles and new innovations within the areas of robotics.

According to the Association for Unmanned Vehicle Systems International (AUVSI), as of 2016, there were 150 drone manufacturers in the United States (Villasenor, 2016). With the expectation of more manufacturers to come, there is also the anticipation of lower costs and more product choices. Currently, there are increasing numbers of available UAV's under $1000, and it is expected that within a short period of time before GPS and video-equipped UAV's will be below $100. As with most technologies, there are advantages that may sound enticing, but there are several disadvantages which certainly include the topic areas of privacy and security.

With new technology use comes uncertainties and risks. Whether for personal or commercial use, issues surrounding privacy and security are paramount as unmanned vehicles can take photographs, videos, capture information and perform a number of other activities that can invade a person's privacy or not secure a person's information.

## 4. PRIVACY AND SECURITY ISSUES

The concept of privacy means separation from others and entails the ability to exclude oneself or exclude information about oneself. Furthermore, privacy as a concept fluctuates on national, individual, and cultural individualities (Serbua & Rotariua, 2015). Security, like privacy, has different meanings in different contexts. Arnold Wolfers (1952) states that the meaning of security is 'the absence of threats to acquired values' which appears to capture the basic intuitive notion underlying most uses of the term security, and can be applied to many different generic situations. Privacy and security as related to drone technology are further complicated by its nascent nature, with few clear rules or regulations.

With new technologies, comes uncertainties and risks, and issues such as security, privacy, and legislation take a back seat to the innovation of the technology itself. While unmanned vehicles can take photographs, videos, capture information and perform a number of other activities that can invade a person's privacy or not secure a person's information, we currently have little understanding of these issues or how to address them.

Drone activities have given rise to activities and possible threats to data privacy. One of the largest privacy concerns is that drones can be used for spying given the fact that most drones have cameras attached to them or embedded within the technology of the drone. Capturing data about a property or peeking into someone's home is an easy task for drones. In addition, drones are capable of being able to capture large amounts of data that can easily include pictures and videos. Other drone activities can include the capturing and exploitation of data in conjunction with other data and the use of facial recognition to identify individuals.

Overt or unwanted surveillance by drones can impinge upon an individual's right to physical privacy. The privacy of personal behavior is concerned with the freedom of an individual to behave as they wish without worry or concern of undue observation and interference from others (Clarke, 2014). A surveillance target may be an area, or one of more objects, as mentioned earlier, including people (Wigan and Clarke, 2006). A combination of physical surveillance with data gathering can provide for the acquisition of information about a person's location at a certain time or place which constitutes tracking and therefore means that inferences may can be drawn about patterns of the individual's behavior. These inferences can then be used for criminal activity such as, stalking, blackmail and harassment.

Drones can be targeted for software and hardware attacks because they fly, capture video, and can be remotely controlled. They can be also targeted for command and control data link jamming and spoofing, in which a hacker can block or falsify the data link in order to disrupt or take control of the device. Navigational sensor jamming can also disrupt and take over navigation. Hackers can also tap the video or photo link, where they intercept the video and other data from the drone.

Drones can also crash, thus allowing others to not only possibly confiscate a product, but gain access to the receiver's name, address and phone number as well as goods and other information within the package. Draper (2015) states that crashes are inevitable because of issues related to weather, other aerial vehicles, buildings, and birds, or hackers who may gain control of the drone, leading to safety concerns for people and property.

Security like privacy has different meanings in different contexts. Arnold Wolfers' (1952) article

entitled "National Security" as an Ambiguous Symbol" appears to be just as applicable and accurate today as it was in the 1950s. Wolfer stated that the meaning of security is 'the absence of threats to acquired values' which appears to capture the basic intuitive notion underlying most uses of the term security, and can be applied to many different generic situations.

Drone units are vulnerable to two different kinds of security attacks that can occur on their GPS navigational systems. 'Spoofing' entails the sending of strong (but fake) GPS signals towards a drone, so that it is essentially "hijacked" instead of following its programmed directions. The drone can then be manipulated to crash or be flown to another location such as the attacker's location or another specified location. This could make it possible for an employee at Amazon to be held responsible for the consequences of the "spoofed" drone since it is very difficult to prove the origin of the navigation signals. It wasn't until 2014 that a successful spoofing attack was conducted against a drone by a researcher at the Department of Homeland Security facility. For now, not all commercial drones use encryption methods that render it invulnerable to any currently known spoofing attack, but still leaves it susceptible to 'jamming.' In a jamming attack, the drone is overwhelmed with signals to the GPS antenna. The encryption ensures that no fake signal is mistaken for the true one, but the true signal cannot get through either. Unintended collisions seem to be unavoidable in such scenarios, especially in an unregulated environment (Rao, B., Gopi, A., & Maione, R., 2016).

