Yang Wang*, Huichuan Xia, Yaxing Yao, and Yun Huang

Flying Eyes and Hidden Controllers: A Qualitative Study of People's Privacy Perceptions of Civilian Drones in The US

Abstract: Drones are unmanned aircraft controlled remotely or operated autonomously. While the extant literature suggests that drones can in principle invade people's privacy, little is known about how people actually think about drones. Drawing from a series of in-depth interviews conducted in the United States, we provide a novel and rich account of people's privacy perceptions of drones for civilian uses both in general and under specific usage scenarios. Our informants raised both physical and information privacy issues against government, organization and individual use of drones. Informants' reasoning about the acceptance of drone use was in part based on whether the drone is operating in a public or private space. However, our informants differed significantly in their definitions of public and private spaces. While our informants' privacy concerns such as surveillance, data collection and sharing have been raised for other tracking technologies such as camera phones and closed-circuit television (CCTV), our interviews highlight two heightened issues of drones: (1) powerful yet inconspicuous data collection, (2) hidden and inaccessible drone controllers. These two aspects of drones render some of people's existing privacy practices futile (e.g., notice recording and ask controllers to stop or delete the recording). Some informants demanded notifications of drones near them and expected drone controllers asking for their explicit permissions before recording. We discuss implications for future privacy-enhancing drone designs.

Keywords: Drone; UAV; tracking; perceptions; privacy.

DOI 10.1515/popets-2016-0022
Received 2015-11-30; revised 2016-03-01; accepted 2016-03-02.

1 Introduction

1984. Small flying machines rove around Airstrip One where Winston Smith lives, and peek through the windows [49].

2015. A small flying machine crashed in the White House where the US President Barack Obama lives [33].

***Corresponding Author: Yang Wang:** SALT Lab, School of Information Studies, Syracuse University, E-mail: ywang@syr.edu
Huichuan Xia: Syracuse University, E-mail: hxia@syr.edu
Yaxing Yao: Syracuse University, E-mail: yyao08@syr.edu
Yun Huang: Syracuse University, E-mail: yhuang@syr.edu

The flying machine that George Orwell imagined in his classic novel 1984 and that crashed in the White House lawn is known as *drones*. The Merriam-Webster dictionary defines a drone as "an unmanned aircraft or ship guided by remote control or onboard computers." Drones are sometimes known as Unmanned Aerial Vehicles or Unmanned Aircraft Systems.

As Figure 1 illustrates, drones often carry cameras to take pictures or record videos. Originally designed for military purposes, this technology has been increasingly adopted for non-military uses. For instance, drones are used to cover ongoing events for journalism [51], record birthday parties [34], deliver packages to customers (e.g., Amazon Prime Air [4]), and to assist police in patrolling and investigation [32].

In this paper, we focus on lightweight drones with operators for civilian uses including public (governmental, e.g. police), civil (non-governmental, e.g., commercial), and recreational (a.k.a, model aircraft) purposes [20]. This type of drones dominates the consumer market and can have broad and emergent impact on ordinary citizens. While no official drone sales data is available, the Consumer Electronics Association (CEA) estimated that 700,000 drones were sold in 2015 in the US [14]. From now on, we use the term drones to denote this type of drones unless specified otherwise.

Because of drones' small sizes and capabilities in flying and taking high-definition images and videos, government agencies, policy makers, consumer advocacy groups, and legal scholars have raised serious concerns about drones' usage. For instance, the US Federal Aviation Administration (FAA) is tasked to devise rules for drone use by 2015. Ann Cavoukian, the Privacy Commissioner of Ontario, Canada, has advocated that designers should adopt a *Privacy by Design (PbD)* approach from the beginning of the drone design process to protect people's privacy [12]. Legal scholars have raised ethical and privacy concerns regarding the use of drones (e.g., [6]).

However, the extant literature mostly from legal scholarship focuses on conceptual analyses of drones and their im-

Fig. 1. A DJI Phantom 2 Vision+ drone that we used in our study

plications. There is a lack of empirical studies that examine people's perceptions of this emerging technology with one exception being a recent survey study of Australian citizens' perceptions of drones [13]. However, little is known about how people in the US feel about drones, particularly around privacy. Understanding people's privacy perceptions is integral in informing future privacy-friendly drone design and regulation. Our research aims to fill this critical gap.

During June to August 2015, we conducted 16 semi-structured interviews to examine people's perceptions of drones. To help our informants get familiar with this technology, we showed them a real drone (see Figure 1) and illustrated its capabilities in flying and taking pictures and videos before the actual interviews. In each interview, we solicited our informants' general perceptions of drones as well as their perceptions under five specific usage scenarios that we adopted from drones' existing real-world uses. We also asked them to compare drones with two tracking/recording technologies that they are already familiar with, smart phones with cameras and closed-circuit television (CCTV), as frames of reference. Lastly, the informants were asked about what kinds of notifications and controls they would expect from drones operated by others as well as what aspects of drones should be regulated.

Our results suggest that our informants had mixed feelings about drones. On one hand, they saw clear values in drones as they identified many benefits and promising applications of drones. On the other hand, they also raised a multitude of safety, security and privacy issues. Our informants were not only concerned about the drones per se, but also the drone controllers that are often invisible. Drawing from Orlikowski's conceptualization of duality of technology, we highlight the *duality* of drones, suggesting that drone design and regulation should consider both drones and their controllers.

This paper makes three contributions. First, we provide a detailed account of people's privacy perceptions of civilian drones. Second, we highlight the *duality* of drone and its value in unpacking people's privacy perceptions of drones. Third, we discuss implications for privacy-enhancing drone designs.

