

JOURNAL OF INFORMATION SYSTEMS APPLIED RESEARCH

Volume 14, Issue. 2
June 2021
ISSN: 1946-1836

In this issue:

- 4. Privacy Concerns and Data Sharing Habits of Personal Fitness Information Collected via Activity Trackers**
Jamie Pinchot, Robert Morris University
Donna Cellante, Robert Morris University

- 14. A Prototype for Distributed Computing Platform using Smartphones**
Jeffrey Wagner, Grand Valley State University
Xiang Cao, Grand Valley State University

- 22. A Comparative Study on Information Technology (IT) Infrastructure and Disaster Recovery Methodology**
Delester Brown Jr., Colorado Technical University
Samuel Sambasivam, Woodbury University

- 31. The Promise and Peril of Drone Delivery Systems**
Victoria Fowler, Lowes Companies, Inc
Austin Eggers, Appalachian State University
Sandra A. Vannoy, Appalachian State University
B. Dawn Medlin, Appalachian State University

- 42. Towards a Leader-Driven Supply Chain Cybersecurity Framework Analysis of Security Features and Vulnerabilities in Public/Open Wi-Fi**
Manoj Vanajakumari, University of North Carolina Wilmington
Sudip Mittal, University of North Carolina Wilmington
Geoff Stoker, University of North Carolina Wilmington
Ulku Clark, University of North Carolina Wilmington
Kasey Miller, Naval Postgraduate School

The **Journal of Information Systems Applied Research** (JISAR) is a double-blind peer reviewed academic journal published by ISCAP, Information Systems and Computing Academic Professionals. Publishing frequency is three to four issues a year. The first date of publication was December 1, 2008.

JISAR is published online (<https://jisar.org>) in connection with CONISAR, the Conference on Information Systems Applied Research, which is also double-blind peer reviewed. Our sister publication, the Proceedings of CONISAR, features all papers, panels, workshops, and presentations from the conference. (<https://conisar.org>)

The journal acceptance review process involves a minimum of three double-blind peer reviews, where both the reviewer is not aware of the identities of the authors and the authors are not aware of the identities of the reviewers. The initial reviews happen before the conference. At that point papers are divided into award papers (top 15%), other journal papers (top 30%), unsettled papers, and non-journal papers. The unsettled papers are subjected to a second round of blind peer review to establish whether they will be accepted to the journal or not. Those papers that are deemed of sufficient quality are accepted for publication in the JISAR journal. Currently the target acceptance rate for the journal is about 40%.

Questions should be addressed to the editor at editor@jisar.org or the publisher at publisher@jisar.org. Special thanks to members of ISCAP/EDSIG who perform the editorial and review processes for JISAR.

2021 ISCAP Board of Directors

Eric Breimer
Siena College
President

James Pomykalski
Susquehanna University
Vice President

Jeffrey Babb
West Texas A&M
Past President/
Curriculum Chair

Jeffrey Cummings
Univ of NC Wilmington
Director

Melinda Korzaan
Middle Tennessee State Univ
Director

Niki Kunene
Eastern CT St Univ
Director/Treasurer

Michelle Louch
Carlow University
Director

Michael Smith
Georgia Institute of Technology
Director/Secretary

Lee Freeman
Univ. of Michigan - Dearborn
Director/JISE Editor

Tom Janicki
Univ of NC Wilmington
Director/Meeting Facilitator

Anthony Serapiglia
St. Vincent College
Director/2021 Conf Chair

Copyright © 2021 by Information Systems and Computing Academic Professionals (ISCAP). Permission to make digital or hard copies of all or part of this journal for personal or classroom use is granted without fee provided that the copies are not made or distributed for profit or commercial use. All copies must bear this notice and full citation. Permission from the Editor is required to post to servers, redistribute to lists, or utilize in a for-profit or commercial use. Permission requests should be sent to Scott Hunsinger, Editor, editor@jisar.org.

