"Spiders in the Sky": User Perceptions of Drones, Privacy, and Security

Victoria Chang, Pramod Chundury
University of Maryland, College Park
[vchang90, pchundur]@umd.edu

Marshini Chetty
Princeton University
marshini@princeton.edu

ABSTRACT
Drones are increasingly being used for various purposes from recording footage in inaccessible areas to delivering packages. A rise in drone usage introduces privacy and security concerns about flying boundaries, what data drones collect in public and private spaces, and how that data is stored and disseminated. However, commercial and personal drone regulations focusing on privacy and security have been fairly minimal in the United States. To inform privacy and security guidelines for drone design and regulation, we need to understand users' perceptions about drones, privacy, and security. In this paper, we describe a laboratory study with 20 participants who interacted with a real or model drone to elicit user perceptions of privacy and security issues around drones. We present our results, discuss the implications of our work, and make recommendations to improve drone design and regulations that enhance individual privacy and security.

ACM Classification Keywords
H.5.m. Information Interfaces and Presentation (e.g. HCI): Miscellaneous

Author Keywords
Drones; quadcopter; privacy; usable security; users

INTRODUCTION
Drones are fast becoming popular in the commercial and noncommercial sectors for a variety of purposes such as providing Internet access, capturing media footage of remote locations, and delivering packages [4, 22, 29]. In fact, the Federal Aviation Agency (FAA) in the United States (US) forecasts the sales of commercial drones will reach 2.7 million by 2020 [14] and civil drones production is predicted to rise from 2.6 to 10.9 billion USD by 2025 [35].

Yet, regulation around drones has been slow to follow [33] although drones affect individual privacy and security because they can record or injure people [8, 32, 17, 39]. Even with recently introduced rules governing drone operation, the FAA only provides unspecified "privacy guidelines" regarding drone usage [16]. To better inform privacy and security enhancing legislation to regulate where drones can go and what data they can collect, store, and disseminate, we first need to understand how users currently perceive drones, their purposes, and capabilities.

In our work, we build on a growing number of studies on understanding the privacy issues around drones; mostly conducted in countries outside of the US [22, 10, 2] with the exception of two closely related studies in the US [19, 39]. Our goal is to help create privacy and security enhancing designs for drones and policies. To achieve this goal, we posed the following research question: how do users feel drones affect their personal privacy and security expectations?

To answer this question, we conducted a study with 20 users in a laboratory setting at the University of Maryland, College Park (US). Each user interacted with a real or a model of a drone to better tease out how drones affect their privacy and security concerns and their attitudes towards drone regulations. We have two main findings. First, we confirm that concerns raised by prior studies such as drones invading privacy through watching and spying [39] still hold a year later in another part of the US and provide new evidence of *negative perceptions* around drones such as fear of damage or injury and unwillingness to disclose personal information under drone surveillance.

Second, we provide further evidence confirming findings from Wang *et al.* [39] that *drone design*, including the color, size, speed, and noise of drones shapes peoples' perceptions of privacy and security. We also provide new evidence that a drone's form factor, wind, guard, movements, camera location and quality, data recording capabilities, and feedback lights also affect privacy and security perceptions. Based on our findings, we make three recommendations for improving regulations and creating drone designs to enhance peoples' sense of privacy and security around drones.

BACKGROUND

Drones, Usage, and Capabilities
Drones are defined as unmanned aerial vehicles (UAVs), remotely piloted aircraft systems, quadcopters, multicopters [8, 22, 1] and can vary in size and capacity from toy drones (micro UAVS) to military (tactical and strategic UAVs) drones. First favored for military purposes, drones are now being hailed for the private sector, law enforcement [38], and hobbyists [8, 22] for non-threatening purposes because they can go to places where people cannot easily go and are becoming

CHI'17, May 06-11, 2017, Denver, CO, USA
©2017 ACM. ISBN 978-1-4503-4655-9/17/05...$15.00
DOI: http://dx.doi.org/10.1145/3025453.3025632

more affordable. Drones also have various sensors; such as cameras capable of streaming real-time video, which can gather information from a number of different vantage points either on a one off or continual basis [8]. Drones affect privacy because they have the ability to collect, retain, use, and disclose personal information [8, 36], and can provide *"pervasive panopticon-like surveillance"* as well as injury to people [17]. Additionally, drones affect security because they can enter private or restricted areas or collide with other things.

Drones and Users

There is a growing body of research examining human-centered issues around drones. For instance, Cauchard *et al.*, have investigated natural human-drone interactions including understanding metaphors and relationships that occur during an interaction with a drone as well as how users encode emotion based on how drones move [5, 6, 21]. Other studies focus on creating novel interfaces to control a drone, e.g., using head and human motions such as walking and crouching [7, 20, 24], and examining different interface types [23]. Research efforts have also focused on how drones can augment existing human activities such as jogging [18]. While these papers examine how users can interact with and perceive drones, they do not specifically address how users feel about privacy and security implications of drones.

Drones, Privacy, and Security

An increasing number of studies tackle how users view privacy and security issues around drones. Lidynia *et al.* conducted a survey of 200 users in Germany to investigate perceptions of drone usage [22]. They found that laypersons felt drones could violate privacy via unwanted intrusions into private spaces and active drone users feared accidents. Their participants also generally did not fear drones and had differing views depending on what the drone was being used for, e.g., emergency drones should fly freely.

In Australia, researchers surveyed 500 people to understand public perceptions of drones [10]. They found that participants had a neutral attitude towards drones and did not consider drones to be overly unsafe, risky, beneficial, or threatening. In this study, users examined images about or read about drones before answering questions. In a similar study, users were asked about drones in the United Kingdom and Italy [2].

In the US, there are at least two studies examining user perceptions of privacy and security issues around drones. In 2014, Herron *et al.* [19] surveyed 1364 US residents in all 50 states. In this study, the results were not definitive because users were largely unfamiliar with drones and still forming impressions. However, most users said benefits of drones outweigh risks. In another related study in 2015 Wang *et al.* [39] asked 16 users residing in Syracuse, New York what they thought about using drones for civilian uses and in specific usage scenarios. They showed people a real drone, if the weather permitted, and illustrated capabilities in flying and taking off videos before interviewing them. They then gathered reactions to five drone usage scenarios (presented without a drone), compared drones to existing technologies, and asked about controls and regulation. They found that users had mixed feelings about drones and recommended that regulation needs to cover drone users and drone controllers.

Our studies differ from these former studies because we systematically elicited feedback on mental models of drones and current regulations through sketching and annotation exercises. In addition, unlike the former studies, particularly Wang *et al.* [39], we showed all of our users a drone or model drone first hand, and allowed each user to see a drone/model drone being controlled, and to control a drone/model drone themselves. Our study also builds off these previous works to provide evidence to confirm their findings hold in another part of the US even though our sample is similar to Wang *et al.*'s [39] sample of college students. Most importantly, we add new evidence around growing negative perceptions of drones and how drone design shapes privacy and security perceptions in a more in depth fashion than prior works. For instance, our work shows that the sound produced by a drone can both annoy and alert users to its presence.

