See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/298427201

# The societal impact of commercial drones

DOI: 10.1016/j.techsoc.2016.02.009							
CITATIONS 24			READS 500				
3 authors, including:							
Ashwin Goutham Gopi New York University 6 PUBLICATIONS 25 CITATIONS  SEE PROFILE							

Some of the authors of this publication are also working on these related projects:

Project Industrial Symbiosis View project

# **The Societal Impact of Commercial Drones**

Bharat Rao NYU Tandon School of Engineering Brooklyn, New York

Ashwin Gopi NYU Tandon School of Engineering Brooklyn, New York

Romana Maione NYU Tandon School of Engineering Brooklyn, New York

#### **Abstract**

The use of drones or Unmanned Aerial Vehicles (UAVs) in commercial applications has the potential to dramatically alter several industries, and, in the process, change our attitudes and behaviors regarding their impact on our daily lives. The emergence of drones challenges traditional notions of safety, security, privacy, ownership, liability, and regulation. With their ability to collect data and transport loads, drones are re-shaping the way we think and feel about our physical environment. However, they also burdened with the perception as being surveillance equipment, and their commercial use has been criticized by both individuals and activist organizations. In parallel, drones have been legitimized by regulations and licenses from federal agencies, are used by companies for surveying, inspecting, and imaging, and their technological development are driven by active communities of hobbyists and enthusiasts. This tension presents unique challenges to their integration in the currently existing public, governmental and private infrastructure. In this paper, we will take a look at a few of these issues to understand how drones influence society, and present recomendations for practitioners, policy makers, and reseachers studying this phenomenon.

## **Key Words:**

## 1. Introduction

The advent of new and emerging technologies undeniably has broad economic, social and personal impacts [1]. Most commonly, they influence practice, the way we do things, perform tasks, achieve goals, etc.; while creating new capabilities and possibilities for action [2]. Take the Internet for instance; it did not just allow us to share information faster and cheaper; it completely changed the way we conceive of and use information. Usually, these changes are not just related to the features of the technology, but also how we interpet their usability. Rather than the technology itself, it is our use of it that affects our perception, and thus our behavior [3]. In this paper, we consider how an emerging technology, viz. commercial unmanned aerial vehicles, more commonly known as drones, affects us by challenging some of our societal values and beliefs. In particular, we argue that the way this technology is currently used has an impact on our conception of safety and security, privacy and ownership, individual and commercial liability, and the effectiveness and process of governmental regulation. Drones are thus becoming increasingly important in the fields of science, technology, and society.

Traditionally, these discussions have been centered on their use in military surveillance and active combat. Since their emergence, the use of UAVs in combat zones has been heavily debated, and the conversation has been focused on their ethics, effectiveness, transparency and legality [4]. Despite multiple criticisms from human rights organizations, their judicial use has been upheld by many of the world's governments. The official stance of governments is that drones prevent casualities by providing accurate surveillance information and presicion strike capabilities, while their opponents emphasize their inability to discern between intended and unintended targets [5]. There has also been increasing discussion around the use of drones over domestic airspace for the purpose of surveillance in the interest of national and local security. The dialogue closely mirrors that of combat drones, as it is the same issues of ethics and privacy that shape the conversation [6]. This is particularly reflected in journals of law, ethics and technology policy as there been multiple articles that have described various issues regarding the use of drones over domestic skies [7].

In this paper, we focus on a related but slightly different phenomenon: the emergence of commercial drones. These drones are designed, built and used by individuals, businesses, and organizations. Though commercial drones owe much of their development to their military counterparts, most designs do not resemble the larger and more expensive surveillance drones [7]. Commercial drones typically are built on a small platform, use cheap and easily available components, and can lift only an average of 4 pounds [8]. They emerge primarily from the work of UAV and quadcopter enthusiasts, and their creations have historically not been the subject of scrutiny, usually due to their small numbers and lack of public interest.

Drones have the ability to carry multiple sensors, transmitters, and imaging equipment. As the use of drones continues to proliferate, they will impact industries ranging from entertainment to agriculture, from construction to delivery markets [4]. Their use in Hollywood film production has already been legitimized through the creation and use of specialized high-definition imaging drones. Civilian UAVs have the potential of becoming a dominant infrastructural platform. Not only are they cheap and easily available, they can be deployed across many industries to perform complex, expensive and dangerous tasks [9]. Currently, short battery life and the lack of proper regulation (and enforcement) remain the two major limitations for their rapid adoption.

Several organizational and industrial standards associations have been created, to either design drones and or to support their integration with existing infrastructure. They have developed new and unique market-focused applications and service platforms, and have thus influenced the social perception of this technology and its associated business models. Thus, this somewhat inevitable growth of drone-based businesses seem destined to transform consumer behavior as well as reshape our notions freedom and responsibility [10]. In the following sections, we will look at how this technology was developed, how it was adopted, and how it is used in individual and commercial applications. It will provide an overview of what drones are, how they have come to be, and how they are perceived and used today. We will then use discourse analysis to explore the impact that drones have had on various societal aspects, and provide recommendations for practitioners, policy makers, and researchers studying this new phenomenon.