2 Related Work

To situate our work in the literature, we review three lines of related research: (1) people's privacy perceptions of tracking/recording technologies, (2) challenging issues of drones, and (3) privacy mechanisms for drones.

2.1 Perceptions of tracking technologies

Since drones are usually equipped with cameras, they can be classified as tracking/recording technologies. The only user study of drones that we are aware of is a recent survey study of Australian public's perceptions of drones [13]. Overall, the respondents did not consider drones to be overly beneficial or risky [13]. However, some respondents (less than one fifth) did raise a general privacy concern about drone surveillance or spying [13]. Prior studies have identified people's privacy concerns over other tracking and recording technologies. For instance, based on interview and survey data, Nguyen and Hayes suggest that people are concerned about leaking personal information about themselves with institutional and end-user tracking and recording technologies, such as credit cards, store loyalty cards, and store video cameras [43].

In studying Internet users' perceptions of online tracking and online behavioral advertising (OBA), McDonald and Cranor find that while people accept that free online content needs advertising, they reject the idea that they need to give up their data for that exchange [42]. Ur et al. show that people have a conflicting sets of opinions towards OBA, describing it as smart, useful, scary, and creepy [61].

Felt et al. find that mobile phone users have varied yet strong privacy concerns in using their phones, particularly, the potential tracking and leakage of their text messages, e-mails, and photos stored in the phones. Users ranked highest risks in using their mobile phones as all contact information being deleted and messages or calls being sent out by malware without their awareness [21]. Tsai et al. show that people also have privacy concerns in using location-sharing technologies, but their concerns vary across different scenarios [60].

Moving on to the physical world, results from a survey conducted shortly after 9/11 show that the majority of respondents approved expanded use of camera surveillance (CCTV) in public [64]. Angeles has found that people have varying level of privacy concerns over the use of Radio-Frequency Identification (RFID) tags [5]. In particular, less information-sensitive people will favor the benefits from RFID more, and will be more willing to buy and pay more to RFID tagged products; whereas more information-sensitive people are more concerned about their privacy with RFID [5].

Prior research has also explored people's perceptions of wearable devices (e.g., glasses or cameras). Hong suggests that since most people have little experience with wearable devices (e.g., Google Glass) before, their perceived value and perceived risks of these devices may change over time [28]. In a study of Augmented Reality (AR) glasses, Denning et al. find that people expect giving their permissions before being recorded by AR glasses [16]. When participants compared AR glasses with CCTV or surveillance cameras, they did not in-

dicate any evident difference in their attitudes. They felt that these technologies are always recording in public and that the introduction of AR glasses did not affect their expectations of being exposed to various recording technologies [16].

These wearable devices can also be used for "lifelogging" where photos and/or audio/video recordings are automatically taken by the devices as a person goes about doing his/her daily activities (e.g., SenseCam [26]). Hoyle et al. find that people have many privacy concerns about lifelogging [31]. For instance, they are concerned about sensitive information appearing in the "lifelog," such as their locations or credit card numbers. They are also concerned about the privacy of bystanders since their faces or behaviors may be captured in the "lifelog" [31]. In a follow-up study, Hoyle et al. also discover that "lifeloggers" are motivated to share their "lifelogged" information for impression management purposes [30].

Last but not least, robots when equipped with cameras also have tracking and recording capabilities. Edward Hall proposes proxemics to refer to people's use of space in mediating their contact with others [25]. For instance, if strangers enter into someone's personal or intimate spaces, then the person would feel uncomfortable [25]. Researchers in the field of human-robot-interaction (HRI) have used this concept in studying the interactions and relationships between humans and robots. Studies have found that a robot's form, speed, and height have different degrees of impact on people's perceptions of the robot (e.g., [10]). In a recent study, Butler et al. find that people desire mechanisms to protect their privacy against remotely tele-operated in-home robots [9].

This literature on tracking/recording technologies suggest that people are likely to have privacy concerns with these technologies, but people might have different levels of concerns. People's privacy concerns might also vary across different scenarios. These findings inform us to examine both general and scenario-based privacy perceptions of drones.

2.2 Challenging issues of drones

Besides the Australian user survey of drones [13], the extant literature on drones has largely focused on privacy and security issues from a legal perspective. The legal scholars posit that drones could potentially violate the Fourth Amendment that protects citizens from unreasonable searches and seizures when drones are used for surveillance. Therefore, the Fourth Amendment rights should regulate and restrict drone usage [18]. They also criticize the FAA for not taking more responsibility and initiative in monitoring drone use. For instance, Barbee comments that the potential use and misuse of drones are both considerable and must not be neglected, yet neither the FAA nor the Congress has paid sufficient attention or taken any action to address the relevant challenges, particularly privacy issues [6]. Research has also suggested that drone developers are somewhat aware of the laws but tend to ignore ethical issues. They would default to some legal considerations of privacy based on their justification of whether the subjects would predict that they are being photographed or video recorded by a drone [15]. Other scholars have heightened concerns due to the fact that drones could be cheaper to obtain than before and could be so tiny yet still with high-definition cameras (a.k.a., "dragonfly drones"). Therefore, drones could potentially get even more detailed pictures of the people being monitored and it would be even harder for people to notice the drones and be aware of them being watched [65]. These legal analyses are informative but lack empirical data about privacy perceptions from ordinary citizens, particularly in the US context. Our study aims to provide this type of empirical data.

