Commercial Drones: Security and Privacy Concerns

Sandra Vannoy, Appalachian State University, USA
Beverly Medlin, Appalachian State University, USA
Victoria Fowler, Appalachian State University, USA

Abstract

This paper addresses an emerging phenomenon, drone delivery and return services of commercial 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 quick delivery of products and services to their homes and possibly while on the road. A number of drone delivery services are being tested today, with countries around the world making sweeping regulatory changes to allow drones into commercial airspace. While drone delivery offers much promise in terms of changing the delivery landscape, these devices also open up a host of issues that must be addressed, with privacy and security is perhaps the most pressing. We provide an overview of the current state of drone delivery and returns as well as some food for thought with regards to privacy and security issues.

Introduction

Given a new emphasis upon drones for commercial use, more investigation is needed regarding the impact of the use of drones for commercial deliveries and returns. This paper will examine the drone in the context of commercial use of drones for consumer delivery and return services. First, we will provide an overview of the current state of consumer drone delivery services in the United States and around the world. Second, we will provide a perspective on privacy and security issues around consumer drone delivery and return services. Lastly, we will conclude with a set of recommendations and directions for future research.

Unmanned aerial vehicles (UAVs) or unmanned aircraft systems (UASes) are known in mainstream societies as drones. Drones are essentially flying robots that can be controlled remotely or fly autonomously through embedded software and sensors that interface with global positioning systems or GPS. These unmanned flying robots have been classified based upon their size, intended use, flight range, speed, power system, among others (Hassanalian & Abdelkefi, 2017).

As is the case with many new technologies in the mainstream today, the drone evolved from use by the military in intelligence gathering. Additionally, the functions of the drones were further examined as weapons carriers beginning in the early 2000s. McNeal (2012) suggested that the emergence of drones into the general public in the United States occurred due to the FAA Modernization and Reform Act of 2012, which loosened restrictions and provided greater airspace for drone flight. Also, in 2015 the FAA granted hundreds of new exemptions for companies to operate drones in commercial space including insurance, construction, and agriculture, but most of these exemptions (over 90%) were granted to small businesses having fewer than 10 employees (Joshi, 2017). Therefore, much of the world has quickly outpaced the United States in terms of the commercial use of drones by dramatically loosening governmental restrictions, with Poland and South Africa being notably aggressive countries in the use of drones (Smith, 2016). Placing drones within the congested nature of commercial airspace in the United States has proven quite complex, and therefore, the United States continues to lag behind much of the world in the use of drones for commercial purposes (Atwater, 2015). Nonetheless, the promise of drone usage within the commercial realm is great, with the global market expected to surpass $120 billion worldwide by 2021 (Joshi, 2017).

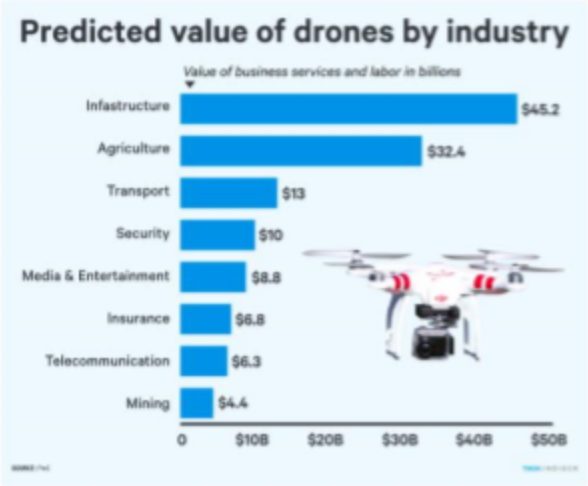

Figure 1: Drones predicted by Industry

In keeping with these projections and in order to compete in the global market place, in October 2017, the President of the United States, Barack Obama, approved a UAS Integration Pilot Program. The program provides an opportunity for local governments to partner with the private sector to accelerate safe UAS integration into national airspace. The Program is expected to provide immediate opportunities for new and expanded commercial UAS operations (https://www.faa.gov/uas/).

