11-13-2018

The Unforeseen in Unmanned Vehicles

Paul Maxwell
Army Cyber Institute

Michael Nowatkowski
Army Cyber Institute

2018 IEEE International Symposium on Technology in Society (ISTAS) Proceedings
Miriam Cunningham and Paul Cunningham (Eds)
ISBN: 978-1-5386-9479-4

The Unforeseen in Unmanned Vehicles

Paul Maxwell
Army Cyber Institute
West Point, NY USA
Email: paul.maxwell@westpoint.edu

Michael Nowatkowski
Augusta University Cyber Institute
Augusta, GA USA
Email: mnowatkowski@augusta.edu

***Abstract* - The development of unmanned vehicle technology is rapidly proceeding and will result in numerous advances in autonomous vehicles. Most of the research effort to date focuses on the safe and effective operation of these vehicles that will allow them to integrate into society. A research gap exists though in the technical, policy, and legal fields regarding illicit use of these vehicles beyond their programmed functions. In this paper we explore possible misuse of unmanned vehicles and illustrate the need for research in the technical, policy, and legal realms.**

Keywords* - *Unmanned Vehicles, Cyber Security, Cyber Policy, Cyber Law

I. INTRODUCTION

Unmanned, autonomous vehicles of all types, e.g., air, ground, water, are rapidly advancing in capability. Plentiful research is ongoing to solve the challenges of safe operation for these systems in our complex environment. This research is necessary for the eventual inclusion of these systems into society. With that task now well underway, it is time to shift some research effort into other aspects of unmanned systems such as security and privacy. Before these systems begin mass production, it would be wise for society to develop rules and regulations protecting both public safety and privacy. As we have seen with other systems, it is more efficient to create designs from the ground up that provide these protections instead of attempting to patch them once fielded. Many in industry would argue to develop then regulate similar to how the automobile and aviation industries developed. However, this method often results in long periods of anguish for users as issues are slowly resolved. Failure to develop solutions to these issues now will eventually result in the use of unmanned vehicles (UVs) in ways that are harmful to society.

As new technology is developed, it often provides benefits to society. It enables people to be more productive, to work more safely, and to live healthier lives. Frequently though, this same technology is co-opted for battlefield or criminal use. Cell phones enable remote triggering of bombs or the illicit tracking of people [1]. Unmanned Aerial Vehicles (UAVs) are used to deliver explosives as documented in attacks by ISIS and the recent assassination attempt in Venezuela. Social media provides command and control networks and recruiting tools for Al Qaeda and ISIS terrorists. Internet of Things (IOT) devices facilitate massive Distributed Denial of Services Attacks [2]. GPS devices are used to stalk people [3]. Eventually unmanned vehicles will be utilized by criminals or terrorists for nefarious purposes as well.

Some of the illicit applications for unmanned vehicles may affect privacy and personal freedoms while others may pose a direct threat to public safety. Many questions arise from these possibilities such as how will stalking or harassment by unmanned vehicles be prevented? Will citizens be protected from constant surveillance that these technologies enable? How will law enforcement or the military stop an unmanned vehicle and how will it gain authorization to search it? How will the perpetrator of an illegal act using an unmanned vehicle be attributed? The answers to these questions and many similar ones are currently unknown. The purpose of this paper is to propose the start of the discussion on these topics including potential technical, legal, and policy solutions to these issues so that the solutions are emplaced prior to mass adoption of these technologies.

To initiate the discussion, the remainder of the paper is organized as follows. Section 2 discusses work related to unmanned vehicles and public safety/privacy. In section 3, we will use several scenarios to illustrate the gaps in current research work and the legal/policy domain. Finally, we will conclude the paper in Section 4.

II. RELATED WORK

The work of Schlag discusses the use of unmanned aerial vehicles by the government to conduct near constant surveillance of individuals [4]. The author proposes a consumer protection law that would designate authorized uses of unmanned aerial vehicles by the government and individuals. In his opinion, this law should help define the public's expectation of privacy from aerial surveillance by drones. This work is a step in the right direction but is focused on aerial vehicles only and on the protection of individual privacy from the government, not privacy protection writ large.

Work is being done by a group at IBM to develop the concept of a digital manifest for unmanned aerial vehicles [5].

The views of the author are his own and do not reflect the views of the United States Military Academy, the United States Army, or the United States Government.

This work proposes a technical solution to implement an unmanned aerial vehicle manifest for onboard goods. The manifest includes details about the origin and destination of the vehicle and a listing of contents that could be displayed on the vehicle or a remote terminal. The intent of this manifest though is to assist an organization with the logistical challenges of creating shipments, assigning transport, and then delivering the goods. The manifest is not intended for use by law enforcement.