2.3 Privacy mechanisms for drones

An number of technical mechanisms have been proposed to protect civilians' privacy specifically regarding drones. For instance, to help drone controllers operate drones appropriately, the FAA has developed B4UFLY, a mobile app that helps drone controllers "determine whether there are any restrictions or requirements in effect at the location where they want to fly" [19]. Besides, ordinary citizens can sign up their addresses as part of the no-fly zones for drones which may be incorporated into the firmware or software of drones and/or honored by drone controllers [47]. To provide citizens more information about drones, LightCense is a system that uses flash lights as a drone's ID. People can look up information about the drone by decoding the sequence of lights via a mobile app [40].

As an example of a server-side mechanism, Yoohwan et al. propose using a combination of encryption, access control, and image/video transformation. Specifically, the system would encrypt the images or videos taken by drones and then deliver them to a privacy server. To access these photos or videos, the privacy server would require a shared key. Depending on the privacy policies of the drone's surveillance area, the pictures and videos can be transformed from high-definition to blurring or totally blank out [37].

While our present research does not design a specific privacy-enhancing mechanism for drones, our study can offer insights to inform future designs of such mechanisms.

3 Methodology

From June to August 2015, we conducted 16 in-person interviews to explore people's privacy perceptions of drones in Syracuse, New York (US). Each interview took about 1 hour with a study compensation of $10. This study was approved by our University IRB.

3.1 Participants

To recruit a diversified set of informants, we posted study fliers and randomly invited adults in public places such as university campus, streets, and parks, to participate in our study. Half of our informants were male, and the other half were female. Their ages ranged from 18 to 62 years old with an average of 29. Our informants represented various ethnic backgrounds, such as White Americans, African Americans, Latino Americans, and Asian Americans. The majority of them were university students, but we also had a news reporter, a student counselor, an office administrator, and a retired worker.

3.2 Interview protocol

To help our informants get familiar with drones, we used a DJI Phantom 2 Vision+ drone as a prop in our interviews (see Fig 1). This drone has a HD camera and can provide live video feed via a dedicated mobile app.

Each interview was structured as follows. First, before the interview, we showed our informants the physical drone and explained in details how the drone could be controlled to fly and take pictures/videos. If the weather permitted (e.g., not too windy or rainy), we also flew the drone in front of the informant. We also encouraged our informants to ask any questions about drones before formally starting the interview. This kind of in-situ investigation could give informants a more realistic impression about the technology and would be more natural to probe people's perceptions, particularly when people are not very familiar with the technology [16].

Specifically, our interview protocol consists of three parts: (1) general questions about people's perceptions of drones; (2) context-based questions about people's attitudes towards drones under different scenarios; and (3) questions about specific aspects of drones, such as comparisons between drones and camera phones or CCTV as well as expected notice, control, and regulation of drones. The interview questions are included in the Appendix A. Using a semi-structured interview approach, we also asked follow-up questions to continue any interesting discussion.

3.2.1 General questions about drones

We began our interview with general questions to explore informants' understanding of and attitudes towards drones. For instance, we asked questions such as, "Have you heard of drones? What is the first thing that comes to your mind when you hear about drones? How do you feel about drones? Do you see any benefits or issues of drones?"

These questions were mainly adapted from two prior studies on Online Behavioral Advertising (OBA) [62] and Augmented Reality (AR) Glasses [16], respectively. We chose to build on these two studies for a few reasons. First, both studies conducted interviews with ordinary citizens in the US. Second, at the time of the studies, OBA and AR Glasses were trendy and somewhat controversial technologies which ordinary people might not have much knowledge or experience. Third, drones, OBA and AR Glasses all can be used to support or benefit people's lives as well as to track people and potentially invade people's privacy.

We also asked informants to compare drones with two widely used and known tracking/recording technologies, smart phones with cameras and closed-circuit television (CCTV), as frames of reference. This comparison between drones and more familiar technologies was inspired by a pioneering study of risk perception [22]. The main reason we chose camera phones and CCTV is that since they are widely used, ordinary citizens are likely to be *familiar* with them so they can be used as references. We did not choose RFID, Google Glass, or other wearable cameras (e.g., SenseCam [26]) because people may be unfamiliar with them just as drones.

3.2.2 Scenario-based questions

There are both theoretical support and empirical evidence that privacy is contextual. For example, Helen Nissenbaum eloquently points out that human behaviors, e.g., a transaction that occurs, is always situated in some concrete context, e.g., certain geographical area and specific constituted norms within a political, cultural environment [45]. As we discussed in the related work, prior privacy studies have also shown that people's privacy preferences of technologies can vary significantly under different contexts or scenarios (e.g., RFID [52], location-sharing systems [60]). These studies motivate us to develop different scenarios and understand people's context-based privacy perceptions of drones under these scenarios.

We created and presented five specific and realistic drone usage scenarios. We asked our informants if they would accept the drone usage for each scenario and why. We adopted news reports of real-world drone usages in creating the five scenarios: a drone is being used in (1) recording a promotion

event that you attend in a shopping mall by a store owner [66]; (2) delivering goods to you by Amazon [4]; (3) recording a friend's party that you attend [34]; (4) reporting a parade that you attend by a news agency [51]; and (5) searching lurking criminals around your residential area by the local police [32]. These scenarios covered a diverse set of contexts, including indoor use (mall) vs. outdoor use (parade); private home (party) vs. public area (parade); the drone controlled by individuals (friend), the government (police), or a vendor (Amazon); and the drone use benefiting self (goods delivery), other people (friend), or other entities (mall).

3.2.3 Expected notification and control

To help inform future drone design and regulation, we also asked informants about what kinds of notifications and controls they would expect and what aspects of drones should be regulated. Specifically, we asked questions, such as "do you expect to be notified about the time periods during which drones can/will be operated" and "do you expect to be notified about the types of information that the operating drones might collect?" These questions were inspired by the *Drone Aircraft Privacy and Transparency Act of 2013*, which was proposed but not enacted in the US. We also asked questions about expectations of consent and control, such as "do you expect to be asked for any kind of 'explicit consent' to allow drones to fly near you" and "do you expect to see detailed explanations if a drone takes pictures or videos that can capture you?" These questions were adapted from a study on RFID [29].