JOURNAL OF INFORMATION SYSTEMS APPLIED RESEARCH

Editors

Scott Hunsinger
Senior Editor
Appalachian State University

Thomas Janicki
Publisher
University of North Carolina Wilmington

2021 JISAR Editorial Board

Ulku Clark
University of North Carolina Wilmington

Christopher Taylor
Appalachian State University

Ed Hassler
Appalachian State University

Karthikeyan Umapathy
University of North Florida

Muhammed Miah
Tennessee State University

Jason Xiong
Appalachian State University

James Pomykalski
Susquehanna University

The Promise and Peril of Drone Delivery Systems

Victoria Fowler
Victoria.fowler@lowes.com
Lowes Companies, Inc.
 Mooresville, North Carolina 28117, USA

Austin Eggers
eggeraf@appstate.edu
Department of Finance, Banking, & Insurance

Sandra A. Vannoy
vannoysa@appstate.edu
Department of Computer Information Systems

B. Dawn Medlin
medlinbd@appstate.edu
Department of Computer Information Systems

Appalachian State University
Boone, North Carolina 28608, USA

Abstract

Despite increasing demand for quick product delivery in today's supply chains, delivery by drone is relatively rare in the United States. Security and privacy concerns along with legislative issues are often cited as barriers to the adoption of home and commercial drone delivery services. The purpose of this study is to examine the current state of drone deliveries, and to identify some of the adoption barriers as well as factors that contribute to the adoption of drone delivery services. Interestingly, the study shows several factors that affect an individual's inclination to adopt delivery by drones such as rural versus urban locations, drone ownership, and propensity to shop online. Academic and practical implications are drawn from these findings to conclude this study.

Keywords: Drone, Supply Chain Management, Logistics, Legislation, Privacy, Security

1. INTRODUCTION

Supply Chain Management (SCM) has been an integral part of our business history. With the integration of technology into supply chain management processes, supply chains can be used to provide quicker deliveries of products and services. A supply chain involves various participants such as customers, vendors, and others who perform a sequence of tasks or activities that can move physical goods or

services from one location to another (Crandall et al., 2015). Therefore, each supplier, vendor, and customer is linked together through the transfer of goods, information, services and payments.

The term "logistics" is often used synonymously with supply chain management. While, logistics focuses more on the movement and coordination of goods and services, supply chain management is the overarching theme of the

entire operation. Ultimately, logistics and supply chain management have become key factors in achieving a competitive advantage in the marketplace. Recently, many industries have begun to pay closer attention to the potential benefits of smart supply chain decisions and the immediate impact upon the company's bottom line.

In an effort to use logistics toward positive impacts upon the bottom line, companies such as Amazon and Walmart are continually seeking ways to move products faster. In 2018, Amazon reported that over 60% of its US consumers were Prime members, paying a premium in order to receive goods in two days without paying additional shipping costs (Kuntze et al., 2018). One way that Amazon and other companies are addressing their commitment to better logistics is by using drones to deliver products efficiently and lower cost than package and service deliveries.

As an example Amazon began employing drone deliveries in 2013 as they raised the bar for other companies around the globe, announcing the implementation of Prime Air Drone Delivery. The Amazon announcement was a large step towards the adoption and use of logistics to further enhance product and service deliveries, while enhancing the bottom line. However, after receiving little to no support in the United States, Amazon moved its efforts in 2016 to a more supportive global marketplace in Cambridge, England. The United Kingdom hastily permitted Amazon's continuation of the exploration of drone deliveries (Abdulla, 2017). With the United States' Federal Aviation Association (FAA) realization that drone deliveries were behind in the U.S., they have become more active in addressing and revising airspace restrictions, allowing for more forms of drone delivery possibilities.

In the last several years, delivery companies such as Flirtey have completed several FAA-approved drone deliveries, including medical supplies to remote area medical health clinics such as in Wise, Virginia, in 2015. Additionally, Domino's Pizza Company is currently delivering pizzas by drones in some areas. Walmart has launched a small pilot program in Fayetteville, North Carolina, delivering packages weighing up to 6.6 pounds within a 6.2 miles round trip (Vincent, 2020). In October 2019, UPS (United Parcel Service) received U.S. Government approval to operate a drone airline and made an inaugural flight from WakeMed's hospital campus in Raleigh, N.C. ("UPS Flight Forward Attains

FAA's First Full Approval For Drone Airline," 2020). The company has also been approved for the use of drones that weigh 10 pounds or less and can cover a 30-minute flight time.