Drone Regulation

Legal scholars have been examining privacy laws governing drone usage [25, 32, 29] and agree that current FAA regulations should include rules on the data collected by drones instead of just drone operation[4, 37]. Specifically, concerns around a drone's collection of information about people by individuals, the government, or private sector and what is done with that information have been highlighted [36].

In 2016, the FAA released the small unmanned aerial vehicle rule [16]. This rule governs drone operations for commercial and personal usage and includes more stringent requirements for drone operator registration. For example, drone owners now need to take a training course as part of registration and be at least 16 years of age. The FAA also created the B4UFLY app to help drone users see if there are specific restrictions on flight in the location that the user is in [15]. However, these rules still do not govern what data a drone can collect or what drone owners can do with that data. In our research, we provide further evidence to inform rules that can protect the privacy and security of individuals.

METHODOLOGY

Recruiting

We conducted our research between March and May 2016 using a study design built on prior studies of privacy and security issues around other emerging technologies (i.e. self-driving cars) [31] and human-drone interaction studies [5]. The study was approved by our institution's Institutional Review Board (IRB). Participants were a convenience sample of students recruited from the University of Maryland College Park, which is located in a major metropolitan area.

We recruited via mailing lists of various academic departments including English Literature, Psychology, Computer Science, and Information Studies and received 53 responses. In our advertisements, we did not use the words 'privacy' or 'security' to avoid bias in recruiting. We also asked for participants without motor, visual, or hearing impairments so they could provide feedback on the drone's features and

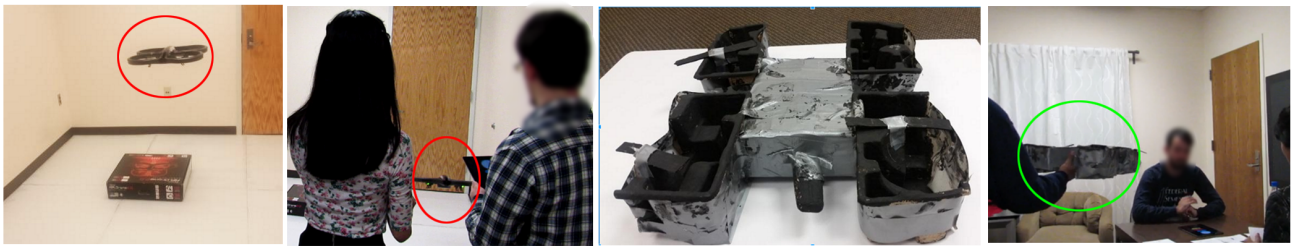

Figure 1. From left to right: Our Parrot A.R.Drone hovering, Participant D7 controls the real drone highlighted in red. Our model drone; Participant ND7 'controls' our model drone highlighted in green. In both scenarios, participants used our pre-programmed iPad application for controls.

maneuver away from our drone in the case of malfunction. We sent each respondent an online survey to gather demographic information and experiences of personal drone usage. This survey included two behavioral scales to measure what people do to protect their privacy (General Caution and Technical Protection Scales (rating from 1=never to 5=always)) and an attitude based scale on Privacy Concern (rated from 1=not concerned at all to 5=extremely concerned) [3]. We also measured the security related behavior of the participants using the Security Behavior Intention Scale (SeBIS) scale [13], a 16 item scale (rated from 1=never to 5=always) mapping device securement, password creation and usage, proactive awareness, and software updating. This survey also allowed us to screen participants for users over the age of 18 who had never owned a drone and with a variety of educational backgrounds.

We received 43 completed survey responses and selected 20 users for our experimental study to balance for age and gender. Participants were randomly assigned to one of two groups that we balanced for gender, one interacting with a real drone and the other group with a model drone. Splitting participants into two groups allowed us to clearly isolate the features of a real drone (such as sound, wind, and speed) that affect privacy and security concerns as opposed to a model drone. We used a model drone over no drone to ensure that all our participants had a realistic mental model of a drone since the model we created was the same size, shape, and color as the real drone along with features to resemble the camera. We also mimicked the real drone's movements with the model as well.

Each participant took part in an in-person session at our institution lasting 60-90 minutes. The session consisted of an initial interview with two exercises, an experimental session, and an exit interview. Two researchers facilitated the session, one leading the participant through the tasks of the session, and the other taking notes and assisting with maneuvering the drone or model drone for the experimental session. The entire session was audio and video-taped. Participants were compensated with a $30 Amazon gift card.

Initial Interview

We conducted the initial interview in a room where a participant could not see our drone or model drone to assess their opinions beforehand. We asked questions about participants' privacy and security habits in general, their knowledge of drones, and discussed their reactions to a scenario where they encountered a drone hovering over their house. We also asked them about their understanding and preferences concerning FAA policies around drones at the time of the experiment.

Next, participants completed two exercises. In the first exercise, we asked them to review the registration certificate that one of the researchers obtained after registering our drone. This certificate is now obsolete since the introduction of new FAA rules that came into effect after the completion of our study [16]. In second exercise, participants were asked to draw a drone and its features to elicit their mental models of drones, a technique used in previous studies [28].

Experimental Tasks

After the initial interview, participants were brought to the experimental room. Ten participants interacted with a real Parrot AR.Drone 2.0, a four-rotor quadricopter [27] seen in Figure 1. This drone is fairly common and relatively affordable to other personal drones. We shall refer to these users as the *drone group* and indicate these participants with the prefix "D". The other ten interacted with a life-sized model drone that we built out of cardboard and tape and painted black (also shown in Figure 1). We shall refer to these participants as the *non-drone group* and use the prefix "ND" to indicate these participants. All participants were walked through five experimental tasks to expose them to the drone's capabilities and get their feedback on how drone would affect their personal privacy and security. *Non-drone* participants interacted with our model drone which was maneuvered by one of the researchers, while the other researcher explained what the task would look like with a real drone using illustrations on a task card.

Experimental Task 1: Drone Design and Surveillance

In this task, we elicited participants' initial reactions to a drone and its basic capabilities, such as unmanned aerial flight and the ability to record and transmit data. Participants in the *drone group* were asked to sit in front of a TV monitor. We programmed the drone to start up and hover at this time so that participants would see the live stream of the video that the drone was taking of them on the monitor. The researchers did not explicitly say anything about or point out the drone recording. Our *non-drone group* participants were shown a task card illustrating the scenario and the fake drone was maneuvered into a hovering position.

Experimental Task 2: Physical Safety and Security

In Task 2, we wanted to examine reactions to the drone physically approaching a participant and determine if

participants would answer personal questions while being recorded by a drone or model drone. In the *drone group*, after participants observed the drone for five minutes in Task 1, the drone would slowly move forward toward the participant. As the drone moved toward the participant, the image displayed on the monitor enlarged as well. In the *non- drone group*, a researcher moved the model drone toward the participant but there was no live feed of video. While the drone or model drone moved forward, we asked each participant three personal questions regarding their grade point average (GPA), income, and household size. We also asked how comfortable they felt answering these questions in the given situation.