The advantages of drone delivery and returns may sound enticing, but there are several disadvantages concerning privacy and security issues. The U.S. Federal Trade Commission has raised several questions surrounding the topic of privacy and security concerns as FTC researchers were able to hack into three different off-the-shelf drones. Furthermore, they took over the camera feed on each drone; for two of the drones, they were able to turn off the aircraft to make it fall from the sky and seize complete control of the flight path (Glass. G., 2016).

Just like military operations, commercial companies such as Amazon can use the data collected from drone deliveries and returns in order to assist in their marketing campaigns. According to Jeff McCandless, Founder and CEO of project44, "Amazon can leverage information about your vehicles, the exterior of your home and any property visible from the outside, and use that to market-related products to people. They can even obtain information about when people are home, when they are outside, etc. There's no telling what other ideas they'll come up with as they bring in rounds of data and begin analyzing it. That said, one has to wonder where it ends."

Under President Obama, Congress held hearings related to privacy issues and the use of drones, with over half of the states enacting some type of drone legislation after the fact. But once again, the issues of privacy and security were not directly addressed. In fact, in every state where laws were passed, the new legislation focused more on the technology itself, rather than the harm that the surveillance could create (Thompson, R. 2015).

As Justice Samuel Alito wrote in a concurrence in United States v. Jones, the January 2012 Supreme Court ruling that ad- dressed the constitutionality of affixing a GPS tracking device to a vehicle without a valid warrant, "[i]n the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical." Although Justice Alito's statement was directed toward GPS tracking, it has direct relevance to UAVs. In comparison with manned aircraft, UAVs can be very inexpensive to procure and operate. As the practical barriers to obtaining aerial imagery fall away, the resulting privacy issues take on heightened importance.

Privacy and security as related to drone technology lead to a range of concerns not seen with many emerging technologies. One of the primary issues is there are few clear rules or regulations holding manufacturers responsible for incorporating security measures that might prevent tampering by malicious hackers (Glaser, 2016). Currently, organizations are more concerned with their bottom line than the issues of privacy and security, as there are only a few to no legal ramifications.

## 5. LEGISLATION AND REGULATION

A variety of laws may be applicable to drones and their usage including trespassing, publication of public facts, and stalking and harassment (Vallesenor, 2013). A complicating factor is that different localities may have differing laws related to airspace usage according to federal legislation. The FAA enacted the FAA Modernization and Reform Act of 2012 (FMRA) that called for the integration of unmanned aircraft systems (UAS), or "drones," into the national airspace by

September 2015. Unfortunately and during that time, "the substantive legal privacy framework relating to UAS on the federal level has remained relatively static: Congress has enacted no law explicitly regulating the potential privacy impacts of drone flights, the courts have had no occasion to rule on the constitutionality of drone surveillance, and the Federal Aviation Administration (FAA) did not include privacy provisions in its proposed rule on small UAS" (Thompson, R., 2015). Under federal law, all UAVs must apply to the FAA for permission to fly unless they fall under the exception clause. The process for obtaining permission to operate drones differs depending on whether the operator is a public operator or a private commercial operator.

One of the key takeaways from the 2012 legislation is the visual line-of-sight (VLOS) mandate. VLOS ensures the pilot will only operate the drone as far as he or she can see. While everyone's vision is different, this ensures that the drone wouldn't legally be able to travel very far or encounter obstacles unknown to the operator. To realistically use drones in commercial deliveries, it will be quite difficult if not impossible to always maintain a line of sight. Therefore, it is assumed that newly adopted FAA regulations may relax some of the regulations for specific classes of UAS operations (Schlag, 2017).

In December 2015, the FAA passed a federal law requiring all drones weighing over 250 grams, or a little over one-half pound, and their users to be registered online. The law has been justified due to privacy and public safety concerns, as the FAA had reported 1133 cases of unsafe use (FAA.gov). Due to the increasing number of UAVs it was posited that with this increase comes the possibility of technical failure either due to the failure of the technology or users' inexperience. As a result of this law, a user flying / owning a without a certificate, and even on their own property, can face both civil and criminal sanctions including fines and imprisonment.