## 2. Background

The definition of UAVs, commonly known as drones, is rather broad, and it is understandable considering the wide range of configurations that exist. In practice, any aerial vehicle that does not rely on an on-board human operator for flight, either autonomously or remotely operated, is considered a UAV [9]. UAVs range in size from large military drones with a wingspan of nearly 200 feet to commercially available inch-wide micro drones. Their ranges of flight vary, with some commercial drones being confined to a few feet away around the operator to advanced military drones that can fly for over 17,000 miles without having to land. Likewise, there is a huge variation in their maximum flight altitude, which can be anything from a few feet to a maximum of 65,000 feet [10].



Figure 1: Structure of a commercial drone

Most commercially available drones today follow a similar design (refer the figure 1). The basic design has a microcontroller that acts as a flight control, usually with four but up to eight motors and propellers, a radio receiver, electronic speed control, and a battery, built on a light plastic or metal frame [11]. In addition, gyroscopes and other sensors are added to increase the mid-air stability of the drone and a GPS device can be used for navigation. Most hobbyist drones also carry a camera for aerial imagery, and a gimbal for added image stability. Additionally, other sensors can be attached, though there is a trade off with increased functionality and weight [11]. DJI, 3DRobotics and Parrot are some of the leading hardware manufacturers, and their sales includes both assembled drones and drone components [10].

## 2.1 Development

The development of unmanned aerial vehicles (UAV) is primarily rooted in military research. Though it was initially conceived as a weaponized vehicle for the purpose of reducing the risk to human operators in hostile territory, the technology, capabilities, and use of UAVs have since evolved to include surveillance and the collection of data [11]. The shift from exclusively military drones to civilian application can be traced to the aftermath of Hurricane Katrina in 2005. In the broad rescue effort that followed, military drones equipped with accurate infrared cameras were widely recognized as a useful field asset. This led to the

Federal Aviation Administration (FAA) first issuing certificates to allow M7RQ series military drones to be used over civilian skies in 2006 [13]. Since then, drones have entered the mainstream market after years of development in the open source and maker communities. For example, 3DRobotics, one of the leading drones manufacturer, began in 2009 with ArduPilot, an open source autopilot platform based on the Arduino [14]. Likewise, DJI and Parrot have open source hardware and software projects where a community of enthusiasts is invited to join the development process. Though most of the development initially was in hardware, there has also been a major improvement in autopilot software that allows autonomous flight. An example is Openpilot, a project that aims to create universal autopilot software that can be used to fly civilian drones for humanitarian, academic, and hobbyist applications [15].

The development of drones draws a parallel to that of other emerging technologies, like 3D printers, for instance. By creating and providing access to development tools, drone manufacturers have invited the open source community to their design process. Since the open source projects consisted of geographically distributed communities, most of the designs were created digitally using modeling software. This made it easy to share, test, and modify the designs [16]. 3D printers also played an important role in this process as they allowed rapid prototyping and manufacture of drone components. In fact, the 3D files containing the design of certain parts are available online for anyone to download and print for free [17]. The drone manufacturers utilize the passion and expertise of the community to create technology that best serves their need. The availability of support, knowledge, and access to resources provided by the community has greatly helped in reducing the barrier of entry for new drone hobbyists and amateur developers [18].

In addition to manufacturers, drone-related services have emerged as a new business in this area. These services take many forms, the simplest being the provision of drone assembly, maintenance, and repair [19]. Rental services for drones have also popped up in many cities, and they allow individuals and companies access to drones on an hourly or daily basis. These rental drones are used for television and film production, real estate marketing, construction and inspection, architectural photography, and photography for events [18]. The third type of services use drones to perform surveillance and inspection on the behalf of their clients, and is common in the agricultural industry. These companies own a fleet of drones and are required to have an FAA license to fly in domestic air space [17]. The final category of services is drone brokers, and they do not own drones at all. Rather, they act as a marketplace to connect people who own and operate drones to clients who usually only require aerial photographs and survey data [20].

The global expenditure on commercial drones in 2014 stood at \$700 million, with DJI being the market leader, followed by Parrot and 3DRobotics [21]. It has been predicted that the market for drones is expected to increase to \$1 billion by 2018, and \$1.7 billion by 2015 [10]. In addition, a fast growing segment is the DIY market, where the sales are primarily in components [21]. The market size of drone related services are also predicted to match that of hardware sales within the next three years. The cost of these drones can range from a minimum of \$50 for micro drones and a standard DJI Phantom for \$699, to the high-end Intuitive Aerial Aerigon that costs up to \$250,000 and is used to shoot high-resolution videos for film production [10]. This wide price-range represents the diversity of capabilities in commercially available drones, and in the following segment, we will take a look at the most common applications.

# 2.2 Commercial Applications

In the commercial space, drones are viewed as platforms for sensors of any kind, and they have been used primarily for surveillance and inspection [4]. Today, drones are being used to survey crops, in search and rescue operations, to count wild life and keep track of animal population, in land surveying, to survey forest fires, and to inspect oil pipelines, power lines and other remote infrastructure [6]. Their ability to carry heavy equipment has been leveraged for spraying crops in large farms and delivering food, medical supplies and drugs to inaccessible locations [9].