Experimental Task 3: Researcher Controls Drone

In Task 3, we elicited reactions to another person controlling a drone and the basic drone flight actions. In the *drone group*, a researcher controlled the real drone via the Parrot A.R. Free Flight application on an iPad. For the *non-drone group*, the researcher maneuvered the model drone to perform the actions instead. The actions for both groups were moving the drone left to right, up and down, and forward and back in the direction of the participant and back to its origin point. Each movement was performed continuously twice.

Experimental Task 4: Participant Controls Drone

In the fourth task, we aimed to gather feedback about the experience of controlling a drone. We chose not to give the participants direct control of the drone due to safety. Drones can lose connectivity with the controller and could cause accidents. We also wanted to minimize the learning phase needed to control the drone, especially for those who had never flown remotely piloted devices.

We created an *iPad application* with a web server coded with node JS, with a front-end application written in HTML, CSS and jQuery, also utilizing the "node-ar-drone" library [26] to execute specific action commands to the drone. We provided six programmed actions, along with buttons for abort, land, stop, reset, and liftoff. Each action was continuous until a user moved to the next action. One researcher directed the participant to try each action in sequence and to move on when the participant felt comfortable to do so.

The six actions were: moving the drone left to right, rushing forward and back toward the participants, moving vertically up and down, rushing vertically up and down, changing the drone's LED lights from green to red and continuously blinking red, and flipping the drone in a 360 degree on the vertical axes. Each movement was performed continuously except for the flips which were done twice. Participants in the *non-drone group* utilized the same *iPad application* as the *drone group*. When they pressed an action button, one of the researchers maneuvered the model drone to perform the relevant action.

Experimental Task 5: Data, Storage, and Transmission

In the final task, participants in the *drone group* were shown the footage taken of them throughout the experiment. We did not show the entire footage, just clips of the experiment until the participant decided to move on from viewing it. Participants in the *non-drone group* were shown prerecorded footage of the researchers because we did not want to record them using any other devices. Also, since our focus on this task was to see participants reactions to seeing recorded footage and the angle of the recording as opposed to the content of the recording, we felt these conditions were equivalent. We asked participants if they knew they were being recorded, how they felt about the drone's data transmission and storage capabilities, and who would own the data taken by the drone.

Exit Interview

Following the experiment, we conducted an exit interview with each participant and asked them to describe what they were thinking in each of the experimental tasks, one by one. We also asked them about their attitudes towards privacy, security, and drones again to see if they had any differing views after encountering a drone or model drone. The end of the exit interview concluded the session and participants were thanked and given their compensation.

Analysis

We transcribed the audio files for each participant's session and one researcher performed a thematic inductive analysis [30] on the transcriptions using Atlas.ti. The transcripts were coded for phenomena of interest at the sentence level. The research team held regular meetings to achieve consensus on the codes, incorporating new codes as new phenomena were discovered. We then grouped our 3,861 codes into categories, which emerged into themes that reflected consensus of the group after extensive discussions. Additionally two researchers coded the participant sketches and annotated FAA registration forms. Finally, we performed a quantitative descriptive analysis on the surveys. From a triangulation of all the data, we arrived at two main themes around privacy and security around negative perceptions of drones and how drone design affects perceptions of privacy and security. The remainder of our data set is beyond the scope of this paper.

FINDINGS

We first summarize participants' demographic information and attitudes towards privacy and security in general and around drones. Next, we describe our two main findings: negative concerns around drones, privacy, and security; and how drone design affects privacy and security perceptions.

Participant Demographics

The median age of our 20 participants was 23 years with a range of 19-56 years. There were 11 females and nine males, with an even gender split in the *drone group*, and females outnumbering males six to four in the *non-drone group*. The age range in the groups was similar. 19/20 participants had never operated a drone before with one being unsure. Nine participants had never seen a drone in person prior to the study.

Privacy and Security Attitudes and Behaviors

Our participants scored a median of 3.3 on the Privacy Concern scale indicating they had about average concerns in terms of privacy attitudes. Participants also had a median score of 2.5 on the general caution scale and a median score of 3.3 on the technical protection scale indicating they were about below to average in terms of privacy related behaviors.

On the SeBIS scale, our participants had a median score of 4.25 on device securement, a median score of 3 on password generation, a median score of 3 in proactive awareness, and a median score of 3.33 in software updating. Finally, participants had a median score of 3.49 on the entire SeBIS scale, indicating that they were about average for security behaviors with an above average rating for device securement.

Negative Perceptions of Drones

We describe how participants reported more in-depth negative aspects of drones than positives, which stands in contrast to findings in prior works.

Drones Still Seen as Privacy Invasive

Participants told us what privacy means to them and that drones are privacy invasive. Similar to previous studies [39, 22], participants also told us that drones are privacy invasive, that they could be used for spying, or recording without consent. Unlike prior works, participants also mentioned not knowing where a drone was looking.

Privacy Definitions: Most of *drone group* participants (7/10) spoke about privacy having to do with the control over anyone interfering with private space. D1's quote exemplifies this concern: *"It's the knowledge that things that you would like to keep to yourself, like your backyard, knowing that nobody can fly over it. It would be kept private if you wanted it to be kept private. Unless you invited somebody over."*. The majority of *non-drone group* participants (6/10) spoke about privacy as having information transmitted only to the intended audience.

Spying Drones: When asked about drones in relation to privacy and security, participants, more than half of all participants (11/20) mentioned the feeling of being watched around a drone, describing *"the window"* as *"where the invasion starts to affect your privacy"* (D7). Most participants (five *drone group* and six *non-drone group*) were also concerned about being spied on by a drone because of its recording capability. In a quote that illustrates this point, ND2 explained how the drone's recording capability could be used for spying: *"Maybe you want to record someone's private life, or some stars, some famous people"*. For this reason, our participants felt that drones should be prevented from entering restricted areas such as government buildings or *"to spy on others"* (ND3).

Recording Without Consent: 80% of our participants mentioned a concern for the potential to be recorded either in public or in their own homes through a window and not knowing that the recording was happening. D7 best reflects what participants told us: *"You can pull up a wall around your house if you want some privacy, but somebody can raise a drone higher, move the drone across the fence and the wall and still access that."*. Others also mentioned an issue of not knowing where the drone was looking. In one exemplifying quote, D3 said, *"People have privacy concerns because you can't really see where the drone's looking"*.

To mitigate these concerns, before seeing the drone or model drone, participants wondered if drones could indicate when they are taking pictures. For instance, a typical quote we heard was similar to that of D2: *"Maybe the drone could have a light or something that indicates that it's taking a picture to make it more safe and make sure that people's privacy is protected, maybe something like an indicator. Or maybe some technology that people could have that could tell them that, "Oh, a drone is in their vicinity," and then taking pictures"*. Overall, participants were concerned for their privacy and wanted feedback to know when they were being recorded.

Fear of Damage or Injury From Drones

Unlike in previous studies [19, 39], we uncovered many concerns around physical safety and injury to wildlife, which were mentioned mostly in the experimental session and exit interview without prompting, although we did ask about wildlife briefly in the pre-interview.

Injury, Weaponization, and Air Traffic: The majority of participants (15/20) worried about physical harm or death because of drones malfunctioning and falling out of the sky . Some heard stories on the news about drones causing injury when they fell. Others just surmised damage or injury from collisions could be an issue before they saw the drone or model for the first time. D3 explained the concern that most raised: *"I really don't want people to get hit with them because I don't even know what they look like. I assume they have blades maybe somewhere. I wouldn't want just random accidents and people getting hit all them time because people fly them too close."*.