The author of [6] imagines scenarios that may result in law enforcement stops of an autonomous ground vehicle. The scenarios include events such as passengers not wearing seat belts, a vehicle that is reported stolen, and broken equipment. These scenarios are the beginning of a more thorough investigation into how unmanned systems may be used by malevolent actors but it does not include scenarios such as terrorist use of a vehicle. Furthermore, as highlighted in the article, the authorities of law enforcement personnel to search the vehicle are not fully defined and require the development of policy and legal solutions.

In the article by Sullivan [7], the actions by states such as California are highlighted. California is proposing laws that require autonomous vehicles to have "law enforcement interaction plans." Developers of these systems would be required to assist law enforcement by identifying vehicle ownership and insurance. The open legal question is can a manufacturer be forced to provide this information on a privately owned vehicle? Again, these draft laws demonstrate some initial thought on how autonomous vehicles operate in a complex society, but they are not inclusive of all vehicle types nor do they examine the most dangerous scenarios.

Kaminiski illustrates how many states are considering privacy rules with respect to unmanned aerial vehicles [8]. The range of state draft regulations on privacy in this area range from treatment of surveillance in public areas as free speech to more conservative approaches that require a subject's consent under various circumstances. A main point is that there is no federal standard and only UAVs are considered in these regulations. Additionally, most of these laws deal with government surveillance drones and do not concern themselves with citizen owned systems.

The MCity project attempts to foresee challenges with regard to autonomous automobiles [9]. One of the products they have released is a threat assessment tool to assist in determining how vulnerable autonomous vehicles are to cyber-attacks. Though the authors hypothesize about various scenarios driverless vehicles could encounter, they only propose possible technical solutions. Their work lacks non-technical issue identification and only considers automobiles.

III. Identifying Technical, Legal, and Policy Gaps

It is clear that researchers are thinking about some of the potential issues that unmanned vehicles will unearth. However, most of the work deals with unmanned aerial vehicles and how unmanned systems interact with the government. Given that drones are now proliferate, this seems reasonable. We propose that now is the time to begin research and have discussions on all unmanned autonomous systems and to extend that discussion beyond the government/public interface. To assist in starting this discussion, we present the following scenarios grouped into three main categories of potential UV exploitation: the Normal UV, the Hacked UV, and the Intrusive UV.

A. The Normal UV

The first category is UVs that are co-opted during the completion of their normal tasks. The vehicle's programmed behavior and design attributes are used to commit criminal, terrorist, or other illegal acts. This is illustrated in The Bomb and The Criminal where well-behaved, normally operating systems facilitate crime or acts of terrorism.

1) The Bomb

One evening, a food delivery robot makes a delivery to a new customer. The robot makes its way through various neighborhoods without difficulty passing several important government facilities and even a few law enforcement personnel. The now common presence of these robots and its good behavior presents no cause for intervention in its operation. At its destination, the food is accepted and payment is made as normal. During the robot's return trip, it suddenly explodes outside of a local government office. Investigators later conclude that the new customer deposited the explosive inside the robot knowing that its return path would take it by the desired target. Using a gps device to trigger the bomb and the robot's deterministically determined return path, the goal of the terrorist was achieved.

Unmanned, autonomous delivery systems are currently developed and in some cases in use [10]–[13]. The research behind these systems includes the technical challenges of navigation, collision avoidance, and the exchange of goods. Items such as how users gain access to system compartments have various solutions [10], [12], [14]. The challenges facing autonomous systems are being solved and once conquered, laws and regulations will most likely evolve to allow their use in public. Before this happens, we need to explore the scenarios for misuse to help design prevention mechanisms.

In this type of scenario, the unmanned system could have many forms such as a taxi, a delivery vehicle, or a service vehicle (e.g., a trash truck). The system in question could be used passively like the delivery vehicle in the scenario. The threat actors merely utilize the access granted to them and publicly available knowledge of its operations to achieve their goal. Alternatively, the system could be partly or completely modified by the threat actor. In this situation, perhaps the controller software is hacked to give control to the actor or the system's sensors are modified or spoofed to provide the controlling system false sensor data.

Some of the research issues that arise from this scenario include how to interrogate an unmanned system remotely to determine its contents and mission. If the system is suspicious or deemed a threat, how is the system disabled or stopped? How is a criminal act attributed to the threat actor? The issues are multi-faceted and include technical, legal, and policy components. There is no single, easy solution.