3.3 Data analysis

We audio recorded all the interviews upon informants' permissions. We also took notes during the interviews. The interviews were then transcribed and analyzed qualitatively. In general, qualitative research or analysis is particularly useful in exploring the why and how questions of a social phenomenon. Qualitative research usually does not claim representative results in the statistical sense but allows researchers to make propositions that can be further investigated by quantitative methods such as surveys or experiments.

In our case, we conducted a *thematic analysis*, which is common for qualitative research [7]. Thematic analysis is "a method for identifying, analysing, and reporting patterns (themes) within data" [8]. First, we immersed ourselves in the data by carefully reading through the interview transcripts, actively looking for and taking notes of meanings and patterns.

Second, two co-authors (coders) used ATLAS.ti, a popular qualitative analysis software, to manually and independently generate initial codes that capture meanings of the same subset of our interview data at a fine-grained level (usually at the sentence level). These codes are considered as the most basic elements of the phenomenon under our study. Then, the two coders convened, discussed, and converged their codes into a code book of 132 unique codes ranging from individual drone features (e.g., cameras) to usage of drones (e.g., parcel delivery) to concerns of drones (e.g., stalking). Next, the two coders used the agreed-upon code book to code the interview data. ATLAS.ti allows us to identify and extract all excerpts associated with a given code. For instance, one interview quote for the code "public space" is "*everyone is free to go in and out of that place whenever they want to and they're basically free to do whatever they want unless it's against the law.*"

Third, we explored how different codes can be merged into high-level themes. We grouped 132 codes into nine candidate themes: drone features, drone usage, attitudes towards drones, cultural differences, private vs. public space, privacy concerns, safety concerns, and drone control. For instance, the theme of drone control included the following codes: notification, accessible to everyone, actions to protect people, controller flexibility, delete recordings afterwards, destination of Information, expected control, know controller, sound of drones, time to fly, and regulations. We wrote codes on colored post-it notes and sorted them into groups/themes on a wall, creating an affinity diagram [36].

Fourth, we reviewed the candidate themes by reading the interview excerpts of each theme to see whether they coherently present the underlying theme. We then adjusted the themes and our affinity diagram accordingly. For instance, the code "battery life" was originally part of the theme of drone features. After reviewing the interview quotes associated with the code "battery life" (e.g., "*they should know if it's safe or not to use and I don't know if they use batteries*" and "*And again it could run out of batteries*"), we moved this code to the theme of safety. Figure 2 shows the final affinity diagram.

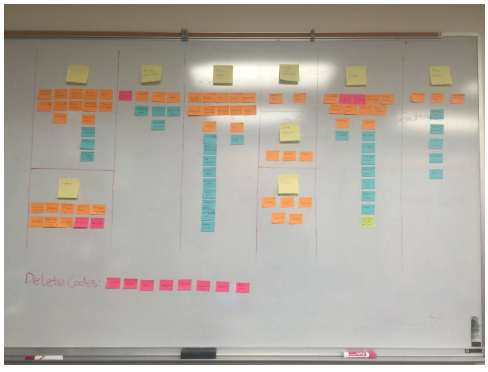

Fig. 2. The final affinity diagram of the themes and their codes.

4 Findings

In this section, we report the major themes emerged from our study. We will use fictitious names for our informants.

Our informants suggested a number of perceived benefits of drones. When asked about potential benefits or applications of drones, our informants focused on a few characteristics of drones, such as their relatively small size, agility, and capabilities to fly and to take high-definition photos and videos in inaccessible or even dangerous environments. They envisioned several drone applications, such as aerial photography, goods delivery, and emergency responses.

Our informants also raised several issues of drone usage related to safety, security, and privacy concerns. Their safety concerns mainly revolved around drones hitting people or interfering with other aircraft. The informants attributed these risks to two sources: the components and/or features of drones (e.g., propellers), and drone controllers' inappropriate or reckless behaviors. Closely related to the safety issues, our informants also brought up concerns about security issues, mainly about drones trespassing on some forbidden or sensitive places such as government or military facilities. When drones encroach on personal spaces which individual informants defined for themselves, a sense of privacy violation arose.

4.1 General privacy concerns

Privacy was a salient and consistent topic across all of the interviews, regardless of the diverse ethnic or occupational backgrounds of our informants. Their discussions about the privacy implications of drones centered around the following themes: (1) the definitions and boundaries of public vs. private spaces, (2) peeking and stalking, and (3) recording and sharing of photos and videos without people's awareness and/or consent. These concerns were related to both their *physical* privacy and *information* privacy. Informants' physical privacy concerns were primarily about the feeling that their private spaces would be intruded by drones. This sense of physical privacy intrusion is similar to when an individual's personal space is invaded by a stranger [24]. In terms of information privacy concerns, our informants were mainly concerned about the collection, use, and sharing of their personal data, such as their locations and pictures/videos that capture them.

4.1.1 Public vs. private spaces

Due to drones' flexibility and mobility, they could intrude into people's private space, compromising people's physical privacy. Territoriality (public vs. private spaces) is a key factor that our informants considered in determining their expectations of privacy and the privacy violations of drones. There was a general consensus among our informants that if a drone takes pictures or records video or even just flies in a *private space*, then the drone would be considered as invading the residents' privacy. While intuitive, this view begs an important question - what is considered a private space? Our informants had various definitions of private space and these definitions centered around three factors: ownership of the space, sensitivity of the space, and nature of activity in the space.