A large portion of participants (12/20) also worried about the drone's capability to carry items and raised the concern of not being able to tell if the *"payload"* was a camera, or weapon such as a bomb or gun. Some participants worried that drone owners might purposefully modify their drones to cause injury to others as D5 emphasized: *"The one thing I could think of would be just making sure you don't modify it to use anything that could hurt somebody, such as a weapon or something."*.

Over half of our participants (11/20) were concerned with damage and interference with air traffic and physical safety to planes. D1 elaborated: *"My biggest concern is air traffic safety, air traffic control safety with drones. Until Amazon gets authorization to start delivering packages and things like they want to. I'm not too worried about security and privacy at this point. I'm more concerned about safety."*. Participants' concerns were exacerbated by the knowledge that the drone could venture out of human vision which would increase the potential for error.

Harming Wildlife: In addition to injuring people, all of our participants' were concerned about drones disturbing nature. In an illustrative quote, D7 said: *"I think in urban areas, the impact to nature will be less, but I don't want to see drones in the Amazon, unless it's used for research purposes or something that will do good to the environment."* In particular, participants did not want drones to harm endangered species or to become *"trash"* and impact the environment.

Accountability For Drone Owners and Consent For Recording

Similar to findings from prior work in New York [39], our more recent study in Maryland also suggests that participants were collectively concerned about how drone owners could be held accountable for their drone's actions. Participants also

wondered how consent could be collected from the people that a drone records. For example, our participants asked how one could link a drone with its owner during a drone encounter as D2 explained: *"How can you prove that it is mine and I use it to do the bad things? You have no proof of that."*. In general, participants felt that commercial owners of drones would be more accountable than personal drone owners because of a fear of legal liability and repercussions.

However, participants wondered about consent for drone deliveries in residential areas. In a quote reflecting the participants' attitudes, D9 explained: *"As a consumer, I'd make my consent that my stuff can be delivered by a drone, but the drone still flies through a community and it occupies secondary space. Taking that consent from everyone is difficult. The government should intervene and they should have some laws regarding this."*.

Additionally, after seeing the drone being controlled and controlling the drone, a fifth of our participants (three *drone group* and one *non-drone group*) raised concerns around the the distance between owners and those being recorded. The *drone group* participants mentioned that the distance created between the owner and the drone was likely to cause a lack of accountability on the part of the owner. Illustrating the sentiments we heard, D6 described this physical distance from the drone to the owner as creating a *"detachment"* which can make it easier for owners to *"project their own sort of dysfunction onto"* the drone.

The six *non-drone group* participants also mentioned concerns about the drone owner being anonymous to them, suggesting that this is a concern that emerges despite not experiencing the physicality of the drone. These participants told us that their privacy and security concerns escalated at the thought of not being able to see the drone owner, since that meant anyone could take a recording with a drone without physically being there. Participants were also concerned with not knowing when they were being recorded and where the data was being transmitting to. When asked to compare the drone recording to a cell phone, participants felt that with a cellphone they could still hide their face, or tell someone to stop or delete a recording. In contrast, they felt that could not easily provide consent to record or prevent a drone recording them.

Distance between Drones and People: Participants felt the allowable distance between a drone and others depended on whether it was carrying a bomb or camera; if it was carrying weapons, the distance would have to be greater. Participants also mentioned that enforcing a strict distance between a drone and people for safety may not work if there are many drones in an area at once. In an extreme example, one of our participants (D2) re-imagined a scenario with Princess Diana being overwhelmed by paparazzi of a*"swarm of drones"*, stating this would be *"creepy"* and potentially dangerous.

To mitigate these concerns, several participants recommended a separation of space for drones and people. For instance, participants recommended commercial drones fly at a different altitude to better separate them out from people and to minimize crashes into other drones. In a typical example, D7 recommended, *"designated spaces"* like a *"road"* for drones, and suggested using highways so that even if drones fell, people would be protected in their cars. A separation of space, participants felt, could also prevent drone to drone collisions as captured by this quote from ND5: *"I think the biggest thing is going to be drones bumping into other drones, either deliberately or accidentally. If there were to be any legislation, I think that that is what should be addressed. Like the FAA has rules about how close things can be"*. Because of concerns about physical security, participants also mentioned limiting the number of drones in a vicinity to minimize the risks of drones.

Distance from Buildings: Unlike in previous work [39], our participants not only spoke about drones being invasive in private spaces but said that they could be equally invasive in public spaces such as office buildings. When asked how far drones should be from buildings, participants responded with distances ranging from 10ft to 50ft or higher. These responses were based on concerns of drones looking into windows, or whether a drone could turn around fast enough without running into a building and cause infrastructure damage to electrical components or balconies. Most participants (17/20) agreed that drones should not be allowed to fly near residences, especially in densely populated areas, and that they should be far enough from buildings that they could not record sensitive data. In a typical example, D5 talked about distances and preventing the record of sensitive materials: *"Preferably something that's not so close that I could read the credit card number off your credit card if I saw it."*. A few participants also mentioned the number of drones that should be allowed near any buildings. ND9 gave the example: *"If we had a million drones going around the Empire State Building, that's just way too much because people are trying to get work done."*. Overall, participants felt drones in numbers could disturb the peace even in public places.

Distance from Wildlife: When asked in the exit interview, all participants quickly opposed drones being near wildlife. The main reasons were that the introduction of a mechanical object in nature could change animal behavior, or that drones could cause harm to, or be harmed by animals. ND9's quote summarized what we heard: *"I really am concerned about wildlife. From my experience, I don't really think that animals would respond that well to them. They'd probably either try to attack them and people would get angry."*. Many people were particularly concerned about birds and other animals who may be injured by drones and their *"blades"* flying around.

Disclosing Personal Information Under Drone Surveillance

In our experiment, it became clear that participants who interacted with a real drone were less comfortable disclosing information under of drone surveillance. For instance, half of our *drone group* participants felt answering questions in front of the drone while it was recording was *"unnerving"* (D5) and as expressed by D4:*"I think I'm a suspect. It is not a very threatening situation, but I feel like I need to pay attention"*. The other half of our *drone group* participants were less concerned about answering private questions in front of the drone, because the drone was so loud that they felt it could

not hear them. Four of these same participants felt that if the drone was quieter and they did not know who was operating the device, that they would be more cautious.

In contrast, the majority of *non-drone group* (8/10) participants were comfortable in giving out personal information in front of the model drone. The two who were not comfortable said that they would be *"very uncomfortable if [he didn't] know who's controlling it"* (ND6) and because the recordings could *"be shown to anyone at any point of time. There is no control with me to actually stop that information."* (ND10). Participants also compared a drone recording them and somebody taking a picture as ND5 explained: *"I don't really think of anybody having any ulterior motives with a random photo where this is close to me and hovering around me and listening to me."* For this reason, our participants often reiterated that they would question the motive of the drone owner.