Drone delivery has also helped to address "the last mile" issue. The last mile is a vital portion of supply chain logistics, as it generally consists of approximately 28% of the overall cost of the delivery transaction. Therefore, a major factor in ensuring consumer satisfaction is making sure that the right item is delivered at the right time. Companies adopting the use of drones, both in delivery throughout the entire stage of the process as well as the last mile, can significantly help in increasing overall efficiency and subsequently decreasing the total time of the delivery, thus addressing time expectations of consumers, suppliers, and vendors.

Given the new emphasis upon drones for delivery of products, more investigation is needed to better understand both the positive and negative impacts. While drones seem to offer an array of benefits, including cheaper costs and faster deliveries, there could also appear negative consequences. Little is known about consumers' perceptions of this new delivery phenomenon, nor do we fully understand the impacts upon traditional delivery methods. Furthermore, does existing policy fully address drones, or is additional legislation needed?

The purpose of this study is to increase understanding of people's perceptions of drone delivery. In the following sections we present a literature review comprising our current understanding of drones as a delivery mechanism, legislative issues, and matters of security and privacy. A survey-based study was conducted and findings are presented. We conclude with recommendations and suggestions for future research.

2. LITERATURE REVIEW

Drones are generally identified as unmanned aerial vehicles (UAV) or unmanned aircraft systems (UAS), essentially flying robots that can be controlled remotely or fly autonomously through embedded software and sensors that interface with global positioning systems (GPS). These unmanned flying robots have been classified based upon their size, intended use, flight range, speed, power system, among other categories (Hassanalian & Abdelkefi, 2017). Drones evolved from the military, which used them initially for intelligence gathering, and

were further expanded for use as weapons and supplies carriers beginning in the early 2000s. They have been especially useful to strike specific targets, and without harming innocent civilians.

Much of the world has quickly outpaced the United States in terms of home and commercial use of drones by dramatically loosening governmental restrictions, as is the case with Poland and South Africa (Smith, 2016). 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 the commercial segment including insurance, construction, and agriculture, but most of these exemptions (over 90%) were granted to small businesses having fewer than 10 employees (Joshi, 2017).

Placing drones within the congested nature of commercial airspace in the United States has proven quite complex, contributing to the United States' questioning the viability of the use of drones for commercial purposes (Atwater, 2015). Nonetheless, the promise of drone usage within the commercial realm is growing, with the global market expected to surpass \$120 billion worldwide by 2021 (Joshi, 2017).

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, drones can often provide services or deliveries to allow for a last mile delivery to the home, which can offer significant reductions in CO2 emissions (Goodchild & Toy, 2017).

In order to compete in the global market place for drones, in October 2017, then President of the United States, Barack Obama, approved a UAS Integration Pilot Program. The program was created to provide an opportunity for local governments to partner with private sector organizations to accelerate safe UAS integration into national airspace. The program was touted as expecting to provide immediate opportunities for new and expanding commercial UAS operations.

Legislative Issues

A variety of laws may be applicable to drones and their usage including trespassing, publication of public facts, and stalking and harassment (Vallesenor, 2013). To complicate things further, different localities such as states and towns may each have differing laws in relation to airspace usage according to federal legislation.

The FAA enacted the FAA Modernization and Reform Act of 2012 (FMRA) that initiated the integration of unmanned aircraft systems (UAS), or "drones," into the national airspace by September 2015. Under federal law, all UAVs must apply to the FAA for permission to fly unless they fall under the exception clause (Thompson, 2015).

The process for obtaining permission to operate drones differs depending on whether the drones are to be operated by private or public commercial operators. In the aviation industry, rules and regulations guiding flight are imposed to ensure safety. Some rules have been applied to UAV's so that the UAV's are operated for legitimate purposes only and not to act as a distraction or threat to the security of people or other items. It is important that organizations as well as companies who need to fly manned aircraft apply for an AOC (air operator certificate). These restrictions can be strict and can also be put in place regarding the ownership and use of the drone. With these restrictions in place the government can monitor airspace usage and put in measures the unapproved use of drones.