Some technical solutions that assist in documenting system contents and mission are found in the ideas in [5], [15], [16]. In the first solution, the legal marijuana industry is developing digital manifests for law enforcement and auditing purposes. The second solution is a proposed idea to create digital manifests that will help companies' logistical systems match cargo to delivery systems. The last solution is an e-manifest proposed by the EPA for hazardous waste cargos. This system could allow for a check on potentially dangerous vehicles and their routes. None of these solutions are sufficient to deal with our scenario though. Manifests are not currently a requirement for any unmanned systems and even those in the manned systems world are usually only subject to inspection under

certain circumstances. Clearly more research work is needed to develop solutions for these questions.

2) The Criminal

An autonomous taxi drives to a requested passenger pick-up site. Upon arrival, it opens its doors to allow the passenger to enter. Instead of a passenger boarding, a package is placed into the vehicle. The vehicle then departs for its requested destination. At that location, the doors open and the package is removed by an unidentified individual. Unknown to the proprietor of the taxi, the vehicle has just facilitated the transportation of illegal substances. The account of the requesting rider is spoofed and the identities of the highly concealed originating and receiving agents is unknown.

In the present day, moving vehicles always have at least one passenger - the operator. As such, law enforcement has the ability to stop a vehicle, potentially search it, and if appropriate hold the operator responsible for any violations of the law. In a world of fully autonomous vehicles, this may no longer be true. It is feasible that vehicles will not only be driverless, but also without passengers. A vehicle could be used solely as a delivery means for cargo. A UV could be sent to the dry cleaners to pick-up an individual's clothing and then return with the cargo. In this scenario, who is responsible if the cargo has illegal contents? Currently, many laws for vehicles are based upon a driver being in control, and often require a determination of intent [17]. How will this occur in a passenger-less vehicle?

One of the first challenges is to attribute ownership of the vehicle. This may be required to identify who is responsible for the illegal action or if a vehicle is authorized to be in a restricted location. A lot of effort is underway with regard to identification of UAVs [18]–[21]. These efforts rely on wireless transmitters and receivers that can interrogate drones to determine ownership. So far, this effort has not been extended to UGVs. Even with this technology, is it proper to hold the owner responsible for the illegal act? What technology needs to be emplaced to protect the owner from these scenarios? If the owner is not responsible, how are all interactions with the vehicle attributed in such a way that a credible chain of responsibility is maintained? One suggestion is that vehicle trips require "signatures" for programmed route/destination instructions thus providing a log as to who is responsible for the journey [17]. Without some form of identifying technology, do police have the right to demand vehicle data from the owner or manufacturer? Questions like these are why some states, such as California, are requiring law enforcement interaction plans when laws for autonomous vehicles are being developed [7].

Another issue is what authorities does law enforcement have to stop a suspicious vehicle? With a human driven vehicle, pre-textual stops based on driving behavior such as excessive speed, lane departure, or failure to signal provide an avenue. These human errors will largely disappear if the promised super-driving capabilities of autonomous vehicles is delivered [22]. Some pre-textual stops may still be valid though such as those based on broken equipment or expired registration [6]. Reasonable suspicion is often enough to stop a vehicle [23] as well. However, what now provides the basis for that suspicion? The route a vehicle takes may simply be a function of its navigation algorithm and may no longer indicate potential misdeeds. Observation of the driver or passengers when the vehicle is empty is no longer a basis for suspicion. Some basis for stops will certainly remain, but the frequency of such stops is sure to decrease [23].

If a vehicle is stopped, what authority does law enforcement have to search it? How can consent to search be obtained if no owner/operator is present (with or without passengers)? Currently the driver is usually the individual who can grant consent for a search. With the potential that there is no driver, how will laws change to grant search consent? Could the owner of the vehicle grant consent remotely? Could states create laws that designate implied consent for search of autonomous vehicles similar to searches that are done with breath, blood, and saliva samples for suspected intoxicated drivers? What will be considered probable cause for search without consent? The "reason for arrest" often provides law enforcement the mechanism to search for evidence [6]. Will the records of a vehicle's trips be searchable without warrant? Autonomous vehicles are likely to store this information locally or remotely so will that be considered "open information" [22]? These are just a few of the legal and regulatory issues that need to be examined prior to widespread UV deployment.

B. The Hacked UV

The second category that we examine is UVs used maliciously through hacking or other means of modification to alter their normal operation. This is described in the Bludgeon, the Plug, and the Kidnapper. These scenarios show what is possible if the hardware, software, or sensing capabilities of the UV are altered to allow the attacker to control or change the behavior of the UV. Once the attacker alters the UV, it can potentially participate in nefarious acts.