With encouragement from governmental bodies as well as changes in regulations in the commercial use of airspace, businesses around the world are starting to enter the consumer drone delivery market. Beyond simple convenience to the consumer, drone delivery offers much promise in terms of the delivery of medicine and food in hard to reach areas. Furthermore, when regulation and technology innovation converge to allow last mile delivery to the home, reductions in CO2 emissions could be significantly reduced (Goodchild and Toy, 2017). Social media company Facebook is even investigating the viability of solar powered drones that provide Internet access to rural areas and developing countries (Collins, 2016).

Literature Review

In December 2013, German postal and logistics group Deutsche Post DHL released a prototype of its Parcelcopter, which was designed to carry packages weighing approximately three pounds. With the intent to deliver and pick up packages in more rural and remote areas, by May 2016, the company had completed trials and successfully delivered packages to consumers in rural areas. DHL announced that customers in the Bavarian village of Reit im Winkl were able to send and receive packages using drones. One hundred thirty successful autonomous drone deliveries were carried out involving heavy loads, long distances and difficult terrain (DHL Completes Three-Month Test of Delivery Drone, 2017). Similarly, in February 2017, United States-based UPS (United Parcel Service0 began testing residential package delivery services by drones, using them in conjunction with its traditional brown van delivery and pick up services. The drone is launched from the van, delivers the package to the consumer's home, and then returns to the van where it is pulled inside the van by a robotic arm (Air we go: UPS in drone delivery, 2017).

Following approval by the Icelandic Transport Authority, in August 2017, Iceland launched arguably the world's first fully operational drone delivery service. It is a cooperative effort between drone company Flytrex and Iceland's online marketplace, AHA. Iceland's transportation authority has stated, "The drones will reduce the load on the transport infrastructure leading to safer roads. Simultaneously, people have access to a better and faster delivery service which can only be seen as an advantage," (Gilchrist, 2017). The hexacopter-type drones are able to pick up orders from restaurants and stores that are no more than 3 kilograms in weight, and deliver them to a drop-off point in the suburb of Grafarvogur where a truck will complete the delivery, significantly reducing delivery wait times and human interactions

(Rubin, 2017). The Icelandic drone delivery solution does not address the "last mile" delivery issue, however, identified by many as the most problematic link in the supply chain (Murray and Chu, 2015).

Supply Chain Management has become a key factor in achieving a competitive advantage in the marketplace. Using the upstream and downstream activities they are "linked," together through either physical or information flows. Companies have been operating and managing supply chains for a long period of time or as long as businesses have existed, but they were not identified using that term. Recently, many industries have paid close attention to the potential benefits of a supply chain decision as it could have an immediate impact on their bottom line. As in this case, the use of drones for delivery and retrieval of products.

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). It should be noted that the United States-based pizza delivery program was approved by the FAA only after the program's success had been demonstrated in New Zealand.

In 2014, Amazon announced that it was involved in testing various drone technologies and began soliciting support from the FAA. Receiving little to no support from the United States, Amazon moved its efforts to the more supportive global marketplace, including England and Canada. In 2016 Amazon completed its first successful drone delivery in the small rural town of Cambridge, England, and was quickly given permission by the UK to proceed with delivery of packages in the rural area weighing up to five pounds (Abdulla, 2017). With the recognition that the United States was lagging behind other countries, the FAA has begun to slowly loosen restrictions, bringing in Amazon's Prime Air and Alphabet, Google's parent company's Project Wing to work with NASA on technology and an airspace plan for drones. While Amazon completed a successful drone delivery demonstration in 2017 at a public event in California, it continues its efforts to make drone delivery to the home a reality by addressing operational and structural challenges, including new ideas for placement of distribution centers. To overcome the challenges of having static distribution centers in a few mostly coastal United States locations, Amazon is looking at ways to develop mobile facilities located on trains, ships and trucks that are capable of maintaining drones and acting as hubs for deliveries (Abdulla, 2017). Other issues that must be addressed are ways to recharge the drones' power systems and safety measures such as drone body structures that break apart in many small pieces reducing the possibility of damage and injuries to those people and structures below. In 2017 Alphabet, in collaboration with NASA, tested air traffic management capabilities for drones, demonstrating that a single operator was able to control six drones built on different platforms, all sharing the same general airspace. Tests like these show that it is possible to avoid collisions with items in the terrain as well as interference with other commercial airspace (Etherington, 2017; Krol, 2015).