One of the key takeaways from the 2012 legislation is the visual line-of-sight (VLOS) mandate. VLOS ensures that the pilot will only operate the drone as far as he or she can see. Everyone's vision is different, but the drone would not be legally able to travel very far. It is expected that it will take time for the FAA to further loosen restrictions in order to address issues such as these. With the use of drones in both commercial and home 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 (Schlag, 2017) and companies may apply for waivers from some restrictions, including VLOS ("Part 107 Waivers," n.d.).

Amazon was one of the first companies to receive approval from the FAA to operate its fleet of Air Prime delivery drones in the United

States. Amazon's certification granted in 2010 will also grant the company an exemption under Part 135 of the FAA regulations which will allow the business to carry property on small drones beyond the visual line of sight of the operator (Palmer, 2020).

Since that time several companies have requested waivers from the FAA to promote commercial drone deliveries. In April 2019, the Alphabet-owned Wing Company became the first drone delivery company to receive FAA approval for commercial deliveries in the United States after implementing many of the safety regulations required of a traditional airline (Jones, 2019). In that same year, the United Parcel Service further obtained permission from the FAA to fly its new fleet of drones as an airline. ("UPS Flight Forward Attains FAA's First Full Approval For Drone Airline," 2019).

Focusing on the privacy and safety concerns of commercial drone operations, the FAA passed a federal law in December 2015 requiring all drones weighing over 250g and their users to be registered online. The law was partly enacted as a result of the 1133 reported cases of unsafe drone usage reported to the FAA that year (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 users' experiences. As a result of this law, a user without a certificate, and even on their own property, can face both civil and criminal sanctions including fines and imprisonment.

Further prompting the use of drone technology, 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 United States. The memo directed the DOT to take proposals from local, state, and tribal leaders over several months, and then select the most promising proposals (Stewart, 2017).

As of 2020, the US Department of Transportation has selected 10 state, local and tribal governments as participants. It is expected that this program will help to address some of the most significant challenges to integrating drones into the national airspace and will reduce risks to public safety and security (U.S. Dept. of Transportation, 2020). In addition, and despite the many restrictions currently regulating drone usage, it appears government agencies are beginning to recognize

the practicality and inevitability of commercial drone deliveries. As noted on December 28, 2020, the FAA issued new policies that would allow drones under fifty-five pounds to operate at night and over people (Diaz, 2020). These revised regulations are a significant step forward in the utilization of drone technology in a commercial setting by obviating some of the most obvious and constraining regulatory impediments prohibiting commercial drone usage in the United States.

Even with guidelines in place, it is expected that drone operators whether intentionally or unintentionally may create scenarios whereby they violate privacy and security laws as well as other established legislation.

Privacy and Security Issues

Though the FAA may not have strict rules for drone use in relation to privacy issues, many states and localities have strict Peeping Tom regulations that may apply if a drone were to hover over private residences. However, the FAA is relying on local law enforcement agencies to address this issue.

Outside of the United States legal system, an international framework that exists in the form of the International Covenant on Civil and Political Rights (ICCPR) exists in order to address issues related to security and privacy. 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 concerning the strength of the Fourth Amendment in relation to consumers and their privacy protections from the use of drones and their capabilities. 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 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 to implicate 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 use technologies to gather an abundance of intimate details and information, 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.

The abilities of drones to hover over or enter private property undetected and to capture information significantly offers opportunities for privacy and security breaches. According to several privacy theorists, when privacy is invaded or violated, it is lost (Margulis, 2005). Privacy can be an unclear term that differs among industries, contexts, and consumers. The ambiguity of the word "privacy" 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 to select the information and mode with which to disclose their personal matters. Privacy can also fluctuate according to cultural, national, individual particularities of a country or region. It has often been associated with the west European culture, where the concept of privacy was developed (Serbua & Rotariua, 2015).

While privacy and data security are important considerations, physical security is also in question. As drones become more popular, increases in accidents are also expected. As for instance, in February 2018 a helicopter crash occurred in South Carolina which was shown most likely to be triggered by a civilian drone, and will most likely not be the last. 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 drones are being purchased (Bloomberg, 2018). The drone nor the owner of this accident could be identified, thus creating another level of justice to be addressed.