Ownership. In general, our informants agreed that their homes (either owned or rent), or personal properties (e.g., a car) are their private spaces. For one group of informants, *ownership* (or temporary ownership such as rental) alone determines private spaces. For instance, Scott (62, retired worker) explained, *"the boundary between public and private space is like a fence of property an individual owns."* Similarly, Bill (25, computer science major) claimed that *"my private space would be my private properties, my home, my rental house, my car, etc. and public space is owned by the government or public administrations, like school, city square, etc."* Dan (27, public relation professional) also focused on ownership: *"like a lot of places outside your own property or where you live is kind of a public space because you don't own it, like a park is a public space."* Emily (18, first year in college) extended her private space beyond her home, explaining *"the surrounding place around my home is still my own private space."* Mary (28, teacher) went to an extreme in saying that *"I just assume the space outside of my house is public space."* For these informants, ownership was reasonably easy to identify and so was their private spaces.

Sensitivity. When a drone operates in a public place, our informants generally felt that the drone is less likely to cause privacy violations. However, some informants effectively treated *sensitive* public places with children or other vulnerable populations as private spaces. For instance, Hannah (19, biology major), who used to assist in an elementary school, considered a school as a private space: *"especially in elementary schools a lot of people don't want their children to be recorded or taking photos of them unless you have the consent of their parents."* This view is compatible with the current US privacy legislation for children, such as the Children's Online Privacy Protection Act (COPPA) which requires the consent from a parent or guardian for collecting personal data about children under 13.

Nature of activity. For some informants, even seemingly non-sensitive public places (e.g., mall) can be their private spaces because of the nature of their activities. For instance, Lily (24, information science major) not only considered the place but also the activity she is engaging in the place at that

time. She elaborated, *"I only regard it a public space when I go to a so-called public area, like a square and in the meantime I am participating in some public event, like a promotion event, or a parade. Otherwise even I am in a public area, I still regard it, particularly my surrounding as my private space."* Lily's viewpoint is related to the notion of proxemics which refers to the personal space (or distance) that people maintain around themselves [25]. Lily desired proxemics against drones even in public places when conducting her personal business.

4.1.2 Peeking and stalking

There were two behaviors of drones that our informants regarded as intrusions to their privacy: peeking and stalking. In terms of peeking, almost all the informants generally loathed being watched or recorded by a drone, peeking through the windows of their private spaces. For instance, Cindy (21, finance major) explained her concern, *"because a drone could fly so high, even if I am living on the top floor of a building, I would still worry that a drone may peek me through the window when I am doing some private things, like taking a bath."* Emily shared the same attitude. She said *"If I'm in my own private home I won't like a drone peeking into my house."* Dan drew an analogy between a drone's peeking and a neighbor's peeking, *"it's the same thing in houses, people don't want the neighbors to peek in. In a society where everything is documented all the time, you know, you don't need another thing adding to that."* By peeking, drones can invade into people's private spaces and lives.

Stalking means that a drone could follow and record an individual's activities. Bill painted a dreadful picture against a backdrop of the current social and cultural landscape in India where he was originally from: *"One concern would be stalking. In India, parents care about their daughter very much, and if they see a drone stalking their daughter, they will be very angry and use every means to find the controller of the drone and punish him, even if the controller is unintentional."* Even perceived or unintentional watching or stalking may lead to revenge and grave consequences. In the US, there were cases where people shot down drones over their backyards [55]. However, Bill's example brought drone controllers to the foreground. They are the ones who will be held accountable for the drones' behaviors.

Mary also denounced stalking or watching and alluded to the problem of the lack of control for drone ownership. She explained, *"there are some very emotionally unstable individuals out there so to have everybody able to own a drone and that I could have some crazy person watching me, yeah that's a problem."* Mary's concern is not unfounded. While the FAA requires licensing of commercial use of drones and registrations of drone controllers, practically anyone can buy a drone for personal use in the US. While the media often focuses on drones' potential use in government surveillance, Mary called attention to misuses of drones by individual controllers.

4.1.3 Recording and sharing

Last but not least, our informants were concerned about drone controllers taking and sharing of photos and videos without people's awareness and/or consent. This concern mainly stemmed from a sense of uncertainty about how drone controllers would collect and use people's information, because a drone can be remotely controlled and can fly out of sight while recording. In other words, both the drone and its controller might be invisible to the people being watched or recorded. Furthermore, people may not be aware of the recording nor have access to or control over the drone recording about them.

Abby (20, environmental science major) explained the invisibility of drones and the lack of awareness and control of the recording, *"People can't tell it's there and will not be aware that they are being watched by such a tiny drone and the footage by drone may be used for whatever purposes without their consent or knowledge."* Abby's concerns pointed to two more fundamental issues: drones' capabilities in capturing pictures or videos of individuals inconspicuously, and bystanders' lack of knowledge of and access to drone controllers.

Dan further highlighted the importance of the drone controller behind the scene, *"drone kind of could be a robot or could be pre-programmed to just like stay in one area all the time so you'd like to know who's behind this and I think that's kind of an important point to raise because people fear what they don't know, so if they don't know who's steering it, that raises some concerns."* Cindy was also concerned about the drone controller and the potential usage of drones' recordings. She elaborated, *"If the person who controls the drone is a person that I don't know, I will be concerned maybe he will use this video to do some other things like put it in the advertisement or yeah, or some illegal things. So I must ensure that the person who controls the drone is someone reliable or the person that I know."* This foregrounding of drone controllers underscores the *duality* of drones. People not only deal with drones but also the people who control the drones. Privacy is deeply relational [59]. Cindy's concern was aggravated or attenuated by the *social relationship* between her and the drone controllers (e.g., strangers or people that she knew).