The most common application for consumer and hobbyist drones is aerial photography. Consumer drones are currently available with in-built cameras or modular arrangements allowing the installation of lightweight devices [4]. Under current FAA regulations, they also can fly only up to 400 ft. and typically require to be controlled in real time by a human pilot during take off and landing, as well as monitoring unexpected obstacles [9]. However, even with these restrictions, they offer an astonishingly wide range of application, offering solutions to different segments of the market. Though the regulation specifies that drones in domestic airspace can only be flown within line of sight, remote flying is currently possible by using on-board cameras to stream live video and sensor feedback to smartphones, laptops, or in-built screens on controllers [6].

Drone manufacturers, service providers, and platform integrators are seriously considering the business potential across these application types. The representation of drones in popular media has diversified from military drones to consumer ones, and this reflects the growing demand in the market [6]. These would change the industry landscape in terms of safety, speed and consequently costs. For example, drones are currently disrupting the use of helicopters by performing similar functions without endangering the people flying in it while costing around a tenth of the price [22]. The application of drones in large factories to transport payloads is being explored. In addition, thanks to the proximity at which the UAV can operate, and its limited noise compared to a real aircraft, it can be deployed for stealthier operations, such as detecting wildlife.

Many industries including law enforcement, movie and news production, and construction are using drones instead of manned aircraft for their operations. Finally, there have been efforts to develop a delivery drone able to transport loads up to 5 pounds are widely known. During the last twenty years, the spread of the Internet as a commerce platform has allowed firms to gain more visibility, reduce costs and the distribution footprint, and thus effectively leave the brick and mortar environment [9]. However, the logistics and distribution infrastructure is still dependent on ground and air transportation. Drones enable a new form of transportation and delivery and thus can completely change the ground rules: Amazon Prime Air, DHL and Google are pioneers in exploring the new type of delivery mechanism. Amazon has declared that once the service will be fully deployed they will be able to deliver more than 80% of their goods through air [23].

Thus, we see that the design, development and use of commercial drones have been shaped by science, technology, politics, social movements, and commerce. The argument can be made that in turn, drones too have had an effect on these aspects of society. The processes behind these changes have been widely explored in the field of science, technology, and society, and we now turn the lens to this particular emerging technology. In order to do so, we performed a study where we conducted an analysis of the debate surrounding the

development and use of drones. In the subsequent sections, we present the methodology and findings of our study, followed by recommendations for practioners in this field and researchers studying this phenomenon.

# 3. Methodology

Understanding a subject as extensive as the relationship between technology and society requires a suitably broad approach. Thus, we performed a discourse analysis of various documents in order to investigate how various stakeholders perceived commercial UAVs. Discourse is a comprehensive concept that includes any practice by which individuals imbue reality with meaning [24]. Though it is found in a wide range of forms (e.g. rituals, myths, customs), we are interested in verbal discourse in textual form. Particularly, we looked at spontaneous discourse, which subjects generate in their everyday lives. These take the form of articles, blogs, books, public records, announcements, reports, or indeed any text produced by an individual or organization [25]. Since individual and group action is largely guided by socially produced and shared patterns, the knowledge of this inter subjectivity helps us understand the social order [26].

In the field of commercial drones, we considered various stakeholders such as governmental regulatory organizations, judicial bodies, research institutes, public policy organizations, drone manufacturers, technology developers, service providers, news organizations, insurance companies, non profits acting in public interest, activists for privacy, activists for and against drones, public and private establishment drone users, and individual users. We used an aggregate corpus of ninety-six articles published between 2001 and 2015, accessed through academic and non-academic databases and search-engines. We considered the text produced by these stakeholders as the object, and used content analysis to make inferences. The text was then divided and coded based on the origin, purpose, and content. Finally, the inferences were classified into three schemes that represented the facets of society, and one that represented the governmental response. We present the findings in the following sections. Though it is not meant to be an exhaustive list of all of Au's effects on contemporary society, it provides a comprehensive overview of the observable social constructs that have been influenced by commercial drones.

# 4. Societal Impact of Commercial Drones

Based on our analysis of the discourse surrounding drones, we identify three broad classes of issues that need further attention. The first one is safety and security, and it relates to personal and property damage, as well as attacks on the drones themselves. The next is privacy and ownership, and this is in regards to the data collected by the drones. Third is personal and commercial liability, which evokes questions about the responsibility undertaken by drone operators. In the following sections, we will briefly examine each of these issues in more detail and delineate the broad concerns, as well as potential ways of addressing them. Finally, we will take a look at the attempts by governments to regulate this industry, and the challenges they have faced.