Clearly, package delivery and returns by drones holds offers many advantages. Much needed medical supplies can be delivered to rural and remote areas. Companies can address consumer demand for faster and faster delivery times for products and services. Environmental concerns around traditional delivery methods can be addressed. However, many questions remain unanswered. At what scale does drone delivery make sense? When a single UPS truck makes an average of 120 stops per day and delivers sometimes thousands of packages, the viability of drone delivery bears closer scrutiny (Jacobsen, 2016). Furthermore, as with any emerging technology, little has been done to understand the legal, privacy, security, and ethical concerns around drone delivery and return services, which exist at a scale never imagined with many other emerging technologies.

Privacy and Security Concerns

The widespread adoption of commercial drone's opens up a wide range of dilemmas and questions regarding privacy and security surrounding both the consumer and the product. In the sections below, we will discuss issues related to privacy and security concerns.

Privacy

According to several privacy theorists, when privacy is invaded or violated, it is lost (Margulis, 2005). Privacy can be an ambiguous term that differs among industries, contexts, and consumers. The term privacy can mean different things in different contexts, which becomes apparent when attempting to apply traditional privacy concepts to newer technologies such as drones. Further, the concept of a private life means separation from others and generally includes the ability of one person to select to disclose information about themselves in a selective way. Privacy can also fluctuate according to cultural, national, individual particularities of a country or region and has been often associated to the west European culture where the concept of privacy was developed (Serbua & Rotariua, 2015).

According to John Villasenor (2013), in his article, Observations from Above: Unmanned Aircraft Systems and Privacy, he indicated the importance of proactively addressing the invasion of privacy as noted in his statement below. "Thus, while it is important to proactively consider how to protect against the privacy abuses UAS [Unmanned Aircraft Systems] could make possible, in doing so it is important to recognize the near impossibility of predicting all of the ways that a rapidly developing technology can be used—for good or for ill—in future years. Maintaining that perspective will be vital in achieving good UAS policy outcomes" (p. 517).

Understanding the risks and liabilities of using commercial drones that can be taken over by hackers or even the insider threats of employees will be issues that will need to be addressed in relation to privacy concerns now and in the future (Pozzi, 2014). As well, legislative actions that protect individuals privacy rights such as the Fourth Amendment to the U.S. Constitution will also need to be addressed in relation to individual's and their expected right to privacy.

Security

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' (Wolfer, 1952) 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, however, lead to a range of concerns not seen with many emerging technologies. One of the primary issues with all connected devices is there are generally few clear rules or regulations indicating to manufacturers of drones what is necessary to do in order to secure drones from being tampered with 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.

Drone units are vulnerable to two different kinds of 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).

As mentioned earlier, the FAA enacted the FAA Modernization and Reform Act of 2012 (FMRA), hat 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. Again, in this paper we focus on the commercial operators that deliver packages for their customers who may need to return packages using drones as their method of return.

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).

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)

One of the primary concerns of the use of drones related to privacy and security is the issue of surveillance which can include both passive and active data collection. Surveillance in relation to drones is about the collection of information. This collection of data may include the indiscriminate recording of people in a broad sweep that passively gathers information as it is on its delivery or return route of a product or a service. For instance, a drone can use a camera sensor that will locate their customer's address, while at the same time collecting other types of data in a broad sweep of the area. The information that may be loaded and then collected is certainly necessary for accurate deliveries, but the collection and storing of a broad area while searching for a specific address by the drone, begs the question of the public's right to privacy. Though the delivery should be to a targeted data collection address, the drone's surveillance may bring forth questions related to the issues of secrecy, autonomy, and anonymity (Thompson, R. 2015).