Positive Perceptions of Drones Were Less Pronounced

Interestingly, unlike in previous studies [39, 19] in the US, we found that the negative attitudes towards drones raised by the participants outweighed the positive attitudes. Surprisingly, the same issues that were regarded as negatives were also seen as positives in case of recording important events and landmarks, surveillance of *"suspicious"* people, and drones being used in warfare to avoid the use of and loss of humans. For instance, participants mentioned that drones could be used for fighting crime with their cameras if they had facial recognition software to help them find and track criminals as reported by earlier studies in NY [39].

Some participants felt that drones could be commercialized for safety purposes much like closed circuit security cameras. These participants said that they would not mind drones infringing on their privacy for the sake of public safety. D8 explained if *"Someone escaped from custody and is running around. You'd want to be able to find them as quick as possible. To prevent others from being harmed."*. For these participants, certain drones would be acceptable in private or public spaces. These findings indicate that positive and negative concerns around drone usage vary according to the perceived privacy and security expectations in a particular context.

Drone Design Affects Privacy and Security Perceptions

Our second major finding is that there are many aspects of the drone itself, such as the color, size, and sound that affect privacy and security concerns supporting findings from previous studies [39]. We also provide new evidence of drone design factors that influence privacy and security concerns such as wind, the appearance of the drone guard, the drone's movements, and recording capabilities.

Drone Attributes Make Drones Appear Threatening

Form Factor: Upon entering the experimental room, some participants immediately noticed and commented on the hovering drone whereas others observed until we asked more questions about the drone. A few participants who had never seen a drone in person before felt that the drone was *"intimidating"* (D4) depending on its proximity. All of the *non-drone group* felt discomfort because the drone was flying too close. Six of the *drone group* participants commented on the drone design saying the drone's form did not inspire trust. D7 elaborated: *"It doesn't make me trust it. It's black, maybe if it was a colorful coat thing. It doesn't come off as friendly right now."*.

The *non-drone group* participants also felt that the drone design did not make them feel comfortable and that as one participant, ND4, put it, *"I think they look like spiders in the air and I think that it would just be a recipe for disaster"* when speaking about widespread drone usage. A few participants also felt that drones reminded them of attacking and military purposes. For example, D6 compared the drone to an object that reminded her of the movie "Terminator" and *"military things"*. These findings stand in contrast to prior work [22, 10] that suggest people do not fear drones.

Color: At least several participants (four *drone group* and three *non-drone group*) expressed similar concerns about the color of the drone evoking feelings of *"unfriendliness"*. These participants were concerned about the drone being a monochrome black or dark color. To make the personal drone appear less likely to *"attack"* (ND6), participants suggested that drones should be painted in brighter colors, have logos, or writing on them. Moreover, participants suggested that drones should have hazard lights so that they can be easily distinguished from the background and allow people to react to them accordingly. At least three participants (two *drone group* and one *non-drone group*) also mentioned that drones used by commercial entities should be friendly looking and have a *"logo of the company on it."*.

Size, Stealth, and Safety: Participants in both groups said that the drone was bigger than what they had in mind which affected their perceptions of privacy and security. Four participants in the *drone group* and six *non-drone group* participants wondered if bigger drones might be concealing something inside them. Four participants from both groups mentioned that drones should also not be too small so as to become too stealthy. In one example given to us, a participant worried that small drones would be able to sneak into air vents and other restricted places or buildings *"that wouldn't normally be accessible to someone"* (ND9). All of the *non-drone group* participants also thought that drones smaller than the Parrot AR would be preferable for reasons such as being less likely to injure people.

Sound: All of the *drone group* participants had a negative reaction to the sound that the drone made. Four participants felt the sound was not *"inviting"*, *"loud"*, *"noisy"*, and *"scary"*. These and other participants wanted the drone to sound less threatening so that it could approach others in a friendlier manner. Although *non-drone group* participants did not hear the drone, two mentioned that there would likely be sound from the drone and commented negatively on it.

Wind: Seven *drone group* participants commented negatively on the breeze that they felt from the drone while in flight. The most concerned response was from D3, who described the sound of the wind as making the drone feel dangerous: *"All the air that it creates is weird. It feels powerful in a way because it's moving so much air that, it feels like if I stick*

my hand in that, it's going to chop it off.". Our participants felt that the noise and wind combined could make the drone seem very *"threatening"* for some people. Only two *drone group* participants did not notice the wind from the drone at all. The participants who interacted with the model drone did not mention the drone producing wind.

More than two thirds of the *drone group* participants felt more strongly about restrictions for personal drone usage after the experiment. Most were worried about limiting the sound, wind and speed of drones and wanted more stringent licensing requirements because drones could injure people when flying fast, scare or make people nervous if they fly too close to them, or if they fly in large numbers or in small spaces.

Guard: Although most of our participants viewed the drone as threatening, after seeing a drone for the first time in the experiment, the majority of *drone group* participants (8/10) were surprised it was made of soft materials and that it had a guard around it. Many felt that the guard was an important design factor for preserving physical safety. These participants felt more secure about drones hitting people or buildings since they felt it would bounce off and not do too much damage. The majority of *non-drone group* participants (7/10) also thought that the drone was safer with the guard since the *"propellers may hurt people"* (ND2).

Advantages of Drone Sound and Wind

Even though most participants commented on the sound and wind of drones as a negative, these attributes were also viewed as preserving privacy because they make drones less "stealthy" (D7). Six of *drone group* participants and one of the *non-drone group* appreciated the fact that the sound of the drone helped people to identify its presence as explained by ND5: *"I was at a wedding way out in the middle of nowhere, about two hours east of Seattle, so seriously in the mountains, seriously in the country. There was a drone flying over most of the time. I was trying to figure out whose it was, where it came from, and it was an annoying noise"*. In another example, D4 said she would recognize a drone is nearby and recording because *"the drone is noisy so [she knows] that it is near."*.

Drone Movements and Physical Security

Our findings suggest that movements of a drone can significantly impact participants' concerns about their physical safety and about drones invading private space. Half of the *drone group* were concerned about the stability of the drone and commented that the way the drone moved exacerbated the feeling that it was an unfriendly and unsafe device: *"When it started, I think that it's a bit unstable and I was a bit worried about where it would go. Now, also, it's not quite stable and it feels also that it might do something."* (D9). In another typical example, participant (D4) felt that when the drone was moving from left to right repeatedly in a very stable manner, it looked like a boxer performing a *"threatening action"*.

Participants also became more concerned when the drone sped up. In the experiment, when the drone rushed up and down, a few *drone group* participants worried that it would hit the ceiling or floor. During these movements, six *drone group* participants also became more aware of the drone's wind, which made them all feel as though they wanted more distance from the drone (D4). Participants also often felt that the drone moved in unusual ways that caused concern about it malfunctioning. For instance, when the drone flipped, half of the *drone group* participants reacted negatively with concerns that the flip movement was not a native function or ability, was scary, or was a malfunction. On the other hand, seven *non-drone group* participants found it *"amazing"* (ND1) or unsurprising. Similar to the participants interacting with the real drone, the three *non-drone group* participants who were concerned about the flip being a malfunction or in physical danger chose to abort or land the model drone.