1) The Bludgeon

An autonomous ground vehicle drives up to a busy intersection and stops at the red light. As pedestrians enter the crosswalk in front of it, it suddenly accelerates into the crowd striking multiple persons. It then proceeds inexplicably to drive onto the nearby sidewalk striking more pedestrians until it finally crashes into a building. The forensics team concludes that the navigation system and key sensors have been modified thus overriding the system's normal safety protocols. It appears that talented hackers have gained access to the internals of the vehicle.

Any system that is operated through the use of computer code and electronics is potentially vulnerable to this type of scenario. As was seen with the Jeep hack of 2016 [24], vehicles are no exception to this problem. Altering the operations of autonomous vehicles from exploiting code to simply modifying the sensors (ex. painting the camera lens) to modifying the environment (ex. placing tape on portions of a Stop sign to fool visual recognition) can take various levels of effort and expertise. No matter the technique, a UV could be altered to respond in this increasingly popular terrorist act.

Presently, an operator is the main mechanism for preventing these types of occurrences. The operator is in a position to prevent or stop modification of the vehicle while they are present. When not present, they have the responsibility to check the vehicle's condition before operation. So, without the operator, how do we know the vehicle is not altered? How does the user/operator know that the state of all embedded software is unaltered prior to driving? What tools can be developed and emplaced that allow civilians and law enforcement to visually or digitally know the vehicle is operating within its designed specifications? What requirements should be placed on

manufacturers to develop prevention mechanisms? What liability should be attributed to the vehicle owner if it is operated while altered? Should government create geofences of areas and require vehicle manufacturers to enforce compliance with these no-travel zones? The answer to all of these questions deserve research and discussion before an enterprising terrorist compromises a UV.

2) The Plug

While driving South out of Washington, D.C. early one Friday evening, the traffic is worse than normal. Listening to the traffic report on the radio, drivers are told of several vehicles stopped in a row across all lanes of the road. No drivers are reported in the vehicles, and no drivers were seen exiting the parked cars. After the cars were removed from the road and forensic investigation completed, it was discovered that the vehicles were remotely piloted to the highway. Once the vehicles were lined up side-by-side, the attackers stopped the vehicles in the road, preventing traffic from moving.

Similar to hacking the vehicle in *The Bludgeon* scenario, several vehicles could cooperate to disrupt traffic. This could be a scenario where the vehicles drive slowly or are completely stopped. Consider a section of road with concrete barriers on one side, and a natural barrier on the other side (mountain, cliff, water, etc.). California State Route 1, a major highway along the Pacific Ocean, is an example of such a road. If an attacker were able to commandeer some unmanned vehicles, they would be able to prevent traffic flow in either direction. This could potentially be done with a single vehicle if parked across a two-lane road with no way to drive around the vehicle. The Golden Gate Bridge in San Francisco connects State Route 1 north and south of the bridge. Using six commandeered vehicles would allow the attacker to block all the lanes of the Golden Gate Bridge, effectively disrupting up to 112,000 vehicles per day (source: http://goldengatebridge.org/tolls_traffic/). New York City is another example where an attacker could seriously impact traffic patterns using a few cars to block one or more major bridges or tunnels into the city.

All states have traffic laws requiring vehicles driving slower than the normal speed to use the farthest right lane, and several states now have laws requiring vehicles to move from the far left, or passing, lane if a faster moving vehicle approaches [25]. The laws are based on section 11-304 of the Uniform Vehicle Code, a set of recommendations initially developed for national standards for states to use [26]. How will law enforcement officials engage with a vehicle violating traffic laws, such as speeding or driving too slowly? A Google self-driving car was pulled over for driving too slowly in 2015 [27], although no ticket was issued by the officer. [6] provides several examples where a UV might be pulled over, but what if the vehicle does not respond to the flashing lights of the police officer?

3) The Kidnapper

During a routine maintenance service for an unmanned aerial system (UAS), a new "feature" is added that allows an attacker to take control of the vehicle, in the same way that researchers took control of ground vehicles in a 2015 and 2017 story in Wired magazine [24], [28]. *During a routine trip to work, the vehicle turns off course, carrying the passenger to an isolated location. Communications on board the vehicle, including voice and live video, are used to send a ransom note to the victim's family.*

This scenario can be extended to ransom in other forms, such as preventing operation of the vehicle, putting the occupant in physical danger. Just as hospitals and home users are encountering ransomware in their networked systems, UVs can fall prey to this attack as well.