Most recently in October 2017, President Donald Trump signed a memo to the Department of Transportation (DOT), directing them to begin the process of developing rules to allow commercial drone operators to fly more freely in the U.S. The memo directs the DOT to take proposals from local, state, and tribal leaders over several months, and then select the five most promising proposals and run small experiments over the next three years, to see which one is the best solution. Then, whichever proposal does the best will be implemented nationally (Stewart, 2017).

Though the FAA may not have strict rules for drone use pertaining specifically to privacy issues, many states and localities have strict Peeping Tom regulations that may apply if a drone were to hover over private residences. Again, the FAA is relying on local law enforcement agencies to address this issues at this time. In a study conducted by the Center for the Study of the Drone at Bard College, they found that at least "…130 localities in the U.S. have their own local drone rules, which have extended beyond the rules implemented by the FAA" (Bard College Surveys Legal Cases Involving Drones, 2017).
Drone delivery presents a particular challenge for law enforcement officials as drone use has increased dramatically, making it difficult for the FAA to monitor their flights as it does with commercial airlines. Unlike manned airlines, drones can be operated almost anywhere and are not supervised by traffic controllers.

Outside of the United States legal system is an international framework, the International Covenant on Civil and Political Rights (ICCPR). In some countries, civil rights may be protected by their constitution, however some of these rights are insufficient to significantly curb the use of drones in the area of visual surveillance. In the United States, the Fourth Amendment is primary to the issue of privacy and UAS operations. Under the Fourth Amendment, Americans are guaranteed a certain right to privacy through the right "to be secure in their persons, houses, papers, and effect against unreasonable searches and seizures" (U. S. Const. amend. IV). There are dissenting opinions, however, concerning the strength of the Fourth Amendment in relation to consumers and their privacy protections from the use of drones. Some advocates of the U.S. Constitution believe that there will be a much stronger measure of protection against government UAS privacy abuses than is widely appreciated, while others suggest that that there is further need for substantial statutory and common law protections that will protect individuals and their privacy rights.

According to some legal scholars, drones, with their current and projected capabilities, present a perfect storm of issues that fall outside of the current Fourth Amendment jurisprudence, but still appear relevant to the Fourth Amendment (Bomboy, 2014). As drones can travel on public airways at low or high altitudes, undetected and with little or no undue noise, and drones can use technologies to gather an abundance of intimate details and information, it has been suggested that law enforcement will likely increasingly use drones for domestic surveillance, and all of these

actions will likely propel drones to the forefront of courts' dockets.

In February 2018, a helicopter crash-landed in South Carolina, with the crash being triggered by a civilian drone. Neither the drone nor owner of the drone were ever found. As drones become more popular, incidents such as this one will most likely be on the rise. Though it is noted to be the first drone-related crash of an aircraft in the U.S., it is expected that more of these occurrences will happen as more and more drones are being purchased for both recreational and entertainment use (Bloomberg, 2018). Though this may have been the first noted crash, there have been a number of other incidents that have created serious and almost deadly results. As examples, a commercial jet and a drone came within 200 feet of colliding near Los Angeles' LAX airport in March 2016 and a JetBlue pilot taking off at JFK Airport reported a near collision with a drone at about 5,800 feet in January of 2017. The FAA chronicled 583 near misses between aircraft and drones between Aug. 21, 2015, and Jan. 31, 2016. That averages out to approximately 116 reported incidents monthly, with that number increasing (FAA.gov, 2017). The US Department of Transportation estimates that by the year 2035 175,000 unmanned aircraft will be used for commercial purposes, surpassing the number of manned aircraft (Volpe, 2013). This statistic emphasizes the impending disruption to traditional commercial airspace and the need for major legislative and regulatory attention with regard to commercial used of drones.

In order to assist consumers with information so that they do not break the law, the Federal Aviation Association is currently leading an outreach campaign to make end-users aware of the privacy and safety issues surrounding drone usage (U.S. Department of Transportation, 2018). The website offers guidance for anyone operating a UAS by providing information about airspace restrictions, and how not to endanger individuals or other aircraft. Additionally, the site offers No Drone Fly campaign materials, and an application called B4UFLY Mobile App that assists in determining airspace restrictions and other flying requirements based on an end-user's GPS location.