The direction and speed of the drone's movements also made participants wary for their physical safely. For instance, half the *drone group* participants expressed physical safety concerns when the drone rushed forward. Like others, D6 said that he felt:*"Concerned for our safety. All three of us. I was worried that it would hit us and then I was like, "Oh, they look okay. They don't look alarmed so it's not going to come at us."*. For him and other participants, looking to the researchers reaction helped them stay calm despite the drone's fast movements towards them.

Non-drone group participants reacted similarly. The majority (8/10) reacted to the drone rushing forward by pressing the *"abort"*, *"land"*, or *"stop"* buttons. Participant reactions were caused by concerns about personal space or physical safety. The general attitude toward the rush was that *"it was invading [my] personal space"* (ND3) and some *"took it as a sign of aggression"* (ND9). The concern then extended into not knowing *"when it will stop."* (ND2, ND10).

In both groups, participants who did not react negatively to the drone's rushing movements or flip were more familiar with the technology or felt that they were safe because they were in a laboratory setting. However, despite feeling safe the two *drone group* participants who did not react said they had backup plans to hit the drone down if needed and looked to the researchers reactions to decide how to react. For example, D5 said *"If the thing had gotten any closer, I probably would have swatted at it. But the fact that you didn't move made me think I'm okay with it."*

Clandestine Data Recording Without Proper Feedback

Participants told us that how the drone is designed for recording, recording quality, data storage, and feedback on recording affects how they feel about privacy and security.

Camera Location: As reported in previous studies [39], our participants commented on the obscurity of the drone's camera and lack of feedback while recording. However, in a new finding, they also commented on being unable to discern the angle of the drone's camera. When six *drone group* participants saw themselves in a streamed video footage on the screen in the first two experimental tasks, they did not know where the recording was coming from. D7's quote summarized what we heard from study participants: *"I did not understand where the image was coming from. Then I said "Oh, it's the drone." It took me two seconds or one second, but*

I was disoriented in a way. Yes. I felt like I was being watched. It just put it on my face that I was being watched."

Six *drone group* participants felt that the discomfort at being under drone surveillance was because in comparison to a video camera, the drone's camera was smaller and *"obscure"*, and less obvious (D10). Other participants felt that the drone's larger size made it obvious when it was recording since the drone itself is hard to hide *"in such way that it's not going to draw attention to itself."*. (D5).

In general, *drone group* participants felt that the drone recording was very clandestine, similar to a *"hidden camera"* (D4), since there was no indication of recording. Participants again expressed feelings of being watched despite its inability to be discrete due to its size and flying ability.

The *non-drone group* also mentioned the invisibility of the camera, and the camera's limited view of its surroundings. For instance, some participants assumed the camera usually sits near the rotors but the camera on our drone was protruding out in the front. Others also talked about not knowing whether the camera was oriented in their direction since it is not clearly marked. ND10 explained how drones compared to his GoPro camera: *"I can know that [the GoPro] is pointing at me. I can know that it is actually looking the way the [operator] is looking. A drone, I'm not sure whether it is looking from the top, whether it is looking from the bottom, whether it is not even looking at me. If it is a drone, then I'm not sure where it is recording, at what angle it is recording."* Participants also indicated a limited view of what the operator can see remotely meaning that the drone could have potential crashes.

Camera Quality: Participants' privacy and security concerns were also related to the quality of the drone's camera. Four of our *drone group* participants were surprised by the camera quality. D3 *"thought it'd be grainy."* At least two felt the camera and video quality were not as advanced as expected. Another concern raised by four *drone group* participants was about the drone having zooming capabilities that could compromise privacy as D7 explained :*"If it has those things, then it can be even more invasive. You can lift it up, and if you're in the National Mall, just zoom into the White House."*. On the other hand, at least four *drone group* participants felt less concerned about privacy after the experiment because they felt that the drones could not zoom in from high altitudes. Four out of ten *non-drone group* participants also brought up concerns regarding drone camera zoom capabilities. All participants wanted to limit the camera quality to mitigate privacy and security concerns around drones' recording data.

Data Recording and Storage Vulnerability: We showed participants the footage captured throughout the experiment on our laptop. Participants had mixed emotions. Most of the *drone group* (8/10) and *non-drone group* (6/10) had concerns about either the way that the drone stored information or the recording process itself. At least two *drone group* participants who talked about the storage of the data mentioned concern about the ease of access of the data. In typical examples, D8 felt this could make distribution of the footage easier which could be a good or bad thing. D6 elaborated that it was scary when the data recorded by the drones was *"Not being clear in terms of how it's regulated, where it's being stored, who's using it, how vulnerable it is."*. Some liked that the recordings could be processed at a later time to when the data was recorded.

Interestingly, participants noticed that the drone did not record sound in our study. The three *drone group* participants who noticed the lack of sound in the recording attributed it to the noise produced by the drone rendering a mic useless. Some felt that a sensitive mic could reconstruct the audio despite the noise. This elevated concerns about drones invading privacy.

Non-drone group participants who were not concerned about the drone's data capture and storage were either familiar with the process, or thought it made sense since it happens with other recording devices. Four *drone group* and the majority of *non-drone group* (6/10) participants said the owner of the drone owns the footage, regardless of who was captured in media. Only one *non-drone group* participant said that that the owner of the drone should not have the rights to the data. Three *drone group* and only two *non-drone group* participants said that the subjects either own or should have a say in the ownership and use of the data. The rest of the *drone group* either did not know (2/10) or said that the media belongs to the registrant of the drone, not necessarily the owner.

Drone Feedback Lights: Compounding privacy concerns, in our experiment, we noted that not all participants saw the drone's feedback lights at first or knew how to decipher them. Half of the *drone group* participants did not notice blinking lights in Task 5 and the other half noticed some or all of the lights changing colors from red to green. Participants who did see the lights in general did not know why the lights were changing. Three *drone group* participants thought that the lights indicated a coding error or malfunction. Others wondered if the lights indicated direction of travel. Participants felt that the lights were a good indicator if something was not right with the drone but agreed that the meaning of the lights were not easy to decipher without a manual.

The *non-drone group* participants could not see the feedback lights blinking but were shown the task card illustrating the concept. These participants had similar concerns to those who interacted with the real drone. Most of the *non-drone group* participants (7/10) were not concerned with the blinking lights, and most thought that it was *"changing colors"* (ND2). Only three *non-drone group* participants hypothesized that blinking lights signaled an issue with the drone, that it was tracking something, or that there was a problem within its vicinity. Thus, the lack of visibility of drone feedback increased privacy and security concerns about knowing when a drone was recording, in violation of regulations, or malfunctioning.

DISCUSSION

Our findings suggest that participants' perceptions of privacy and security issues around drones are similar to those indicated in previous studies [10, 22, 19, 39] but also that there are many more negative perceptions of drones than prior works suggest. In addition, our study demonstrates how the drone design itself affects privacy and security concerns around drones.

We make three recommendations based on our findings: geo-fencing, creating designated spaces for drones, and enhancing the design of drones to mitigate privacy and security concerns. We also outline study limitations and future work.

