PRIVACY, SECURITY, LEGISLATIVE, AND REGULATORY ISSUES SURROUNDING DRONE DELIVERY

Emergent Research Forum (ERF)

B. Dawn Medlin
Appalachian State University
vannoysa@appstate.edu

Sandra A. Vannoy
Appalachian State University
medlinbd@appstate.edu

Austin Eggers
Appalachian State University
eggersaf@appstate.edu

Abstract

This paper addresses commercial drone usage in relation to consumer deliver of products. As these unmanned flying vehicles become more prevalent in today’s society, they are being embraced as a mechanism to address the consumer’s ever-growing need for a quick delivery of products. In this paper, we provide an overview of the current state of drone delivery as well as addressing the issues of privacy and security, and current legislative actions.

Keywords


Introduction

Drones, essentially flying robots that can be controlled remotely or fly autonomously through embedded software and sensors that interface with global positioning systems or GPS (Hassanalian & Abdelkefi, 2017), are receiving increased attention around the globe. There has been a recent emphasis upon drones for commercial use, particularly in the area of consumer product delivery; however, little is known about the impact of this commercial application. 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.

First, we will provide an overview of drone usage in the commercial market. Secondly, we submit some information regarding security and privacy around commercial drone usage. Then, we give some updates on legislation and regulatory action, and conclude with a summary of how this paper will be extended to provide value to the body of knowledge around the commercial drone market.

Commercial Drone Use

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).
Interest by companies toward commercial drone usage and growth in e-commerce may be closely linked. Online retail sales is expected to grow to around $4 trillion by 2020. This means that almost 15% of the total retail market will account for e-commerce sales. The upward tick of e-commerce growth 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. This shift in the way consumers shop and receive goods offers opportunities for companies to consider the use of drones for the delivery of packages. While little is currently known about the promise and potential for delivery of packages by drone, 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 2013, Amazon announced its intention to implement a global drone-enabled delivery system, Prime Air. Since that time, Amazon, along with a number of other companies in the United States have expended tremendous effort in developing safe and reliable drone delivery, including delivery company Flirtey (Flirtey Continues to Lead Drone Delivery Industry, 2017), package delivery service UPS (Golgowski, 2017), and Google’s parent company, Alphabet’s Project Wing (Heath, 2018).

With the expansion of drone usage in commercial space, additional benefits can occur that include the economic benefits of job creation and new technological innovations.

**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.

The promise of commercial drones as data gathering agents is tremendous. Both quality and speed of data collection are improved, as drones can easily access areas where humans cannot. In fact, oil giant BP was the first company to receive FAA approval to operate a commercial drone for use of observation and data collection. The drone operator maintains both flight and camera control which allows fields of view that would otherwise be impossible (Four Reasons Commercial Drones Are Taking Flight in the Oil and Gas Industry, 2017). However, this capability gives rise to issues surrounding privacy and security as unmanned vehicles can take photographs, videos, capture information, and perform a number of other activities that can invade a person’s privacy. Additionally, little is known about how the information gathered by drones can be secured. 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.” However, of greater concern is that should this information fall into the wrong hands.

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. However, drones can also crash due to cyberattack, thus allowing others to not only possibly confiscate a product intended for delivery or even steal the drone itself, allowing miscreants to have access to the customer’s name, address and possibly phone number as well as other proprietary information.

Drones are similar to smart phones or other wireless devices, in that they can be hacked. They can be
targeted for command and control data link jamming and spoofing, which means that a hacker can block or falsify the data link in order to disrupt or take control of the device. Navigational sensor jamming can disrupt and take over navigation. Furthermore, hackers can tap the video or photo link, wherein they intercept the video and other data from the drone. U.S. Federal Trade Commission researchers were able to hack into three different off-the-shelf drones. They took over the camera feed on each drone; for two of the drones, they were able to turn off the aircraft during flight, making it fall from the sky as well as seize complete control of the flight path (Glaser, 2016).

Drone units are vulnerable to two 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, for example, 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. Currently, not all commercial drones use encryption methods that render them invulnerable to any currently known spoofing attack, but still leaves them 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 may be unavoidable in such scenarios, especially in an unregulated environment (Rao, B., Gopi, A., & Maione, R., 2016).

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 with all connected devices is that there are generally few clear rules or regulations instructing manufacturers of drones what is necessary to do in order to secure them from 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.

**Legislative and Regulatory Issues**

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 2007, the FAA banned commercial use of drones without a special permit. However, in 2012, Congress instructed the FAA to update current regulation, resulting in 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, the FAA missed that deadline, frustrating progress toward commercial drone operations in the US. Furthermore, “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 & Richard, 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 mandate. Visual line-of-sight ensures the pilot will only operate the drone as far as he or she can see. Efforts have been directed toward the FAA to further loosen restrictions, and largely depend upon innovations in technology to compensate for line-of-sight requirements. With the use of drones in commercial deliveries it will be quite difficult 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 in the short term (Schlag, 2017).
In December 2015, the FAA passed a federal law requiring all drones weighing over 250 g and their users to be registered online. The FAA justifies this law, having 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 technology or the user's experience in operating the UAV. As a result of this law, a user without a certificate can face both civil and criminal sanctions including fines and imprisonment, even when operating the UAV on their own property.

Further legislation regarding the commercial use of drones occurred under the Obama administration. Congress held hearings related to 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 impact of the technology on privacy and security (Thompson, 2015).

In June 2016, the FAA instituted a new rule pertaining to safety regulations for unmanned aircraft drones weighing less than 55 pounds that are used for commercial purposes. The ruling was intended to integrate UAVs into national airspace with an eye toward positive economic, scientific, and societal benefits, and with potential to generate more than $82 billion for the U.S. economy and create more than 100,000 new jobs over the next 10 years. U.S. Transportation Secretary at the time, Anthony Foxx, suggested that such rulings are essential, as "...the potential for unmanned aircraft will make it safer and easier to do certain jobs, gather information, and deploy disaster relief." The new rule is more concerned about safety and security, and unfortunately, does not specifically deal with privacy issues in the use of drones. However, for the first time the FAA is acknowledging privacy as a consideration, and intends to educate commercial drone pilots as part of the certification process, building upon guidance published by the National Telecommunications and Information Administration in consultation with privacy advocates and industry (Dorr & Duquette, 2016).

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, the proposal that appears the most promising will be implemented nationally (Stewart, 2017).

Conclusion

This paper introduces a number of issues that should be considered concerning the commercial use of drones. As interest in drones for commercial use increases, challenges including privacy and security give rise for the need for increased legislation and regulation that go beyond simple physical safety and the economic benefits.

Currently, we know very little about consumers’ attitudes toward product delivery by drone. Constructs important to this area of study are consumer intentions toward use, perceptions about privacy and security, as well as trust. Will there be a critical mass of consumers willing to purchase a product knowing that it will be delivered to their homes by drone? Given the promise of the drone as a viable “last mile” delivery alternative for products, now is the time for researchers to endeavor to more fully understand and address the myriad of issues surrounding this emerging phenomenon.

REFERENCES