In 1997, Great Britain conducted a type of target by drones identified as discriminatory targeting (Lynch, 2012). Their surveillance indicated that "Black people were between one-and-a-half and two-and-a-half times more likely to be surveilled than one would expect from their presence in the population" (Norris & Armstrong, 1997).

Though not a commercial drone, but as an example of the rate of collection on public places and individuals. In 2013, the U.S. Air Force Intelligence, Surveillance and Reconnaissance (ISR) Agency was streaming over 7 terabytes of data a day into their system from drones. That's about 1,600 hours every single day as early as 2013 (Asli, 2017). Between the public and private sector, that number is going to be a lot higher in 2017. But with that much data coming in, the question still remains "What are they doing with it once they've collected this info? (Asli, 2017).

Just like the military, 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."

Presented below are possible scenarios of deliveries and returns, repairs, and waste scenarios that address issues related to privacy and privacy.

Delivery and Return

Scenario Below, is a delivery and return scenario by a drone that involves both the supplier and the consumer as well as multiple aerial locations. The question becomes, who is addressing the issues of security and privacy throughout the process? This is certainly a question that will need to be asked as drones are being used more often for deliveries of many different types of items.

1.1 Returns Scenario

Suppose a customer ordered a product from Amazon, but when it arrived, it was a different color than the one that was ordered. The customer could use the Amazon app on their phone to place a Product Return Order. The app would then instruct the customer to put the incorrect item back into the box in which the original drone had delivered it and place it on a specific location on their property. If a drone was already in the area delivering a package, a notification would be sent to it to pick up the Product Return Order on its route back to the Amazon warehouse. If there was not a drone within a certain radius, one would be dispatched to pick up the package and return it to Amazon. This is certainly a benefit to have an item received so quickly and to be returned so promptly. But the question remains, how many security issues will the drone be faced with as it has been directed and redirected to many different sites? What about the privacy of the consumer if the drone is hacked and their information is no longer private? Just as shown in this scenario, the drones' flexibility and mobility gives them the ability to intrude into people's private space and compromise people's physical privacy.

1.2 1.2 Repairs Scenario

Suppose a customer breaks down on the side of the road due to a flat tire, battery issue, or running out of gas. The customer could use the AAA Roadside Assistance application on their phone to report the type of issue. A drone would then be deployed from a repair center, using the location services of the customer's phone to determine its destination. The drone would have a speaker on it with step-by-step instructions for the customer as well as any tools necessary to complete the repair. Depending on the issue, a new tire, battery, or gallon of fuel may also be attached to the drone. Certainly, the benefit of the drone delivery and assistance of AAA Roadside Assistance could cut their service time in half and customers could be back on the road in a matter of minutes. The question surrounding privacy still remains in this situation, what if the wrong product is delivered, or the incorrect address is provided by the consumer and the drone has to make another flight and return to another destination? All of this information of where the drone had been and will be going has been recorded as well as the consumer's private information. Hackers thereby have a wealth of information such as personal information of location, names, addresses and phone numbers of the consumer. Also, of concern is what these companies do with this information. As services like AAA only will offer a number of towing opportunities, they must track how many services have been used by the consumer and where they services were provided. Questions of privacy and security related to these types of instances only show how vulnerable information is handled.

1.3 Hazardous Waste Disposal Scenario

Suppose a restaurant had an issue with hazardous grease disposal. Restaurants produce an average of 40 lbs. of grease per week. However, most restaurants only dispose of their grease once a month. Collecting old grease creates many hazards, such as fire and health risks. With weekly drone pickups, the grease could be taken to a biodiesel company for a healthier and easier waste disposal activity. This could benefit both the restaurants and the biodiesel production plants. But what if the drone dropped the product over a busy highway causing possible automobile accidents and/or deaths? What information is made available and to whom? Would the media pick up on this accident and be reporting it on the news, thus affecting the privacy information of the company?