Though this may have been the first noted crash, there have been drone near misses that have created serious and almost deadly results. Another example of near misses occurred when 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 (FAA.gov, 2017).

According to John Villasenor (2013), in his article, *Observations from Above: Unmanned Aircraft Systems and Privacy*, "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."

Understanding the risks and liabilities of using drones that can be taken over by hackers, or even the inside threats of employees, will be an issue that must be addressed (Pozzi, 2014). Furthermore, legislative actions that protect individual's privacy rights such as the Fourth Amendment to the U.S. Constitution will also need to be addressed in relation to individuals and expectations of privacy.

Security, like privacy, has different meanings in different contexts. Arnold Wolfer's (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). This statement captures the basic intuitive notion underlying most uses of the term security and can be applied to many different generic situations.

Security, as related to drone technology, leads to a range of concerns that is not typically seen with other emerging technologies. One of the primary issues is the lack of clarity. With all connected devices related to drone operation, there are very few clear rules or regulations indicating the necessary steps to securing drones from being tampered with by malicious hackers (Glaser, 2016). It could be surmised that, organizations are more concerned with their bottom line than the issues of privacy and security, as there are currently only a few legal ramifications.

Drone units are vulnerable to two different kinds of attacks that can corrupt their GPS navigational systems. Spoofing entails the sending of strong, fake GPS signals towards a drone. It is essentially "hijacking" and

redirecting the drone instead of allowing it to follow the intended directions. The drone can then be manipulated to crash or be flown to another destination, such as the attacker's location. This could open the door for employees of drone companies to be held responsible for the consequences of spoofed drone shipments. Since it is very difficult to prove the origin of the navigation signals, it would be challenging to determine who is at fault in this situation. It was not until 2014 that a successful spoofing attack was conducted against a drone by a researcher at the U.S. Department of Homeland Security facility.

Currently, few commercial drones use encryption methods that render them invulnerable to the presently known spoofing attacks, but they are all still 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 et al., 2016).

As mentioned earlier, 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 during that time, as indicated by Thompson (2015), "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" (para. 1). 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.

The advantages of drone delivery are enticing, but there are important questions to be addressed. 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, 2016). While President Obama was in Office, 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 surveillance, for example, could create (Thompson, 2015).

Surveillance can include both passive and active data collection. This collection of data may include the indiscriminate recording of people in a broad sweep that passively gathers information as it is on the way to deliver or return a product or service. For instance, a drone can use a camera sensor that will locate their customer's address, while simultaneously collecting other types of data in the area. The information obtained is certainly necessary for accurate deliveries, but the collection and storing of such data within the drone's path while searching for a specific address begs the question of the public's right to privacy. Though the delivery or return is to a specifically targeted address, the drone's surveillance may bring forth questions related to the issues of secrecy, autonomy, and anonymity of those in the surrounding area (Thompson, 2015).

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 (Arash, 2017). Between the public and private sector, that number is expected to quickly increase. With that much data coming in, the question remains "What are they doing with it once they've collected this info?" (Arash, 2017).

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, and what activities that they may be participating in. From a consumer's perspective, this may be unnerving.

3. RESEARCH METHODOLOGY

Data Collection

A 22-question online survey was developed to collect data on the public's perspective on home

and commercial drone deliveries and the related issues of legislation, privacy and security. A pilot study was conducted with thirteen respondents who best represented the typical general population. After receiving feedback from the pilot study, several changes were implemented to improve the clarity of the instrument. A link to the survey was posted on Facebook, LinkedIn, and emailed to other participants to include as wide a range as possible of individuals representing the general population in the United States. A total of 227 usable surveys were collected.

Of the 227 respondents, approximately 70% fell between the ages of 18-25 years old, with the overall age range falling from 18 to 83 years. Fifty-two percent of the respondents were male, with the remaining 48 percent being female. Within the housing segment, 56.83% of the respondents were urban dwellers and 43.18% were rural dwellers. Additionally, more than half of the respondents answered that they shop online approximately once per month. Most of the respondents did not own a drone, but approximately 11% intended to buy one in the future. Of the 227 respondents, over 25% of them have had personal information stolen at some point in their lives (see Table 1).