Geo-Fencing Using Existing Infrastructures

Our participants did not want drones to be near people, buildings, other drones, and wildlife to maintain their privacy and physical security. While current FAA regulations restrict drone flight to 5 miles away from airports, there is nothing preventing an operator from overstepping these rules aside from "good faith". To properly mitigate these privacy and security concerns, we recommend that geo-fencing [17] could be used to prevent drones from getting too close to places such as schools, government buildings, landmarks, or wildlife areas. Geo-fencing for drones is not a new idea. For example DJI prevented its' drones from near airports in 2015 [12]. However, without regulations backing geo-fences, they may not ultimately be effective. For instance, a startup called NoFlyZone [9] wanted to erect geo-fences against drones around public residences but failed because drone manufacturers did not feel the need to participate in the service or implement geo-fencing technologies in their drones. Effective geo-fencing would thus require revised drone regulations to mandate that drone manufacturers implement geo-fencing technologies and methods to ensure that drones have up to date built-in geo-fencing mechanisms.

Another route to make effective geo-fences against drones is to exploit existing infrastructures such as home networks to help create low-cost virtual drone barriers, given recent developments in Wi-Fi positioning [11]. For example, when a Wi-Fi network is detected by a Wi-Fi enabled drone, the drone could limit its distance from the router, and the network owner could also be alerted of nearby drones. This kind of technique would not only mitigate privacy and security concerns but it would allow users to better track drones in their vicinity.

Designated Spaces for Drones

Our participants were also worried about widespread drone usage and having multiple drones in an area potentially causing harm from drone to drone collisions, and to protect their privacy from drone recordings. Participants also voiced concerns about not being able to easily identify an out of sight drone operator as raised in prior works [39]. To address these concerns, one possibility for future work would be to explore how drones could operate in designated spaces or drone "highways". These spaces would allow people to easily identify drones and their operators at a distance, protect people physically from drones by having them in a separate space, and mitigate privacy concerns by having drones at a distance from 'private' spaces. Fully exploring this option requires careful consideration of how to make these spaces cost-effective and an overhaul of current regulations that are not well suited to handling multiple drones in an area.

Drone Design and Privacy and Security Perceptions

Our findings between the two study groups were similar but we found that the *drone group* perceived sound and wind as threatening drone attributes more than the *non-drone* group. The *drone group* was also more concerned about the uncertain location of the camera, especially when asked to disclose personal information. By comparison, *non-drone* participants were more comfortable disclosing their personal information around the model drone. Both groups also commented on sound and wind being privacy enhancers because of hearing a drone before seeing it. These findings suggest that future drone designs should explore the use of non-visual cues and recording feedback to enhance users' privacy and security.

Towards "Friendly" Drones

Our study also showed that participants perceived drones as threatening and unsafe and that participants were concerned about potential payload due to the drone's color, shape, and size. These findings suggest that a drone's appearance and features can be manipulated to enhance perceived privacy and security and to make people more wary of certain drones. We suggest that drone designers carefully consider the use of colors, logos, and decorations to make drones *"friendly"*, or *"unfriendly"* in cases where it is necessary for people to keep their distance from certain drones. Drone sizes could be balanced to ensure that they are not perceived as too stealthy or concealing dangerous items. Some of our participants even suggested that circular drones would be less threatening, which aligns with previous work in human robot interaction suggesting that the shape of the robot can influence human perceptions [34]. Similarly, stabilizing or carefully engineering [6] *"friendly"* drone movements can help people perceive the drone as friendly and/or safe or vice versa. Finally, to help protect wildlife, we also suggest that drones could be designed with visual or audio animal repellents.

Limitations and Future Work

Our study is limited to a small sample of the student population at our institution with about average privacy and security concerns and behavior intentions. Moreover, our study exposed users to drones indoors which may have amplified the effects of sound and wind, although participants mentioned these issues even when talking about drones they encountered outdoors. Future work should survey a larger more representative sample of the US population to see how our findings generalize. Also, we did not ask participants about or demonstrate an exhaustive set of scenarios of drone usage or drone types, or use a drone outdoors. These situations can be addressed in future studies.

CONCLUSION

We conducted a laboratory study with 20 university participants where users interacted with a drone or model drone to elicit privacy and security concerns around drones and drone regulation in the US. We found similar privacy and security concerns exist around drones to prior studies but that users also hold many negative perceptions around drones that were not covered in prior works. We also found that the drone design itself shapes privacy and security concerns and attitudes towards drone regulation. We recommend investigating how to make effective use of geo-fences, designated spaces for drones, and drone design to enhance positive drone perceptions and better protect users' privacy and security from drones. Future work will tackle these open questions.