## 4.1 Safety and Security

Safety, the freedom from harm, and security, the freedom from fear of harm, are basic human rights that are guaranteed and protected by the constitutions of most nations. Currently, the use of drones in civilian airspace has triggered concerns about the challenges to these basic

rights. These concerns are directed towards both the technology and the user. Concerns regarding the technology center around the battery life, lift capacity, airworthiness, and reliability of the drones. The primary criticism with the flying of commercial drones over public space is that small mistakes could result in crashes that threaten the health, well-being and property of the public. Furthermore, if they crash into public infrastructure such as electricity poles, or wanders into airports and other protected airspaces, they could result in dangerous scenarios that put lives in danger.

These fears are not unfounded as there have been cases of such incidents that have been reported. Currently, there are a few issues that challenge the security of drones in flight. Drone navigation units are vulnerable to two different kinds of attacks on their GPS 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 the attacker's location. This would make it possible for a drone operator 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 a Department of Homeland Security facility. This controlled but sophisticated attack was achieved with \$1000 worth of equipment. For now, military GPS uses encryption that renders it invulnerable to any known spoofing attack, but still leaves it 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. There have been several incidents that have caused substantial losses without the owners of the devices being found [27].

Aside from attacks on the navigation of the drone itself, there is the security of the payload being carried: for example, one can imagine several logistical challenges faced by drone delivery services that are being envisioned (e.g. by Amazon). Likewise, the intentions of drone operators have been called into question, as currently, there is not regulation that controls the payload that is carried on the drones. Critics have speculated that drones could theoretically be used to conduct attacks on a civilian population, though no cases have been reported thus far. In fact, currently available commercial drones lack the lift capacity to carry any equipment capable of creating damage, yet it is important to note that their lift capacities have been improving over the last decade.

## 4.2 Privacy and Ownership

Outside of the military and commercial environment, the information carried by cameras and sensors on drones operating in the consumer space may be even more valuable to attackers and easier to target. If a private UAV is compromised, it is difficult for the owner to detect the leak of information, and ensure the security of the information as well as claims on ownership. These attacks aren't hypothetical, either: an investigation prompted by a handful of documented cases of militants in Iraq who apparently captured videos on their laptops revealed that a piece of \$26 off-the-shelf software was capable of intercepting feeds from US military drones [28] [29]. Currently, even the military isn't capable of securing its videos such attacks, and therefore foolproof security is not yet expected of police forces, private firms, or consumers using drones.

This problem only gets more complicated as device endurance improves and their costs decrease, giving the opportunity to any individual engaging in episodic or persistent surveillance at the expenses of others' "reasonable expectation of privacy". As a matter of fact, the traditional notion of privacy itself is under threat: "the state in which one is not observed or disturbed by other people" will have to be defended not only from obvious and detectable threats such as people nearby or objects on the ground, but also from quiet and distant flying objects as well. This also raises the issue of airspace over private property and standards and expectations for its protection. In a public space such as a park or on a street, the reasonable expectation of privacy does not apply. Therefore, since a person is present in a public place, there is also not legal basis to make a claim of a breach of their privacy.

The same argument also extends up to an extent, to private property that is visible from public spaces. However, these laws assume that sight is confined to the eye-level. Drones disrupt the expectations of reasonable privacy since they are operated in a public place, yet can capture images and sound from that aren't traditionally available to the public. This gap in the law allows for the possibility of unwarranted surveillance without fear of repercussion. Current privacy laws stat that it is illegal to record the interior of a home or a privately owned building, even if the camera is placed outside. This creates uncertainty since even if the drone is being flown within eyesight and over the private property of the operator, there is the possibility of being in violation of privacy laws since it provides a monitoring capability that is not yet legitimated by the law.

# 4.3 Personal and Commercial Liability

Drones now face complex coverage and liability issues in regards to insuring their commercial use. These problems arise from the complexity of various factors such as the different types of accidents, procedures for air control, and uncertain privacy laws. Insurance companies are yet to develop insurance plans for UAVs, and there is very little guidelines or precedent to follow. Personal injury and the invasion of privacy are the most important issues, considering that many UAVs fly over habited regions. In order to judge a case of personal injury, insurance companies need access to a vast amount of information. They need the location of take off and landing, flight path, intent of flight, altitude, etc. Likewise, for breach of privacy, the insurance companies need to take into consideration the drone's ability to collect a massive quantity of data, which can either be stored on board or transmitted to a remote device. Moreover, it is very difficult to prove the intention behind the collection and use of data.

Currently existing FAA guidelines are not specific enough to dictate the coverage policy for personal and commercial liability, invasion of privacy, personal injury or property damage. Commercial liability should include financial loss since many drone companies are still in the startup phase. The property coverage also should include the processes of production, assembly and wholesaling. Likewise, rather than just focusing on the finished product, it is important to realize that most drones are modular and could be comprised of independently sourced components. Even more confusion arises from the lack of a strict definition of a drone. Currently, due to the broad range of standards and applications, drones could be classified as quad copters, model aircraft, or even light aircraft. This lack of categorization makes it challenging to properly assess the coverage policies since each class of aircraft has its own set of guidelines.