## 6. CONCLUSIONS

Little research has been done to understand the impact of the drone in commercial activity. The rapid growth of drone use by both civilians and businesses has created a number of challenges that include privacy and security concerns as well as legislative and regulatory issues. Existing regulations do not fully address the impact of these unmanned flying objects, and there is also the strong potential for intentional as well as unintentional misuse. Drones will inevitably be a key part of our trillion-sensor future, transporting a variety of sensors (thermal imaging, pressure, audio, radiation, chemical, biologics, and imaging) and are already connected to the Internet. This opens up possibilities for device-to-device communication, with operators, as well as introduces the potential for hacking.

These authors intend to extend this paper by incorporating a study of user acceptance of the drone as a "last mile" delivery mechanism. Similar to the rationale of Im, Kim, & Han (2008), we hypothesize that perceived risk and technology type will be important factors in users' acceptance of the drone as a delivery to the home mechanism.

Future research into the impact of the drone is needed. For example, an economic impact analysis of the impact of drone delivery upon traditional commercial delivery could help prepare the package delivery industry for the future. Additionally, economic impact analysis could help identify new revenue streams and job opportunities. A host of other issues could be examined to lead to a better understanding of commercial drone usage, including the social, political, and cultural contexts.

## 7. REFERENCES

Bamburry, D. (2015). Drones: Designed for product delivery. Wiley Online Library. Retrieved on May 19, 2018 from http://onlinelibrary.wiley.com/doi/10.1111/drev.10313/pdf.

Bard College Surveys Legal Cases Involving Drones. (2017). Retrieved on on June 5, 2018 from http://www.aero-news.net/index.cfm?do=main.textpost&id=74ea7944-ff2b-4e96-b5f8-4e9e09958f17.

Bloomberg News. (2018). This might be the first Drone-Related Aircraft Crash. Retrieved on February 25, 2018 from http://fortune.com/2018/02/16/south-carolina-drone-helicopter-crash/.

Bomboy, S. (2014). A Legal Victory for Drones Warrants a Fourth Amendment Discussion, NAT'L CONST. CTR. Retrieved on February 9, 2018 from http://blog.constitutioncenter.org/2014/02/

acourt-victory-for-drones-warrants-a-fourth-amendment-discussion.

Chamata, J. E. (2017). Convergence of the Unmanned Aerial Industry. Theoretical Economics Letters, 7(02), 175.

Clarke, R. (2014). The regulation of civilian drone's impacts on behavior privacy. Computer Law & Security Review, 30(1), pp. 286-305.

FAA.gov (2017). FAA Releases Updated Drone Sighting Reports. Retrieved on February 27, 2018 from https://www.faa.gov/news/updates/?newsId=87565on.

Im, I., Kim, Y., & Han, H. J. (2008). The effects of perceived risk and technology type on users' acceptance of technologies. Information & Management, 45(1), 1-9.

Kwon, H., Kim, J., & Park, Y. (2017). Applying LSA text mining technique in envisioning social impacts of emerging technologies: The case of drone technology. Technovation, 60, 15-28.

Laguna, J., & Marklund, M., Business Process Modeling, Simulation, and Design, Prentice Hall, New Jersey, 2005.

Michel, H.A. & Gettinger, D. (2017) Drone Incidents: A Survey of Legal Cases. Retrieved from http://dronecenter.bard.edu/files/2017/04/CSD-Drone-Incidents.pdf on February 9, 2018.

Pogue, David. (2016). Amazon reveals details about its crazy drone delivery program. Yahoo Tech. Retrieved on March 5, 2018 from https://www.yahoo.com/tech/exclusive-amazon-reveals-detailsabout-1343951725436982.html.

Slove, D. (2006). A taxonomy of privacy. University of Pennsylvania Law Review, 154(3), pp. 477-56-.

Stewart, J. 2017. PRESIDENT TRUMP MOVES TO FILL AMERICA'S SKIES WITH DRONES. Retrieved on February 17, 2018 from https://www.wired.com/story/faa-trump-drones-regulations/.

U. S. Const. amend. IV.

United States v. Jones, 132 S. Ct. 945, 963 (2012) (Alito, J., concurring in the judgment).

United States Department of Transportation (2018). Where to fly. Retrieved from https://www.faa.gov/uas/where_to_fly/ on February 17, 2018.

Vallesenor, J. (2013). Observations from above: unmanned aircraft systems and privacy. Harvard Journal of Law Public Policy, 36(2), 457-517.

Wigan, M., & Clarke, R. (2006). Social impacts of transport surveillance. Prometheus, 24(4), 389-4