REFERENCES

1. Maria de Fatima Bento. 2008. Unmanned aerial vehicles: an overview. *Inside GNSS* 3, 1 (2008), 54–61.
2. Philip Boucher. 2015. 'You Wouldn't have Your Granny Using Them': Drawing Boundaries Between Acceptable and Unacceptable Applications of Civil Drones. *Science and Engineering Ethics* (2015), 1–28. DOI: http://dx.doi.org/10.1007/s11948-015-9720-7
3. Tom Buchanan, Carina Paine, Adam N. Joinson, and Ulf-Dietrich Reips. 2007. Development of Measures of Online Privacy Concern and Protection for Use on the Internet. *J. Am. Soc. Inf. Sci. Technol.* 58, 2 (Jan. 2007), 157–165. DOI:http://dx.doi.org/10.1002/asi.v58:2
4. Eric Baldwin Carr. 2013. Unmanned aerial vehicles: Examining the safety, security, privacy and regulatory issues of integration into US airspace. *National Centre for Policy Analysis (NCPA). Retrieved on September* 23 (2013), 2014.
5. Jessica R. Cauchard, Jane L. E, Kevin Y. Zhai, and James A. Landay. 2015. Drone & Me: An Exploration into Natural Human-drone Interaction. In *Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp '15)*. ACM, New York, NY, USA, 361–365. DOI: http://dx.doi.org/10.1145/2750858.2805823
6. Jessica Rebecca Cauchard, Kevin Y. Zhai, Marco Spadafora, and James A. Landay. 2016. Emotion Encoding in Human-Drone Interaction. In *The Eleventh ACM/IEEE International Conference on Human Robot Interaction (HRI '16)*. IEEE Press, Piscataway, NJ, USA, 263–270. http://dl.acm.org.proxy-um.researchport.umd.edu/citation.cfm?id=2906831.2906878
7. D. Cavett, M. Coker, R. Jimenez, and B. Yaacoubi. 2007. Human-Computer Interface for Control of Unmanned Aerial Vehicles. In *2007 IEEE Systems and Information Engineering Design Symposium*. 1–6. DOI: http://dx.doi.org/10.1109/SIEDS.2007.4374014
8. Ann Cavoukian. 2012. *Privacy and drones: Unmanned aerial vehicles*. Information and Privacy Commissioner of Ontario, Ontario, Canada.
9. Ethan Chiel. 2016. The Service That Promised to Keep Drones Away From Your Home Silently Shut Down. (2016). http://fusion.net/story/305654/noflyzone-no-fly-zone-drone-shuts-down/
10. Reece A Clothier, Dominique A Greer, Duncan G Greer, and Amisha M Mehta. 2015. Risk perception and the public acceptance of drones. *Risk analysis* 35, 6 (2015), 1167–1183.
11. Adam Conner-Simons. 2016. Wireless tech means safer drones, smarter homes and password-free WiFi. (2016). Retrieved from https://news.mit.edu/2016/wireless-tech-means-safer-drones-smarter-homes-password-free-wifi-0331.
12. *DJI Geo System*. http://www.dji.com/flysafe/geo-system
13. Serge Egelman and Eyal Peer. 2015. Scaling the Security Wall: Developing a Security Behavior Intentions Scale (SeBIS). In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15)*. ACM, New York, NY, USA, 2873–2882. DOI: http://dx.doi.org/10.1145/2702123.2702249
14. FAA. 2016. FAA Aerospace Forecasts. (2016). Retrieved September 13, 2016 from https://www.faa.gov/data_research/aviation/aerospace_forecasts/.
15. Federal Aviation Administration 2016a. B4UFLY Smartphone App. (2016). Retrieved September 13,2016 from https://www.faa.gov/uas/where_to_fly/b4ufly/.
16. Federal Aviation Administration 2016b. Unmanned Aircraft Systems. (2016). Retrieved September 13,2016 from https://www.faa.gov/uas/.
17. Dan Gettinger and Arthur Holland Michel. 2015. Drone sightings and close encounters: An analysis. (2015). Retrieved September 13,2016 from http://dronecenter.bard.edu/files/2015/12/12-11-Drone-Sightings-and-Close-Encounters.pdf.
18. Eberhard Graether and Florian Mueller. 2012. Joggobot: A Flying Robot As Jogging Companion. In *CHI '12 Extended Abstracts on Human Factors in Computing Systems (CHI EA '12)*. ACM, New York, NY, USA, 1063–1066. DOI: http://dx.doi.org/10.1145/2212776.2212386
19. Kerry G Herron, Hank C Jenkins Smith, and Carol L Silva. 2014. US Public Perspectives on Privacy, Security, and Unmanned Aircraft Systems. (2014). Retrieved September 13, 2016 from http://crcm.ou.edu/pvcy2014/report.pdf.
20. Keita Higuchi and Jun Rekimoto. 2013. Flying Head: A Head Motion Synchronization Mechanism for Unmanned Aerial Vehicle Control. In *CHI '13 Extended Abstracts on Human Factors in Computing Systems (CHI EA '13)*. ACM, New York, NY, USA, 2029–2038. DOI: http://dx.doi.org/10.1145/2468356.2468721
21. Hyun Young Kim, Bomyeong Kim, and Jinwoo Kim. 2016. The Naughty Drone: A Qualitative Research on Drone As Companion Device. In *Proceedings of the 10th International Conference on Ubiquitous Information Management and Communication (IMCOM '16)*. ACM, New York, NY, USA, Article 91, 6 pages. DOI: http://dx.doi.org/10.1145/2857546.2857639
22. Chantal Lidynia, Ralf Philipsen, and Martina Ziefle. 2017. *Droning on About Drones—Acceptance of and Perceived Barriers to Drones in Civil Usage Contexts*. Springer International Publishing, Cham, 317–329. DOI: http://dx.doi.org/10.1007/978-3-319-41959-6_26
23. A. Mashood, H. Noura, I. Jawhar, and N. Mohamed. 2015. A gesture based kinect for quadrotor control. In *Information and Communication Technology Research (ICTRC), 2015 International Conference on*. 298–301. DOI:http://dx.doi.org/10.1109/ICTRC.2015.7156481

24. Mikhail Matrosov, Olga Volkova, and Dzmitry Tsetserukou. 2016. LightAir: A Novel System for Tangible Communication with Quadcopters Using Foot Gestures and Projected Image. In *ACM SIGGRAPH 2016 Emerging Technologies (SIGGRAPH '16)*. ACM, New York, NY, USA, Article 16, 2 pages. DOI: http://dx.doi.org/10.1145/2929464.2932429

25. Robert Molko. 2012. The Drones Are Coming! Will the Fourth Amendment Stop Their Threat to Our Privacy? *Will the Fourth Amendment Stop Their Threat to Our Privacy* (2012).

26. *A node.js client for controlling Parrot AR Drone 2.0 quad-copters*. Retrieved from https://github.com/felixge/node-ar-drone.

27. *Parrot AR.Drone 2.0*. https://www.parrot.com/us/drones/parrot-ardrone-20-power-edition.

28. Erika Shehan Poole, Marshini Chetty, Rebecca E. Grinter, and W. Keith Edwards. 2008. More Than Meets the Eye: Transforming the User Experience of Home Network Management. In *Proceedings of the 7th ACM Conference on Designing Interactive Systems (DIS '08)*. ACM, New York, NY, USA, 455–464. DOI: http://dx.doi.org/10.1145/1394445.1394494

29. Chris Schlag. 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 (2012), i.

30. Irving Seidman. 2013. *Interviewing As Qualitative Research: A Guide for Researchers in Education and the Social Sciences*. Teachers college press.

31. Manya Sleeper, Sebastian Schnorf, Brian Kemler, and Sunny Consolvo. 2015. Attitudes Toward Vehicle-based Sensing and Recording. In *Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp '15)*. ACM, New York, NY, USA, 1017–1028. DOI: http://dx.doi.org/10.1145/2750858.2806064

32. Jay Stanley and Catherine Crump. 2011. *Protecting Privacy from Aerial Surveillance: Recommendations for Government Use of Drone Aircraft: Report*. American Civil Liberties Union, Washington,D.C.,USA.

33. David Stuckenberg and Stephen Maddox. 2014. Drones in the US National Airspace System. *International Journal of Aviation Systems, Operations and Training (IJASOT)* 1, 2 (2014), 1–22.

34. Ja-Young Sung, Lan Guo, Rebecca E. Grinter, and Henrik I. Christensen. 2007. "My Roomba is Rambo": Intimate Home Appliances. In *Proceedings of the 9th International Conference on Ubiquitous Computing (UbiComp '07)*. Springer-Verlag, Berlin, Heidelberg, 145–162. http://dl.acm.org/citation.cfm?id=1771592.1771601

35. Teal Group Corporation 2016. Teal Group Predicts Worldwide Civil UAS Production Will Total $65 Billion in Its 2016 UAS Market Profile and Forecast. (2016). Retrieved September 15, 2016 from http://www.tealgroup.com/index.php/about-teal-group-corporation/press-releases/.

36. Richard M Thompson II. 2015. *Domestic Drones and Privacy: a primer*. Vol. 43965. Congressional Research Service.

37. W Gregory Voss. 2013. Privacy law implications of the use of drones for security and justice purposes. *International Journal of Liability and Scientific Enquiry* 6, 4 (2013), 171–192.

38. Tyler Wall. 2013. Unmanning the police manhunt: Vertical security as pacification. *Socialist Studies/Études Socialistes* 9, 2 (2013).

39. Yang Wang, Huichuan Xia, Yaxing Yao, and Yun Huang. 2016. Flying Eyes and Hidden Controllers: A Qualitative Study of People's Privacy Perceptions of Civilian Drones in The US. *Proceedings on Privacy Enhancing Technologies* 2016, 3 (2016), 172–190.