Several companies around the world are currently testing working prototypes for UAVs which will function as air taxis in cities, carrying passengers from roof top to roof top [29]–[33]. One author discusses six different companies with prototype unmanned aerial systems (UAS). Feist states "the technology is ready, but the legal systems and safety for passengers and people below have a long way to go yet." [30] He does not expect to see active air taxi systems in the United States before 2020; however, Dubai, in the United Arab Emirates, is pushing to have active systems before that, hoping to be the first city in the world with autonomous air taxis. Other experts consider a more reasonable timeframe for ground vehicles to be 2030 [34], while more recent predictions place the date as sometime in 2021 [35].

The technology to operate a UAS may be ready, but to maintain safety and control of a high density of vehicles is not. NASA is working on a system to handle a high density of UAS, partnering with Uber to collect data. The system is the UAS Traffic Management (UMT) network (https://utm.arc.nasa.gov/index.shtml). [31]

If autonomous vehicles, whether air, ground, or sea variant, can be compromised and remotely controlled by an attacker, what can technology, policy and law do to prevent or mitigate the damage? Can the occupant of the vehicle always have manual override of the vehicle? Or will some form of a "big red button" that puts the vehicle in a safe shutdown mode be mandated?

C. The Intrusive UV

Lastly, we examine UVs that are operated by their owner to perform legal, yet obtrusive and persistent surveillance of a target, potentially violating individual privacy norms. The Private Investigator and the Stalker are examples of this type of UV exploitation. The ability of UVs to operate in public spaces for extended durations may create an opportunity to infringe on individual privacy that are not easily achieved in the present day.

1) The Private Investigator

A private investigator is hired by a citizen to monitor the actions of a selected individual. The investigator has unmanned aerial and unmanned ground systems at her disposal. Unlike in years past when the investigator's surveillance was limited to their personal time investment, these new tools allow for constant surveillance of the target. Ground systems monitor the target's home and workplace positioning themselves legally in public spaces. Aerial vehicles monitor all of the target's travels. There is no escaping the unblinking eye of the unmanned vehicles and their cameras and microphones.

Issues with regard to unmanned vehicles, mostly aerial, have been well examined in the courts and this examination will continue for the near future [36]–[39]. These cases primarily deal with the issue of privacy with regard to the government and the Fourth Amendment. The issue of the

legality of private citizens conducting surveillance on other private citizens without their consent is not well explored.

When privacy is potentially violated by the government, the salient issues revolve around factors such as the duration of the surveillance, whether it is recorded, if the technology is commercially available, whether the area of observation is in the curtilage of the home, and if magnification/augmentation is used. A popular framework used in some of these cases to determine the legality of the surveillance is the "Mosaic theory." This suggests that a single person's view of an individual's movements over a period of time is limited and therefore an expectation of movement privacy exists with regard to that person [40]. Our scenario would fail the Mosaic theory test. Clearly the targeted individual is under constant surveillance and has no privacy of movement. Despite this, the actions of the investigator would not be illegal because it's not the government conducting the surveillance.

The authors in [39] maintain that even if the government is involved, the concept of "open fields", public areas and private property that "do not provide the setting for those intimate activities that the Fourth Amendment is intended to shelter from government interference or surveillance", allow legal surveillance. The private investigator in this scenario will often be conducting their work in these open fields. Additionally, in the case of *US v Vela*, it was ruled that using night vision goggles to see into a vehicle on a public road was allowable thus reinforcing the idea that surveillance in public was o.k. even for the government [41]. Certainly if the government is allowed to surveil individuals in public spaces, then private citizens must be able to do it too. The question remains though, is this something that we wish to condone? Should the Mosaic theory apply to civilian surveillance? Can citizens seek relief from the unwanted surveillance?

Some government agencies are providing a possible path in this area. The United Kingdom's Regulation of Investigatory Powers Act (RIPA) 2000 requires permission for a UAS to record surveillance of a residential premise or private vehicle and that surveillance system operations must notify individuals of its operation so that copies can be requested if desired [42]. Indiana state law makes it a misdemeanor for anyone to place a data recording device on another's property without consent (no mention of public spaces) [43]. States such as Texas and Missouri have considered laws prohibiting video of an individual's property without their consent [8]. Clearly there is some concern for the privacy of individuals regardless of government involvement. As such, coherent policies and regulations need to be developed to cope with the surveillance powers that unmanned vehicles provide citizens.