Table 1. Descriptive Statistics of Categorical Variables

| Variables | Description | Frequency | Percent |
|--------------------|-----------------------------|-----------|---------|
| Age | 18-25 | 159 | 70.05 |
| | 26-35 | 23 | 10.12 |
| | 36-45 | 7 | 3.08 |
| | 46 + | 38 | 16.72 |
| Gender | Male | 118 | 51.98 |
| | Female | 109 | 48.02 |
| Housing | Urban | 129 | 56.83 |
| | Rural | 98 | 43.17 |
| Online Shopping | 2-3 Times per Week | 18 | 7.93 |
| | Once per Week | 64 | 28.19 |
| | Once per Month | 124 | 54.63 |
| | Once per Year | 17 | 7.49 |
| | Do not shop online | 4 | 1.76 |
| Own a drone | Yes, I own a drone | 15 | 6.61 |
| | No, but I intend to buy one | 25 | 11.01 |
| | No, I do not own a drone | 187 | 82.38 |
| Information Stolen | Yes | 57 | 25.11 |
| | No | 170 | 74.89 |

Furthermore, the survey contained questions based on consumer perceptions and attitudes which were measured on a Likert scale anchored by 1 = Not at All and 5 = Extremely or 1 = Extremely Unlikely and 5 = Extremely Likely. The dependent variable, Intention to Use Drones, was measured on a scale of 1 = Extremely Unlikely and 5 = Extremely Likely (see Table 2). Like variables were then grouped and renamed according to their factor loadings. The loadings of exploratory factor analysis show that the items within each question highly loaded with their corresponding latent constructs showing sufficient discriminant validity. Prior to factor analysis the Kaiser-Meyer-Olkin Measure of Sampling Adequacy (KMO = .789) and Bartlett's Test of Sphericity (p = .000) were conducted. Items were maintained to make up three factors. The latent constructs are named, legislation, feelings, and skepticism. Indicator validity can be assumed if all indicator loadings are higher than the threshold of .70 (Chin, 2010). Items with loadings below .70 were discarded (see Table 2).

Analysis and Results

In this research, factor analysis and step-wise linear regression was conducted using IBM SPSS Version 24. After analyzing the data through visual representation in addition to skewness and kurtosis measures, the continuous variables appear to be normally distributed. In order to determine the degree of multicollinearity, variance inflation factors (VIF) are calculated. The VIFs indicate that there is no multicollinearity problem within this model, since they are all less than 10 (Chin, 2010).

The results of the stepwise regression analysis as shown below in Table 3, suggest that consumers are more likely, and not surprisingly so, to choose drone deliveries if they include cheaper shipping costs and faster deliveries. While the consumers' perspective of drone legislation, feelings of skepticism, and their frequency of online shopping also played a role, shipping cost and delivery speed again played a primary role in their decision.

Table 2. Descriptive Statistics and Factor Loadings of Continuous Variables

| Description | Construct | Loadings | Mean | Std Dev |
|--|--------------------|----------|------|---------|
| How would you feel if you saw a drone flying near your home? | Excited/Feelings | .832 | 2.69 | 1.21 |
| | Curious/Feelings | .832 | 3.74 | 1.19 |
| | Nervous/Skepticism | .781 | 2.69 | 1.27 |
| Identify your level of concern for the following statement: I am concerned that delivery drones will collect personal information for other purposes without my permission | Skepticism | .780 | 3.04 | 1.26 |
| Identify your level of concern for the following statement: I am concerned that too much of my personal information will be collected during drone deliveries. | Skepticism | .871 | 2.82 | 1.26 |
| Identify your level of concern for the following statement: I am concerned about my privacy during drone deliveries. | Skepticism | .853 | 2.90 | 1.33 |
| How likely are you to believe the following statement: I believe current legislations that protect personal | Legislation | .725 | 2.56 | 1.02 |

| Description | Construct | Loadings | Mean | Std Dev |
|--|-------------|----------|------|---------|
| privacy from drone delivery services are serious against unauthorized access? | | | | |
| How likely are you to believe the following statement: I believe current legislations that protect personal privacy from drone delivery services are enough to combat contemporary technologies? | Legislation | .882 | 2.33 | 1.04 |
| How likely are you to believe the following statement: I believe current legislations that protect personal privacy from drone delivery services are strong enough to protect my personal privacy? | Legislation | .792 | 2.38 | 1.10 |