# 4.4 Regulation – Attempts and Challenge

Regulations for military and civilian drones application differ considerably. Military drones, which have existed for a while, have regulations developed over time to cover only a very limited set of activities in a specific and controlled airspace. The broad applications of civilian drones, and their relatively small impact if compromised, have appreciably clogged and therefore delayed regulations related to the commercial and private environment. This effect has been exacerbated by the open source development of the technology, which makes it difficult to keep track of the changes. Thus, as often happens, technology already far outpaced the regulatory process. This has implications for the widespread acceptance and adoption of drones as a viable platform.

For the private use of drones there are two key factors that concern people: privacy and safety. While drone-filmed videos and footage are positively portrayed by the popular media and are a source of entertainment on the Internet, they are also fostering an active debate about their lawfulness and questionable behavior. Since there is no clear regulation to follow, drones have been freely hovering in public places, causing discomfort and controversial reactions by the oversight agencies involved [30] [31]. The use of drones is not yet regulated in order to insure individual property rights and safety. There is more than one stakeholder involved in this process: the government at the federal, state and city/town levels, drone manufacturers, software vendors, as well as end-users all have their own motivations. Typically, as in other emerging technology-based products, the customers want choice and access, businesses want to manufacture and sell products unhindered while meeting customer needs, and the regulatory and law enforcement agencies need to have confidence in the regulations themselves as well as their ability to enforce violations.

Both governmental and business entities are actively working to improve the technology in order to safely integrate drones. In 2012, Congress passed the FAA Modernization and Reform Act, with a view to formulating guidelines for airspace use by civilian Drones. In February 2015, the FAA consequently proposed a simple approval process that any firm interested to fly drones for commercial purposes could follow. This proposed process would be necessary for the deployment of any UAV under 55 pounds, and operators would be required to pass the same written exam (that had a validity of two years) vetted by the Transportation Security Administration for private pilots. These pilots would need to obtain a certificate from the agency and respect the safety requirements [32] [33] of flying below 500 feet during daytime, within eyesight, away from private property, and should remain least 5 miles from the closest airport.

The Federal Communication Commission (FCC) and the International Bureau together with the Public Safety and Homeland Security Bureau have been putting efforts to secure GPS Protection and improve Receiver Performance. As of now, the main improvements have been carried out by drone makers, as they seek to improve the wireless link between drones and operators and to enable the devices to sense and avoid obstacles automatically. For example, DJI Innovations, a leading drone-maker, has already implemented in its latest product design a GPS-based localization that would prevent the aircraft from flying over 500 feet, and from getting into restricted airspace, e.g., around and over airports. However, the technology has proliferated into mass use and it is not clear that these rules will completely prevent accidents and close calls. Washington-based DroneShield LLC has installed about 200 of its audio-based detection systems world wide over the past 18 months, including around prisons, government buildings and power plants. Resilient Solutions Ltd., in Alexandria, Va., is

working with a European defense contractor to develop a sophisticated system that can detect and track a drone and identify whether it is a threat [34].

From a privacy perspective, the issue is intricate since the line between private and public can no longer be defined by physical boundaries. Furthermore, there are concerns over effect on sovereignty since a commercial drone flown over international airspace or the airspace of another country, could be viewed as a threat to national security. The International Civil Aviation Organization explicitly empowers individual national agencies to set their own regulations [35]. In Europe, the European Aviation Safety Agency (EASE) is contemplating the possibility of shifting the responsibility of regulation from each Member State to a coregulatory approach that would reduce resource constraints, but at the same time would increase the risk of backlash caused by the curtailment of enforcement powers and stakeholder engagement [36].

In the US, the Association for Unmanned Vehicle Systems International, which represents the UAV industry, recently developed and released a "Code of Conduct" - generic rules in order to observe current privacy and liberty rights and to avoid accidents - but it is not clear how these rules will be enforced [37]. Similarly, the FAA has been trying to create separate, and less-demanding rules for unmanned aircraft weighing less than five pounds. The proposal explicitly notes that agency officials have the right to pursue hobbyists and other recreational users if they are found to operate devices in a "reckless manner". Currently, these rules affect recreational use of drones, the use of which is already permitted as long as users obey safe-operating requirements, and hence they fail to deal with privacy issues. The FAA has never handled privacy concerns before, and the rapid adoption of civilian drones is challenging the organization. This challenge has hampered the FAA for years and is evident in their constant postponement of a definitive ruling [38] [39]. The Government Accountability Office reported a lack of "consensus of opinion", stating that the FAA will not create new rules before 2017 [40].

In December 2015, the FAA passed a federal law requiring all drones weighing over 250 grams and their users to be registered online [41]. Taking effect on the 21st of that month, the law was justified in the interest of privacy and public safety and security as they reported 1133 cases of unsafe use. The law is posited to counteract a "market failure" which includes the increasing number of UAVs, possibilities of technical failure, and the lack of users' experience. It is currently applicable to individuals and not companies, thus only affecting recreational users and hobbyists. As a result, a user without a certificate or a flying an unregistered drone, even on their own property, would result in civil and criminal sanctions including fines and imprisonment. Though it is not possible to predict if this law would effectively reduce the number of accidents, communities of drones enthusiasts and activism groups have already denounced it. These criticisms challenge the FAA's assumptions about drones and their operators, the extent and effectiveness of the sanctions, the vagueness of definitions, and the legitimacy of a federal organization's authority over domestic activities.