These examples identify a number of different scenarios that a company and its consumer might face while attempting to distribute and return products that have been delivered by drones and shows some of the issues that might be faced related to privacy and security. As mentioned above in the scenarios, each can offer an advantage, but what about the disadvantages that can create harmful and lasting impressions and customers that may have to deal with issues such as identify theft for years? Often with new technologies, privacy and security are dealt with as an afterthought and add-on, with most emphasis being placed upon financial gain and first to market. With the drone being so new on the delivery landscape, it would behoove researchers and innovators to identify ways that privacy and security protections can be built in from the front end.

Conclusions

It is expected that the number of drone deliveries and returns will only grow in the coming years as companies use this type of method in order to remain competitive. Issues of responsibility, security and privacy issues are certainly at the forefront of issues that must be addressed in both the areas of delivery and the return of a product. Several questions remain answered surrounding responsibilities or legal liabilities of drone's that have either been hacked or have arrived at unbeknownst locations.

Security and privacy issues in relation to drone delivery of such items as medicines also offer opportunities for cyber criminals to become more active in the movement and sales of products. As noted earlier, situations can exist where hackers might be able to command or take over the drone and change its destination. Other items related to warfare, police actions and other critical issues should also be of concern as drones can be rerouted to other locations.

Future research is needed beyond privacy and security to address a number of questions around social, cultural and legal ramifications of drone delivery services. For example, the nature of "culture" is reflected in the use of drone information as it refers to the shared beliefs, customs, and behaviors that characterize a society. Culture is handed down generally from one or a group of individuals who live a certain way of life and is often considered the broadest influence on a consumer's behavior. An individual's culture has been shown to be a large and influential effect on the items that they purchase. The saying of "keeping up with the Joneses has been proven many times. This phrase originated from a cartoon strip by that name in 1913 and was published for 26 years (Pritchard, 2013). But this phrase still continues today as individuals watch on cable TV shows such as Keeping up with the Kardashians. We have become a culture of "keeping up," and we desire and in fact demand instant gratification. This has driven companies to continually find ways to get their products in the consumers' hands in the shortest amount of time. As mentioned earlier, companies like Amazon must incorporate ways to address consumer demand for instant gratification, such as delivery by drones.

This paper addresses a nascent phenomenon, drone delivery services. The drone delivery phenomenon brings a number of issues that must be addressed and further investigated as the skies will inevitably become busier with drone deliveries and returns.

References

Abdulla, H. (2017). Amazon mulls drone hubs on trains, ships and trucks. Retrieved from https://www.juststyle.com/news/amazon-mulls-drone-hubs-on-trains-ships-and-trucks_id131444.aspx.

Air we go: UPS in drone delivery. (2017, February). Retrieved from http://link.galegroup.com/apps/doc/A482080053/BIC1?u=boon41269&xid=3adae98e.

Arash, A. (2017). Only Taking What They Want. Retrieved from https://www.forbes.com/sites/forbestechcouncil/2017/01/03/data-from-drones-how-companies-cancollect-store-and-use-these-insights/#578da298397d.

Atwater, D. (2015). The Commercial Global Drone Market: Emerging Opportunities for Social and Environmental Uses of UAVs. Graziadio Business Review 18(2).

Behavioral Targeting (2017). Retrieved from https://www.bluefountainmedia.com/glossary/behavioraltargeting/.

Collins, J. (2016). Drones: Is drone delivery simply pie in the sky? Retrieved from https://www.journalofaccountancy.com/issues/2016/dec/drone-delivery.html.

DHL Completes Three-Month Test of Delivery Drone (2016, May). Retrieved from http://www.ttnews.com/articles/dhl-completes-three-month-test-delivery-drone.

Etherington, D. (2017). Google's Project Wing team takes a key step towards making drone delivery real. Retrieved from https://techcrunch.com/2017/06/07/googles-project-wing-team-takes-a-key-steptowards-making-drone-delivery-real/.