In addition, the audio part of videos can be another concern. For instance, one informant said "*if you're having a conversation with someone like on the quad and that's still like your own kind of private conversation...well maybe not ever but most of the time I wouldn't want like audio recorded.*"

Lily raised a quite different concern not due to the flights of drones per se but due to pictures being taken by drones and later being posted on the Internet. She explained, *"I know someone immigrated from Afghanistan, and they don't like their pictures being posted on the Internet because they are still in touch with their families, and it's a security issue for them. If they are studying in the university and the tribes are here, (post their pictures on the Internet) will be bad for them."* Lily's example reminds us the privacy and security risks are engendered in their rich social and cultural settings. Exposing people's seemingly public activities such as studying in a US university could potentially put people and their families at risk. The lack of knowledge and control of data collection and sharing by drones paralyzes people's desires and abilities to manage boundaries between themselves and others in achieving the right level of privacy.

4.2 Context-based privacy perceptions

After asking our informants' general perceptions of drones, we then provided five specific drone usage scenarios to further probe informants' context-based privacy perceptions of drones. Our informants' perceptions of drones varied across these scenarios. The differences mainly stemmed from three sources: (1) whether the scenario occurs in a public or private space; (2) what is the intended purpose of the drone usage; and (3) notification and consent of the drone usage.

4.2.1 Scenario 1: shopping mall event monitoring

We described this scenario to our informants, "*Imagine you are in a shopping mall where a promotion event is going on, like on the Black Friday. The store owner decides to use a drone to monitor and record this event, and you happen to be in that event.*"

12 out of 16 informants considered a shopping mall as a public space, and they expressed little concern about being recorded by the drone in this scenario. However, four informants considered shopping mall a private space. For instance, Cindy explained, "*Shopping mall is a relatively private space for me if I go shopping with my intimate friends and I don't want to be audio or video recorded if I am having some private conversation with my friends.*" Again, Cindy's reasoning points to the relational aspect of space, or the social space is characterized by the social relationship therein. The intimate personal relationship makes the space intimate and private.

Several informants expressed that the drone's recordings should be restricted to the promotion event and that the drone should not appear around sensitive areas, such as the dressing room. A few informants would *prefer* to be notified about drone recording, as Emily put it, *"I guess you could like put out some sort of notification to the people...or making people aware that you will be recorded."*

4.2.2 Scenario 2: recording a friend's party

In this scenario, we told our informants, "*Imagine you are at your friend's party, and your friend decides to use a drone to record the party.*" Five informants perceived their friend's party as a public space. For example, Sue held that, *"it is a public setting so I don't really see that would bother me too much."* However, the other 11 informants felt it is something in between. For instance, Cindy said *"I think it's kind of between the private and the public. There are many friends I know so it can be taken as private, but there are lots of people, so I also think of it as public."* This perspective suggests that it is not always a clear cut whether a space is public or private.

Another important factor they considered was the purpose of the recording. Sue commented, *"I could see some concern about that but if you're concerned about your image, you should not consent to go to that party and get drunk in public and anyone can record it."* Grace could accept this scenario if it is for personal use. She explained, *"I think if it's for his personal use I think it's okay because you've shown consent in being in that space and being with other people."*

4.2.3 Scenario 3: delivering goods

We told the informants "*Imagine that Amazon decides to use drones to deliver goods that you have bought in its online store to your house.*" All informants felt that a drone delivering goods would fly close to their home, which was unanimously regarded as their private space. However, most of them felt this drone usage is cool. Dan shared his excitement, *"that's like an efficiency thing, that's making life more convenient and better, and it serves a good purpose and I guess yeah, I think that would be pretty cool, that's a cool way of using technology."* The informants did mention the potential safety risks such as drone crashes. In addition, some informants felt it is not necessary for the drone to carry a camera. For instance, Abby noted that *"I think the drone should have the whole map in its GPS system, you know, you don't have to use the camera."*

Among the five scenarios, our informants expressed the least demand for notification and consent in this scenario perhaps due to its "useful" nature. However, Grace still wanted notifications: *"there should be some sort of disclosure on how it's going to be sent because normally when you purchase something on Amazon you choose your shipping method."*

4.2.4 Scenario 4: reporting a parade

For this scenario, we told the informants "*Imagine you are in a parade. Some news agency decides to use a drone to record the parade.*" In general, our informants were least concerned about this scenario. They all agreed that this scenario occurs in a public space. In addition, all informants except two felt that the drone's recording in this case is acceptable because the purpose is for journalism and if they have already decided to participate this parade, they would rather the parade be recorded and publicized.

However, Mary and Cindy had some reservation. Mary was concerned about her vanity. She explained, *"That's just like vanity...just like wish that I would have done my hair that day so that my appearing on news would be great."* Mary cared about the presentation of herself, a form of impression management practice that Goffman observes [23].

Cindy was more concerned about whether the parade is controversial or not. She elaborated, *"Say I am in a feminist parade. If my face is recorded by the drone and it is put online or in the newspaper, or in other media. The people from the other side, the anti-feminist side, if they meet me later in street, they may revenge me."* This example alludes to the lack of prior notice of and control over drone recordings as well as the potential ramifications. If she had prior notice, she might have reconsidered her participation in the parade.