# 5. Discussion and Implications

When it comes to drones is it possible to divide the population in two main categories: those who can be defined as UAVs enthusiasts, looking forward to use them either for private or commercial use; and those who believe these devices are a threat - with the potential of endanger their freedoms as well as daily activities. Despite the huge improvements that drones can provide, the public is skeptical: a recent surveys on a sample of 2405 US citizen's

shows that 42% disapprove private ownership of drones, mostly because of privacy concerns [42]. Many have questioned the recent FAA rules on commercial drones, suggesting that rules will adversely affect small drone based businesses, as well as questioning their clarity. The lag between meaningful and enforceable regulation compared to the pace of development of new devices, is creating more confusion. For example, in the aforementioned survey, most of the respondent are basically unaware of existing regulation (30% of them believe FAA is not regulating class G airspace, which is below 1200 feet), are confused about which certificate is needed to operate a drone (the Certificate of Authorization COA vs. Exemption vs. Waiver vs. ... [43]), and what those certificates imply, since the rules does not cover all potential situations. Forty seven percent of the companies surveyed in the report state they have been operating in Class G airspace even without the regulation in place, which means that potentially they are already exposing civilian to the threats they would like to avoid, and 62% are currently flying without commercial liability insurance for their UAVs. This also raises questions about the potential implications for the insurance industry. Currently, there are not policies available, though they are in the process of being developed to cover such contingencies. Another 47% of respondents state that they are postponing the creation of jobs since they are not sure whether the regulation would make the industry favorable or not, and 61% would be willing not to start their operations, or to shut down the one that already exists if the regulations are perceived to be unfavorable [44].

In fact, there is some evidence that delays in developing a clear framework have prompted several private manned aircraft frequently operate without flight plans around working areas to capture images above sites without asking for approval prior to take off, even if those operations are currently in violation of FAA policy. Thus, on one hand private users are not at all regulated and can create potential safety issues, while on the other hand commercial development is criminalized [45]. The ability to enter private property undetected and to record information that can be streamed live originates significant opportunities for privacy breaches. Generally speaking, the risk of UAV usage as every other technology for illegal activities is unavoidable. However, since existing guidelines and rules overlook the possibility of a hard-to-notice flying camera widely available to masses, they also increase the potential of misuse.

As mentioned above, many countries have already started the process to adapt their regulations to address safety and technical issues. Nevertheless those arrangements do not engage in fixing the most imperative problem created by drone technology: faulty privacy and surveillance regulations. Even Australia, which is one of the pioneers of the use of drones for commercial activities, has recently pointed out the inappropriateness of its Commonwealth Privacy Act, that does not cover collection and use of personal information by private citizens and small businesses [46]. Furthermore at this time, traditional enforcement appears weak and expensive and new infrastructures need to be established. It is paramount to first update the current definition of privacy and finds new ways to guarantee its protection balancing freedom of expression, open justice, public safety and national security. Given the current fuzziness of directions, businesses will face difficulties in lawfully developing hardware and software solutions to exploit the huge industry potential. Another critical aspect in integrating the UAS in the National Airspace System is law enforcement, which is currently ineffective and expensive.

Untrustworthiness creates huge resistance to new technologies: a way to sensitize masses to drone misuse consequences is to assign accountability and liability. As for now, in the US only broad general guidelines have been provided and basic tool such as evidence collection

and operator/witness identification and interview have been performed in case of UAV related accidents [47]. However, since UAV can cause physical damages as cars do, it seems legitimate to hypothesize the introduction of compulsory specific insurance plans, that would create a registry of devices to link each and every sold one to its owner and therefore help in assigning responsibilities for illegal activities. Furthermore, as for now each jurisdiction is empowered to determine its own rules they will eventually cause inconsistency across contiguous regions and Countries. Ideally standards have to be set throughout governmental and private organizations as well as across Countries. Also, in order to be valid to protect the interest of privacy as long as possible they should not be strictly related to the single technology. Some directions on how the aforementioned goals can be achieved are summarized in Table 1.

Table 1: Key Challenges of UAVs and their Mitigation

Issues	Major Challenges	Possible Solutions
Privacy	Detection/Access to justice	Hardware and software for device detection, and data retention / Registry of owners and devices
Ownership	Accountability	Registry of owners and devices/ Assign liability for UAV owners/
Security	Control/Enforcement	Creation of new infrastructure and development of proper assets: UAV trackers devices/automatic safe landing / Establishment of insurance entities etc.
Regulatory	Lack of comprehensive rules and uniformity across jurisdictions	Redefinition of "reasonable expectation of privacy"/ Definition of physical aerial boundaries / Centralization of Powers
Business Models	Lack of clear guidelines to operate in compliance with the law	

## 6. Contributions & Conclusion

The rapid evolution of drones for civilian applications has created several challenges: regulatory, safety, privacy, security, and the uncertain landscape for new business models. The paper shows that there are several bottlenecks that are hampering more rapid adoption of drones, including regulatory and enforcement clarity and lag, cultural perceptions or misconceptions of what drones are and what they can do, as well as significant challenges that can be thrown up by a more rapid proliferation of drones. As the population of civilian drones and their users expands globally, the risk of accidents both digital and physical are destined to multiply. The Internet revolutionized personal computing thanks to a confluence of technical, social, regulatory and cultural trends and efforts. The future success of civilian

drones depends on the ability of varied stakeholders to reconsider how this emerging technology platform can be best harnessed to serve the broad interests of society.