Flirtey Continues to Lead Drone Delivery Industry (2017, July). PR Newswire. Retrieved from http://link.galegroup.com/apps/doc/A499279501/BIC1?u=boon41 269&xid=55fd4fed.

Gilchrist, K. (2017, August). World's first drone delivery service launches in Iceland. Retrieved from https://www.cnbc.com/2017/08/22/worlds-first-drone-delivery-service-launches-in-iceland.html.

Glasser, A. (2016). Obama says the U.S. government still doesn't know who shut down the internet last week. Retrieved from https://www.recode.net/2016/10/25/13406546/internet-shutdown-outagebotnet-attack-ddos-denial-of-service.

Goodchild, A., & Toy, J. (2017). Delivery by drone: An evaluation of unmanned aerial vehicle technology in reducing CO 2 emissions in the delivery service industry. Transportation Research Part D: Transport and Environment. In press.

Hassanalian, M., & Abdelkefi, A. (2017). Classifications, applications, and design challenges of drones: A review. Progress in Aerospace Sciences. 91, 99-131.

Jacobsen, M. (2016). The Promise of Drones. Harvard International Review, 37 (3), 27-31.

Joshi, D. (2017, August). Commercial Unmanned Aerial Vehicle (UAV) Market Analysis – Industry trends, companies and what you should know. Retrieved from http://www.businessinsider.com/commercial-uavmarket-analysis-2017-8.

Krol, C. (2015, November). Is delivery by drone the future of shopping? Telegraph Online Biography in Context. Retrieved from http://link.galegroup.com/apps/doc/A433568818/BIC1?u=boon4126.

McNeal, G. (2012, April). A primer on domestic drones: Legal, policy, and privacy implications. Forbes. Retrieved from www.forbes.com/sites/gregorymcneal/2012/04/10/a-primeron-domestic-drones-andprivacy-implications/.

Margulis, S. (2005). Privacy as a Social Issue and Behavioral Concept. Journal of Social Issues, 59(2), 243261

Murray, C. C., & Chu, A. G. (2015). The flying sidekick traveling salesman problem: Optimization of droneassisted parcel delivery. Transportation Research Part C: Emerging Technologies, 54, 86-109.

Pozzi, S. R. (2014). Drones in our future. Best's Review, 115(2), 56. Retrieved from http://web.b.ebscohost.com/ehost/detail/detail?vid=2&sid=f34c5299-d508-4ea9-860d573932ebf745%40sessionmgr113&hid=106&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#db=bth&AN= 96327351.

Pritchard, M. (2013, January). Who Are the Joneses and Why Are We Trying to Keep Up With Them? Retrieved from https://www.huffingtonpost.com/mary-pritchard/keeping-up-with-thejoneses_b_2467957.html.

Rao, B., Gopi, A., & Maione, R. (2016). The societal impact of commercial drones. Technology in Society. 45, 83-90.

Rubin, E. (2017, August). Buzzing Over BDS, Israeli Firm Launches World's First Drone Delivery Service. Retrieved from https://www.haaretz.com/israel-news/business/1.809072.

Serba, R. (2015), 22nd International Economic Conference – IECS 2015 "Economic Prospects in the Context of Growing Global and Regional Interdependencies", IECS 2015.

Sifton, J. (2012, February). A brief history of drones. The Nation. Retrieved from http://www.thenation.com/article/166124/briefhistory-drones.

Smith, G. (2016, May). Here Comes the Latest Drone Army. Retrieved from http://fortune.com/2016/05/09/here-comes-the-latest-drone-army/.

Thompson, R. (2015, March). Domestic Drones and Privacy: A Primer. Retrieved from https://fas.org/sgp/crs/misc/R43965.pdf.

Villasenor. J. (2013). Observations from Above: Unmanned Aircraft Systems and Privacy. Retrieved from https://pdfs.semanticscholar.org/ec9a/8458e8fe4c2511c2e18f557eae8ddedb2289.pdf.

Wolfers, A., "National Security" as an Ambiguous Symbol', Political Science Quarterly, 67, 483.