Our informants mainly requested for prior notice of using their images in news, especially when the images reveal their identities. For instance, Sue (21, biology major) suggested, *"I guess you would need people's permission before you use their face and you know you post their image on website or social network whatever."*

4.2.5 Scenario 5: searching for criminals

We told informants "*Imagine that there are some suspects or criminals lurking in your residential area. The police department decides to use drones to search for these people in your residential area.*" Most informants felt this is acceptable, and some of them even applauded this practice. For instance, Joe (59, newspaper reporter) explained, *"That could be better because a drone could get there immediately even before police car gets to the scene. So I think it will be very useful. If waiting for the police, by the time the police comes, maybe the subjects have already fled away."*

However, three informants considered the surrounding area of their residence as their private space and felt uncomfortable having a drone patrolling around their house, invading their physical privacy. For example, Emily said, *"I would be uncomfortable but I understand why they have it, like if it was in my neighborhood for example, and there was a drone flying around I would be thinking like what's going on."*

Given the recent Snowden revelation of the extensive government surveillance, it is perhaps not surprising to see that most of the informants requested explicit notification and consent for this practice. Bill, articulated his expectation, *"I would like to have explicit information from the police department. Because the home is my private space, having a drone flying above me and recording is like having a policeman watching me around my living place all the time...I don't like to be watched or surveilled by a drone, especially without my permission and prior knowledge."* In Bill's view, the patrolling drone is like a pair of flying eyes watching his life at home.

Many issues that surfaced from these scenarios include physical privacy, purpose of data collection and usage, notice and control. These issues have long been recognized when examining privacy implications in technologies. However, this begs the question: are drones any different from other familiar tracking technologies that have raised similar privacy issues?

4.3 Comparing drones with other familiar tracking technologies

We asked our informants to compare drones with two familiar technologies that have tracking/recording capabilities: smart phone with a camera, and closed-circuit television (CCTV). Our informants pointed out both similarities and differences.

4.3.1 Comparing drones with camera phones

From the informants' perspective, the main similarity is that both drones and camera phones can take pictures and record videos. The major differences, however, lie in the distance of recording, and the visibility or accessibility of the owner or controller. For instance, Dan explained eloquently, *"It would be a lot further away with a drone and they're hidden away but still get a really good shot. So I feel like there's that kind of not knowing that this is happening as opposed to a cell phone where you get a much larger chance of seeing that person taking that photo of you."* Dan's reasoning again speaks to the flying (drone) cameras at a distance that can take pictures or videos of individuals inconspicuously (i.e., without their awareness).

Emily focused on the controller of the device. She said, *"When you see some people taking picture of you using their phone, you can go to them and ask them to delete the pictures or videos. But when a drone is taking picture or recording video of you, you cannot control it, and it can easily fly away, or the pictures and videos have already been trans-*

ferred to the controller's mobile phone and you may not even know where the controller is." She emphasized the hidden controllers that are behind the scene, inaccessible to the people being recorded. As such, the invisibility and inaccessibility of drone controllers make people's usual privacy practices (e.g., ask camera controllers not taking or deleting the photos) futile.

4.3.2 Comparing drones with CCTV

While both drones and CCTV can take videos, the informants suggested a few notable differences, including their flexibility, visibility, intended purposes, and trust in the controllers. For instance, Mike focused on the flexibility. He said, *"Drones can fly anywhere so it can dynamically record everything. As far as I know, CCTV can only record as long as you're in that area."*

Emily explained the difference in purpose, *"Well there's obviously a reason why they have the (CCTV) cameras in there, it's like for security and safety and like I know why they're there and I think it's kind of like the norm. People are already like kind of used to having security cameras."* Emily highlighted that CCTV is a familiar technology now and people have established norms or expectations of it, whereas drones are too new to have agreed-upon norms.

In terms of visibility, Grace articulated the difference, *"A security camera is put in a place where it's very visible, usually places will post some sort of sign that says there's a security camera. So there's that disclosure and you understand if you step into that space you are going to be recorded. But I think a drone has the ability to enter someone's space rather than the person going into a space and then not having that disclosure that it's being recorded."* What Grace illustrated is a metaphor that CCTV passively waits for people to be recorded whereas drones actively enter into people's space to record them. In a way, this nature of drones shifts the initiative from the people to drones, weakening the people's control of the situation.

Our informants also pointed out differences in their trust of the controllers. "*I wouldn't mind what you would be doing indoors, that's for security, but outside then it's beyond your control because inside you know who is having that, who is handling that...definitely we know who is handling the drone. Maybe the security person or something like that, right. So you trust them, you would not fear unless you are the one who's going to be the trouble inside.*" This informant highlighted the importance of trust or the lack of it for drone controllers.

Because drones and their controllers can be more difficult to recognize and approach, we next discuss what people would expect in terms of controlling and regulating drones.

4.4 Expected notification and control

Our informants proposed a few controls of drones and their controllers. They also suggested regulating drones in terms of their size as well as their flying altitude, area, speed, and time.

4.4.1 Tracking drone controllers

Because of the potential for safety issues and malicious use, several informants suggested the need for drone controllers to register so that they can be tracked and held accountable. In addition, training and certification were recommended for operating drones. Interestingly, our informants used driver's license or gun license as an analogy to drone controller license.