#### References

- [1] Bijker, W. E., & Law, J. (1992). Shaping technology/building society: Studies in sociotechnical change. MIT press.
- [2] Mackay, H., & Gillespie, G. (1992). Extending the social shaping of technology approach: ideology and appropriation. Social studies of science, 22(4), 685-716.
- [3] Schultze, U., & Orlikowski, W. J. (2004). A practice perspective on technology-mediated network relations: The use of Internet-based self-serve technologies. Information Systems Research, 15(1), 87-106.
- [4] Finn, P. (2011). Domestic use of aerial drones by law enforcement likely to prompt privacy debate. Washington Post, 22.
- [5] Oudes, C., & Zwijnenburg, W. (2011). Does Unmanned Make Unacceptable? Exploring the Debate on Using Drones and Robots in Warfare. IKV Pax Christi.
- [6] Finn, R. L., & Wright, D. (2012). Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications. Computer Law & Security Review, 28(2), 184-194.
- [7] Thompson, R. M. (2012, September). Drones in domestic surveillance operations: Fourth amendment implications and legislative responses. Congressional Research Service, Library of Congress.
- [8] Austin, R. (2011). Unmanned aircraft systems: UAVS design, development and deployment (Vol. 54). John Wiley & Sons.
- [9] Newcome, L. R. (2004). Unmanned aviation: a brief history of unmanned aerial vehicles. Aiaa.
- [10] O'Brien, S. (2015, January 7). Drone startups swoop up millions. Retrieved October 14, 2015, from http://money.cnn.com/2015/01/07/technology/ghost-drone/
- [11] Cummings, M. L., Bruni, S., Mercier, S., & Mitchell, P. J. (2007). Automation architecture for single operator, multiple UAV command and control. Massachusetts Inst Of Tech Cambridge.
- [12] Robinson, A. (2006). FAA Authorizes Predators to Seek Survivors. US Air Force Archives.
- [13] Craighead, J., Murphy, R., Burke, J., & Goldiez, B. (2007, April). A survey of commercial & open source unmanned vehicle simulators. In Robotics and Automation, 2007 IEEE International Conference on (pp. 852-857). IEEE.

- [14] Deseilligny, M. P., & Clery, I. (2011). Apero, an open source bundle adjusment software for automatic calibration and orientation of set of images. ISPRS-International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences, 38, 5.
- [15] Chao, H., Cao, Y., & Chen, Y. (2010). Autopilots for small unmanned aerial vehicles: a survey. International Journal of Control, Automation and Systems, 8(1), 36-44.
- [16] Marks, P. (2011). 3D printing takes off with the world's first printed plane. New Scientist, 211(2823), 17-18.
- [17] Ahmed, N. A., & Page, J. R. (2013, November). Manufacture of an unmanned aerial vehicle (UAV) for advanced project design using 3D printing technology. In Applied Mechanics and Materials (Vol. 397, pp. 970-980).
- [18] Maza, I., Kondak, K., Bernard, M., & Ollero, A. (2010). Multi-UAV cooperation and control for load transportation and deployment. Journal of Intelligent and Robotic Systems, 57(1-4), 417-449.
- [19] Ping, J. T. K., Ling, A. E., Quan, T. J., & Dat, C. Y. (2012, October). Generic unmanned aerial vehicle (UAV) for civilian application-A feasibility assessment and market survey on civilian application for aerial imaging. In Sustainable Utilization and Development in Engineering and Technology (STUDENT), 2012 IEEE Conference on (pp. 289-294). IEEE.
- [20] Jacques, C. (2014, October 14). Led by Agriculture, Market for Commercial Drones Will Reach \$1.7 Billion in 2025. Retrieved October 14, 2015, from http://www.luxresearchinc.com/news-and-events/press-releases/read/led-agriculture-market-commercial-drones-will-reach-17-billion
- [21] Klochkov, V., & Nikitova, A. (2008). A Simplified Approach to Economic Efficiency Analysis of UAV Pipeline Surveillance. Transport & Engineering, Vol. 27, p172-180.
- [22] Paganini, P. (2014, April 25). Privacy and Security Issues for the Usage of Civil Drones InfoSec Resources. Retrieved October 14, 2015, from http://resources.infosecinstitute.com/privacy-security-issues-usage-civil-drones/
- [23] Lega, M., & Accardo, A. F. (2003, September). Index of risk and safety objectives for civil UAVs. In AIAA 2nd "Unmanned Unlimited" Systems, Technologies, and Operations—Aerospace, Land, and Sea Conference and Workshop & Exhibit, San Diego (CA)–USA (pp. 15-18).
- [24] Gee, J. P. (2014). An introduction to discourse analysis: Theory and method. Routledge.
- [25] Jørgensen, M. W., & Phillips, L. J. (2002). Discourse analysis as theory and method. Sage.
- [26] Schutz, A. (1962). On the methodology of the social sciences. The problem of social reality, 3-47.
- [27] Boyle, M. J. (2015). The Race for Drones. Orbis, 59(1), 76-94.