2) The Stalker

An individual becomes interested in the activities of another person. He desires to not only monitor what that person does and when, but also to disrupt their life. He directs unmanned aerial vehicles to constantly fly nearby the target creating noise pollution and recording all visible activity, some of which is later posted on social media. Ground vehicles follow the target and occasionally impede the free movement of the person. Other ground vehicles position themselves outside the person's home and flood the wifi channel that the target's home router occupies thus limiting their ability to use the internet. Finally, unmanned vehicles direct lights and lasers into the windows of the target's home at night making it difficult to rest yet not violating any noise statutes.

This scenario shares some of the features of the private investigator. The individual using the unmanned vehicles is not a government official. The vehicles remain within public spaces and thus are not trespassing. Deliberate attention is paid to avoid violating local laws. The main difference here is the intent of the stalker.

Technology is advancing quickly that provides features enabling this scenario. A Google patent granted in 2015 [44] describes a UAV system equipped with Automatic Target Recognition and tracking. This technology could enable a UAV owner to autonomously identify and follow their prey without the interaction of a pilot. Additionally, the authors of [45] describe an autonomous patrol system that is capable of stalking ground-based personnel. Certainly the context of both these systems is initially military in nature but as we have seen, military technology frequently becomes civilian technology as time passes.

Given current and future technology, what protections should individuals have against unmanned vehicle stalking/harassment? The limitation of the stalker's time is no longer a limiting factor on the harassment. A stalker can be issued a restraining order but how would that apply to unmanned vehicles? Adding to the difficulty of developing policies and regulations to deal with this type of scenario is the fact that anti-stalking laws are mostly a local affair. Definitions of stalking vary, but terms such as willful, malicious, repeated, unwanted are used in many. Intent, actual harm done, and the perception of a "reasonable person" also factor into these laws [46]. Overall, the lack of federal laws regarding stalking create a challenging environment to regulate unmanned vehicle use in these cases.

Despite this difficulty, it is clear that some action is being taken. Cases in Arizona, Colorado, and Wisconsin have resulted in individuals being punished for using technology such as GPS trackers placed surreptitiously on vehicles to stalk others [3]. As unmanned technology becomes more readily available to the public, society needs to determine how it will cope with its capabilities in these unforeseen scenarios.

IV. Conclusions

While experts argue about the exact timeframe for autonomous systems to be commonplace, they do agree that these systems are an eventuality. Technology is making rapid progress, but our policies and laws have not kept pace. Will manufacturers be allowed to place these systems in to operation as soon as they are ready, or will the legal system prevent them from operating until policy makers can decide how to emplace safety measures and other controls in place? Legal and policy regulations regarding liability may prevent the implementation of unmanned vehicles [35].

Eventually, these systems will be commonplace in our society. To avoid misuse of these UVs, it is time to research and discuss solutions to potential problems such as those mentioned in this work. We cannot afford to "develop and then regulate" given the potential for harm. Scientists, policy makers, and legal experts must unite to focus on prevention.

References

[1] T. Ristenpart, N. Dell, K. Levy, and D. McCoy, "How domestic abusers use smartphones to spy on their partners," *Vox*, 21-May-2018. [Online]. Available: https://www.vox.com/the-big-idea/2018/5/21/17374434/intimate-partner-violence-spyware-domestic-abusers-apple-google. [Accessed: 24-May-2018].

[2] US-CERT, "Heightened DDoS Threat Posed by Mirai and Other Botnets," 30-Nov-2016. [Online]. Available: https://www.us-cert.gov/ncas/alerts/TA16-288A. [Accessed: 09-Dec-2016].

[3] J. Voelcker, “Stalked by satellite - an alarming rise in GPS-enabled harassment,” *IEEE Spectrum*, vol. 43, no. 7, pp. 15–16, Jul. 2006.

[4] C. Schlag, “The New Privacy Battle: How the Expanding Use of Drones Continues to Erode Our Concept of Privacy and Privacy Rights,” *Pitt. J. Tech. L. & Pol’y*, vol. 13, p. 24, 2013.

[5] G. Hoareau, J. J. Liebenberg, J. G. Musial, and T. R. Whitman, “Package transport container and transport operations for an unmanned aerial vehicle,” US20160207627A1, 21-Jul-2016.

[6] J. F. Weaver, “Robot, Do You Know Why I Stopped You?,” *Slate*, 27-Jun-2016.

[7] P. Bigelow, “On the Path to Autonomous Vehicles, Police Get Left Behind | News | Car and Driver,” 27-Apr-2017. [Online]. Available: https://www.caranddriver.com/news/on-the-path-to-autonomous-vehicles-police-officers-get-left-behind. [Accessed: 30-Mar-2018].

[8] M. E. Kaminski, “Drone Federalism: Civilian Drones and the Things They Carry,” Social Science Research Network, Rochester, NY, SSRN Scholarly Paper ID 2257080, Apr. 2013.