Note: Likert Scale 1-5

Table 3. Regression Analysis Results

| Model | Unstd B | Std Err | Std | Model | Unstd B | Std. Err |
|----------------|---------|---------|-------|--------|---------|----------|
| (Constant) | 1.519 | .416 | | 3.647 | .000 | |
| Shipping Cost | .282 | .088 | 314 | 3.200 | .002 | 4.552 |
| Delivery Speed | .262 | .087 | 293 | 2.991 | .003 | 4.555 |
| Legislation | .249 | .072 | 167 | 3.436 | .001 | 1.113 |
| Skepticism | -.226 | .064 | -.187 | -3.531 | .001 | 1.328 |
| Frequency | -.187 | .075 | -.114 | -2.482 | .014 | 1.003 |

The final model eliminated six factors: Age, Gender, Housing, Owning a Drone, Having Information Stolen, and Feelings. Interestingly, these demographics seem to be irrelevant to consumers' perceptions of drone deliveries. Initially, it was assumed age would influence decisions, since older individuals are generally less trusting of technology (Vaportzis et al., 2017). Since the participants were almost perfectly split between genders, it would have been easy to see if one gender had a preference over the other. It was also surmised that if a consumer owned a drone and was familiar with how they operate, they would automatically be more open to drone deliveries. However, these initial assumptions were not supported.

Additionally, the results indicated that consumers are more than likely not well-versed in current legislation concerning drone usage. Therefore, their decisions about the use of drones would not necessarily be based upon what is or what is not legal. Even if an individual orders online packages every day, there is not enough evidence to demonstrate a significant impact upon their decision to choose drone deliveries based upon their privacy and security concerns. All factors are outweighed by the consumer's desire for faster and cheaper deliveries.

4. CONCLUSION

Our study indicates that consumers do indeed value cheap and fast delivery, regardless of age, gender, or even concerns about privacy and security. Given consumer demand as well as positive impacts in the supply chain, it is expected that drone deliveries will increase.

The final question of the survey allowed participants to fill in what they would like to see implemented as it relates to drone delivery. Of the 122 that chose to respond to this question, many of them suggested new laws surrounding data collection, noise pollution controls, and delivery insurance measures. Others suggested that they would prefer drones not be used for delivery at all.

While we have much yet to learn, the COVID-19 pandemic of 2020 has further emphasized the importance of alternative delivery methods. We have witnessed the need for deliveries of items like prescriptions, food, educational supplies, etc., as individuals are working, studying, and even quarantined in their homes. While our study showed that fast and cheap delivery is important to the consumer, we need to keep in

mind that this is a nascent phenomenon. We understand little as of yet about the true impact of drone deliveries on a mass scale and further and additional research is needed.

5. 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-cancel-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).
- Bamburly, D. (2015). Drones: Designed for product delivery. Wiley Online Library. Retrieved from <http://onlinelibrary.wiley.com/doi/10.1111/drev.10313/pdf>.
- Behavioral Targeting (2017). Retrieved from <https://www.bluefountainmedia.com/glossary/behavioraltargeting/>.
- Chin, W.W. (2010). How to Write Up and Report PLS Analyses. *Handbook of Partial Least Squares*, Springer, Berlin Heidelberg, pp. 655-690.
- Collins, J. (2016). Drones: Is drone delivery simply pie in the sky? Retrieved from <https://www.journalofaccountancy.com/issues/2016/dec/drone-delivery.html>.
- Crandall, R.E., Crandall, W. R., & Chen, C.C. (2015). *Principles of Supply Chain Management*. CRC Press, Boca Raton.
- Diaz, J. (2020). U.S. Announces New Rules for Drones and their Operators. Retried from <https://www.npr.org/2020/12/29/951010863/u-s-announces-new-rules-for-drones-and-their-operators>.
- DHL Completes Three-Month Test of Delivery Drone (2016). Retrieved from