- [28] Chow, E., Cuadra, A., & Whitlock, C. (2014, June 20). Retrieved October 8, 2015, from https://www.uavdach.org/News/Missbrauch/2014-06-20Fallen from the skies\_ drone crashes database Washington Post.pdf
- [29] Cuadra, A., & Whitlock, C. (2014, June 20). How drones are controlled. Retrieved October 14, 2015, from http://www.washingtonpost.com/wp-srv/special/national/drone-crashes/how-drones-work/
- [30] Serna, J. (2014, June 21). As hobby drone use increases, so do concerns about privacy, security. Retrieved October 14, 2015, from http://www.latimes.com/local/la-me-drone-hobbyist-20140622-story.html
- [31] Schlag, C. (2012). New Privacy Battle: How the Expanding Use of Drones Continues to Erode Our Concept of Privacy and Privacy Rights, The. Pitt. J. Tech. L. & Pol'y, 13, i.
- [32] Nicas, J., & Pasztor, A. (2015, February 15). FAA Proposes Rules to Allow Commercial Drone Flights in U.S. Retrieved October 14, 2015, from http://www.wsj.com/articles/obamaissues-privacy-rules-for-government-drones-in-u-s-1424015402
- [33] FAA. (2015, February 15). Small UAS Notice of Proposed Rulemaking (NPRM). Retrieved October 14, 2015, from https://www.faa.gov/uas/nprm/
- [34] Nicas, J. (2015, January 28). Criminals, Terrorists Find Uses for Drones, Raising Concerns. Retrieved October 14, 2015, from http://www.wsj.com/articles/criminals-terrorists-find-uses-for-drones-raising-concerns-1422494268
- [35] Clarke, R., & Moses, L. B. (2014). The regulation of civilian drones' impacts on public safety. Computer Law & Security Review, 30(3), 263-285.
- [36] Association for Unmanned Vehicle Systems International, 2015. Code of Conduct. Retrieved October 14, 2015, from http://www.auvsi.org/conduct
- [37] Beasley, S., & Levin, A. (2014, December 31). FAA Fails to Meet 2014 Goal for Proposed Drone Regulations. Retrieved October 14, 2015, from http://www.bloomberg.com/news/articles/2014-12-31/faa-fails-to-meet-2014-goal-for-proposed-drone-regulations
- [38] Whitlock, C. (2014, June 30). FAA will miss deadline to integrate drones in U.S. skies. Retrieved October 14, 2015, from https://www.washingtonpost.com/world/national-security/faa-will-miss-deadline-to-integrate-drones-in-us-skies-report says/2014/06/30/fd58e8e2-007f-11e4-b8ff-89afd3fad6bd\_story.html
- [39] Holton, A. E., Lawson, S., & Love, C. (2014). Unmanned Aerial Vehicles: Opportunities, barriers, and the future of "drone journalism". Journalism Practice, (ahead-of-print), 1-17.
- [40] FAA.gov., (2015). Unmanned Aircraft Systems. Retrieved December 16, 2015, from https://www.faa.gov/uas/

- [41] FAA.gov,. "Unmanned Aircraft Systems (UAS) Registration". N.p., 2015. Web. 16 Dec. 2015.
- [42] Ipsos, & Reuters. (2015, February 5). Ipsos/Reuters Poll: Drones. Retrieved October 14, 2015, from http://www.ipsos-na.com/news-polls/pressrelease.aspx?id=6749
- [43] J. Rupprecht, (2015). Drones: Their Many Civilian Uses and the U.S. Laws Surrounding Them.
- [44] Anand, S. (2007). Domestic use of unmanned aircraft systems: an evaluation of policy constraints and the role of industry consensus standards. ASTM Standardization News, 35(9), 30.
- [45] Crovitz, G. (2014, December 28). The Grinch Who Stole . . . Drones. Retrieved October 14, 2015, from http://www.wsj.com/articles/l-gordon-crovitz-the-grinch-who-stole-drones-1419811476
- [46] Christensen, G. (2014). Eyes in the sky: Inquiry into drones and the regulation of air safety and privacy. Australia's House of Representatives Standing Committee on Social Policy
- [47] FAA. (2014). Law Enforcement Guidance For Suspected Unauthorized Uas Operations. Retrieved October 14, 2015, from:
- https://www.faa.gov/uas/regulations\_policies/media/FAA\_UAS-PO\_LEA\_Guidance.pdf