[9] A. Weimerskirch and D. Dominic, “Assessing Risk: Identifying and Analyzing Cybersecurity Threats to Automated Vehicles.” Mcity, Jan-2018.

[10] “Marble, How We Do It,” *Marble*. [Online]. Available: https://www.marble.io/. [Accessed: 30-Mar-2018].

[11] Panasonic Corporation, “Panasonic Autonomous Delivery Robots – HOSPI – Aid Hospital Operations at Changi General Hospital in Singapore,” 23-Jul-2015. [Online]. Available: https://www.businesswire.com/news/home/20150723005636/en/Panasonic-Autonomous-Delivery-Robots-%E2%80%93-HOSPI-%E2%80%93. [Accessed: 30-Mar-2018].

[12] “Starship.” [Online]. Available: https://www.starship.xyz/. [Accessed: 30-Mar-2018].

[13] “Why the wait for delivery drones may be longer than expected,” *The Economist*, vol. 423, no. 9044, pp. 10–13, 10-Jun-2017.

[14] “How it works — Dispatch.” [Online]. Available: http://dispatch.ai/how-it-works/. [Accessed: 30-Mar-2018].

[15] O. US EPA, “Learn About the Hazardous Waste Electronic Manifest System (e-Manifest),” *US EPA*, 05-Mar-2016. [Online]. Available: https://www.epa.gov/e-manifest/learn-about-hazardous-waste-electronic-manifest-system-e-manifest. [Accessed: 30-Mar-2018].

[16] “Metrc | The System,” *Metrc, The System*. [Online]. Available: https://www.metrc.com/the-system. [Accessed: 11-Jun-2018].

[17] F. Douma and S. A. Palodichuk, “Criminal Liability Issues Created by Autonomous Vehicles,” *Santa Clara Law Review*, vol. 52, no. 4, p. 1157, Dec. 2012.

[18] M. McFarland, “White House pilot program to allow more drone tests - Oct. 25, 2017,” 25-Oct-2017. [Online]. Available: http://money.cnn.com/2017/10/25/technology/business/drones-trump-local/index.html. [Accessed: 30-Mar-2018].

[19] DJI, “‘What’s In a Name?’A Call for a Balanced Remote Identification Approach,” *Dropbox*, 22-Mar-2017. [Online]. Available: https://www.dropbox.com/s/v4lkyr2kdp8ukvx/DJI%20Remote%20Identification%20Whitepaper%203-22-17.pdf?dl=0. [Accessed: 30-Mar-2018].

[20] C. Ramsey, “AIR6388 (WIP) Remote Identification and Interrogation of Unmanned Aerial Systems - SAE International.” [Online]. Available: https://www.sae.org/standards/content/air6388/. [Accessed: 30-Mar-2018].

[21] S. French, “Drone identification: What we know about the FAA ARC plans so far,” *The Drone Girl*, 30-Jun-2017. [Online]. Available: http://thedronegirl.com/2017/06/30/drone-identification-faa-arc/. [Accessed: 30-Mar-2018].

[22] O. Kerr, “Opinion | How self-driving cars could determine the future of policing,” *Washington Post*, 16-Jun-2017.

[23] R. Roseman, “When Autonomous Vehicles Take over the Road: Rethinking the Expansion of the Fourth Amendment in a Technology-Driven World – Richmond Journal of Law and Technology.” [Online]. Available: http://jolt.richmond.edu/2014/01/06/when-autonomous-vehicles-take-over-the-road-rethinking-the-expansion-of-the-fourth-amendment-in-a-technology-driven-world/. [Accessed: 25-Apr-2018].

[24] A. Greenberg, “A Deep Flaw in Your Car Lets Hackers Shut Down Safety Features | WIRED,” 16-Aug-2017. [Online]. Available: https://www.wired.com/story/car-hack-shut-down-safety-features/. [Accessed: 23-Apr-2018].

[25] A. Essex, D. Shinkle, and A. Teigen, “Transportation Review | Speeding and Speed Limits,” 16-Feb-2017. [Online]. Available: http://www.ncsl.org/research/transportation/transportation-review-speed-limits.aspx#Keep%20right. [Accessed: 21-May-2018].

[26] “Uniform Vehicle Code,” *National Committee on Uniform Traffic Control Devices*. [Online]. Available: http://www.ncutcd.org/Pages/default.aspx. [Accessed: 21-May-2018].