- <http://www.ttnews.com/articles/dhl-completes-three-month-test-delivery-drone>.
- Donahoe, S. (2016). Amazon and Drone Delivery: The Pros and Cons. Retrieved from <http://imsuccesscenter.com/amazon-and-drone-delivery-the-pros-and-cons/>.
- 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/>.
- UPS Flight Forward Attains FAA's First Full Approval For Drone Airline. Retrieved from <https://pressroom.ups.com/pressroom/ContentDetailsViewer.page?ConceptType=PressReleases&id=1569933965476-404>.
- Flirtey Continues to Lead Drone Delivery Industry (2017, July). PR Newswire. Retrieved from <http://link.galegroup.com/apps/doc/A499279501/BIC1?u=boon41269&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.
- Hassanalain, 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>.
- Kang, Hyun. (2013, May). The prevention and handling of the missing data. Korean Journal of Anesthesiology. www.ncbi.nlm.nih.gov/pmc/articles/PMC3668100/
- 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>.
- Kuntze, C., Martin, A., Regnier, C., & Silva, I. (2018). Deliver on time or pay the fine: Speed and precision as the new supply-chain drivers. Retrieved from <https://www.mckinsey.com/business-functions/operations/our-insights/deliver-on-time-or-pay-the-fine-speed-and-precision-as-the-new-supply-chain-drivers#>.
- Jones, P. (2019, April). Alphabet's Wing drones get FAA approval to make deliveries in the U.S. Retrieved from www.theverge.com/2019/4/23/18512658/google-alphabet-wing-drone-delivery-service-faa-approval-commercial-deliveries.
- Laguna, J., & Marklund, M. (2005). Business Process Modeling, Simulation, and Design. Prentice Hall, New Jersey.
- 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), 243-261.
- Murray, C. C., & Chu, A. G. (2015). The flying sidekick traveling salesman problem: Optimization of drone assisted parcel delivery. Transportation Research Part C: Emerging Technologies, 54, 86-109.
- Palmer, Annie. (2020). Amazon wins FAA approval for Prime Air drone delivery fleet. Retrieved from <https://www.cnbc.com/2020/08/31/amazon-prime-now-drone-delivery-fleet-gets-faa-approval.html>.
- Part 107 Waivers. (2019). Retrieved from https://www.faa.gov/uas/commercial_operators/part_107_waivers/.
- Pogue, David. (2016). Amazon reveals details about its crazy drone delivery program. Yahoo Tech. Retrieved from

- <https://www.yahoo.com/tech/exclusive-amazon-reveals-detailsabout-1343951725436982.html>.
- 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=JnNpdGU9ZWwhvc3QtbGl2ZQ%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>.
- Rupprecht, J. (2018, January 29). Drone Delivery – 3 Big Legal Problems (2018) -. Retrieved <https://jrupprechtlaw.com/amazon-drone-delivery-3-major-legal-problems-amazon-prime-air>.
- 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/br-ieffhistory-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>.
- Unmanned Aircraft Systems. (2012). Retrieved from FAA Seal. Retrieved from www.faa.gov/uas/.
- U. S. Const. art. IV.
- U.S. Department of Transportation. Retrieved from <https://www.transportation.gov/connections/unmanned-aircraft-systems-integration-pilot-program-selectees-0> on June f28.
- Vaportzis, E., Clausen, M. G., & Gow, A. J. (Oct. 7, 2017). Older Adults Perceptions of Technology and Barriers to Interacting with Tablet Computers: A Focus Group Study. <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5649151/>.
- Villasenor, J. (2013). Observations from Above: Unmanned Aircraft Systems and Privacy. Retrieved from <https://pdfs.semanticscholar.org/ec9a/8458e8fe4c2511c2e18f557eae8ddedb2289.pdf>.
- Vincent, J. (2020). Walmart begins testing drone deliveries for household goods and groceries. Retrieved from <https://www.theverge.com/2020/9/10/21430280/walmart-drone-delivery-pilot-program-north-carolina-flytrex>.