[27] D. Melvin, “Cop pulls over Google self-driving car, finds no driver to ticket,” *CNN*, 13-Nov-2015. [Online]. Available: https://www.cnn.com/2015/11/13/us/google-self-driving-car-pulled-over/index.html. [Accessed: 28-May-2018].

[28] A. Greenberg, “Hackers Remotely Kill a Jeep on the Highway—With Me in It,” *WIRED*, 21-Jul-2015. [Online]. Available: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/. [Accessed: 23-Apr-2018].

[29] M. Moon, “Dubai tests a passenger drone for its flying taxi service,” *Engadget*, 26-Sep-2017. [Online]. Available: https://www.engadget.com/2017/09/26/dubai-volocopter-passenger-drone-test/. [Accessed: 07-May-2018].

[30] J. Feist, “Drone taxi service - passenger drones - DroneRush,” 13-Apr-2018. [Online]. Available: https://www.dronerush.com/drone-taxi-passenger-drones-10666/. [Accessed: 30-May-2018].

[31] L. Greenemeier, “Here’s What’s Needed for Self-Flying Taxis and Delivery Drones to Really Take Off,” *Scientific American*, 15-May-2018. [Online]. Available: https://www.scientificamerican.com/article/heres-whats-needed-for-self-flying-taxis-and-delivery-drones-to-really-take-off/. [Accessed: 13-Jun-2018].

[32] M. Margaritoff, “Watch the Ehang 184 Passenger Drone Successful Taxi Someone Around,” *The Drive*, 05-Feb-2018. [Online]. Available: http://www.thedrive.com/aerial/18261/watch-the-ehang-184-passenger-drone-successfully-taxi-someone-around. [Accessed: 30-May-2018].

[33] A. J. Hawkins, “Airbus’ autonomous ‘air taxi’ Vahana completes its first test flight,” *The Verge*, 01-Feb-2018. [Online]. Available: https://www.theverge.com/2018/2/1/16961688/airbus-vahana-evtol-first-test-flight. [Accessed: 11-Jun-2018].

[34] S. Underwood, “Automated, Connected, and Electric Vehicle Systems,” p. 154, Dec. 2014.

[35] J. Walker, “The Self-Driving Car Timeline - Predictions from the Top 11 Global Automakers,” *TechEmergence*, 29-May-2017. [Online]. Available: https://www.techemergence.com/self-driving-car-timeline-themselves-top-11-automakers/. [Accessed: 13-Jun-2018].

[36] A. Cavoukian, *Privacy and drones: Unmanned aerial vehicles*. Information and Privacy Commissioner of Ontario, Canada Ontario, Canada, 2012.

[37] Marc Jonathan Blitz, “The Fourth Amendment Future of Public Surveillance: Remote Recording and Other Searches in Public Space,” *Am. U. L. Rev.*, vol. 63, no. 1, 2013.

[38] T. Dunlap, “We’ve Got Our Eyes on You: When Surveillance by Unmanned Aircraft Systems Constitutes a Fourth Amendment Search,” *S. Tex. L. Rev.*, vol. 51, pp. 173–204, 2009.

[39] J. J. Vacek, “Big Brother Will Soon Be Watching—or Will He? Constitutional, Regulatory, and Operational Issues Surrounding the Use of Unmanned Aerial Vehicles in Law Enforcement,” *N.D. L. Rev.*, vol. 85, p. 20, 2009.

[40] A. B. Talai, “Drones and Jones: The Fourth Amendment and Police Discretion in the Digital Age,” *Cal. L. Rev.*, vol. 102, p. 729, 2014.

[41] B. Stubbs, “Technological Ubiquity and the Evolution of Fourth Amendment Rights,” *Drake L. Rev.*, vol. 62, pp. 575–598, 2014.

[42] R. L. Finn and D. Wright, “Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications,” *Computer Law & Security Review*, vol. 28, no. 2, pp. 184–194, Apr. 2012.

[43] A. Bohm, “Status of 2014 Domestic Drone Legislation in the States,” *American Civil Liberties Union*, 30-Jun-2014. [Online]. Available: https://www.aclu.org/blog/status-2014-domestic-drone-legislation-states. [Accessed: 30-Mar-2018].

[44] K. Kokkeby, R. Lutter, M. Munoz, F. Cathey, D. Hilliard, and T. Olson, “Methods for autonomous tracking and surveillance,” 12-Dec-2008.

[45] J. Oyekan and H. Hu, *Towards Autonomous Patrol Behaviours for UAVs*. .

[46] E. Petch, “Anti-stalking laws and the Protection from Harassment Act 1997,” *The Journal of Forensic Psychiatry*, vol. 13, no. 1, pp. 19–34, Jan. 2002.