For example, Cindy treated a drone license like a driver's license: *"just like drivers need driving lessons, I think the drone controller also needs a license because if you didn't control it very well and it can make some damage to the environment and may also intrude other people's privacy."*

Those who compared a drone's license with a gun license felt both technologies can be used for bad purposes. For instance, Hannah proposed a drone license to keep track of the controller, *"You can't just buy drones whenever and wherever, you have to have like a license or it would be registered under your name with that serial number so people can identify whose was that, so people can't use it and like if they used it for something bad it would be under your name."*

4.4.2 Tracking and controlling drones

Our informants also proposed ideas to track drones such as using a unique ID, and detecting and monitoring drones via a mobile app. Mary was one of the informants that proposed a unique ID for each drone. She explained, *"For example, let's say some people use a drone to do bad things, and you can track the drone by the serial number. It would be an evidence that you have used your drone to do bad things, such as you used your drone's camera to see the forbidden spot."*

Grace hoped for something more convenient. She imagined, "*I would hope to see in an app or something to show what the drone could see or record from flying above my home.*" What she requested is a technology that could essentially discover nearby drones and monitor what the drone camera can see, but more fundamentally, she asked for more awareness of drones and their operations.

While our informants provided suggestions for tracking drones, they felt that they cannot stop drones from flying or taking pictures. For instance, Lily said "*I can't stop them [drones] from taking pictures. I will just stay away.*" Abby also

expressed her inability to stop drones but suggested that drone manufacturers may do something to prevent misbehaviours of drone controllers. She speculated, "*Let's say they [drone manufacturers] have a backup chip to capture the images from the phone, so if a controller is doing any illegal activity that would be stored in this purposeful part of this chip, which a controller has no access to but the manufacturer can get into that. That would be the only way to curb the bad activity.*"

Given the powerful nature of drones, regulation is warranted. While the FAA has been finalizing their drone regulation, what do people expect from the regulatory front?

4.4.3 Regulations on drone features and operations

When asked what aspects of drones should be regulated, our informants' responses focused on two aspects: drones' physical properties such as size, speed, and color; and drones' operational properties such as flying height, area, and time.

Some informants held that the size of a drone should not be too small or too big. Abby explained, *"If a drone's size is too small then that would be weird because you cannot see it and that's definitely used for spying. I don't want a drone like a Boeing though, that would be pretty bad if it flies low and it would be scary. It should not be bigger than this table [one yard long, and 16 inches wide]."* Besides, Hannah felt the need to regulate drone speed. She said, *"I would want to regulate the speed of drone, about how fast it goes...may be not too fast."* Several informants mentioned about noise control. Mike explained, *"Personally you may not want to hear any noise. I may be sleeping so if somebody is outside flying a drone, I feel like so it's just getting annoying."*

Finally, a few informants proposed to color specialized drones, e.g. drones used by the police, so that they can be more identifiable by the public. Hannah explained, *"Using color that is specifically for police, just dye your drone would help people. So when I see that drone flying I know that this is for the police and I'd be kind of okay with that."* The colors signify purposes or ownership which could produce trust: "*I fly somebody's drone then how can you be sure that that drone does not carry a gun. How can you trust those things...that's why I say if you use different colors you trust them that it's some government or some legalization purpose so you trust*"

In terms of drone operations, our informants proposed to regulate its flying height, area, and time. For instance, a few informants emphasized that a drone should not be allowed to fly at night for privacy and noise considerations. For example, Sue said, *"It would be weird if the drone is flying at night...particularly if it is flying around my private space."* Drone regulations should consider these dimensions.

5 Discussion

While all of our informants had heard of drones before, it is still a relatively new technology to them. Overall, they had mixed feelings about drones. On one hand, they saw clear values in drones as they identified many benefits and promising applications of drones, such as aerial photography, goods delivery, and emergency responses. On the other hand, their positive perceptions were overshadowed by a multitude of safety, security and privacy issues that they raised. Drones can be something our informants love or loathe. They used a wide range of adjectives to describe drones: from cute, cool, fun, useful and beneficial to weird, risky, suspicious, invasive, disturbing, chaotic, and dangerous. None of our informants completely ruled out drones as they always saw some drone usage under certain conditions as beneficial, but some participants expressed the sense of inability to have control over or stop drone usage.

5.1 Unpacking privacy concerns

While the news stories and government regulations tend to emphasize the safety and security concerns, the privacy issues have received less attention. Our findings suggest that the informants had various privacy concerns regarding drones. There are several characteristics of these concerns.

First, we highlight the *duality* of drones. Our informants' perceptions of or concerns about drones were not only about drones per se, but also about the perceived relationships with the drone *controller*. Wanda Orlikowski posits the duality of technology, a recursive relationship that exists between technology and human action. On the one hand, technology mediates human action, however, it is also changed by human action [48]. Similarly, we suggest the duality of drones. Drones mediate drone controllers' interactions with citizens, and they are also changed by drone controllers' actions. One aspect of this duality represents the physical form and properties of the device (drone) as designed and manufactured by people and/or organizations, whereas the other aspect of this duality emphasizes the social construction of drones by the adopters and controllers through the different meanings they attach to the technology. In other words, drones manifest and extend the controllers' agency and intention. As such, our informants often negotiated their privacy with the imagined and often hidden drone controller, mediated by the drone. It is also worth noting that drones can be used or controlled by different kinds of entities such as individuals, organizations, and governments.

Related to the social construction of drone, people's privacy perceptions are deeply relational [50, 59]. In the friend's

party scenario, the social relationships between the friend and the guests parochialize the private party/space and eased some informants' concerns. In the police scenario, the perceived relationships between citizens and the government (where government being a "Big Brother" or a safety guard) affected informants' perceptions.

Second, drones could violate both people's *physical privacy* [3] and *information privacy* [56]. Physical privacy often refers to the concepts of solitude and bodily privacy [3]. Information privacy relates to the collection, use, and sharing of one's personal data [56]. In their seminal paper on privacy, Warren and Brandeis advocate for "the right to be let alone" [63]. The fact that drones can fly close to people or enter into their spaces can be viewed as intruding people's solitude. Jerry Kang discusses privacy in physical space as "the extent to which an individual's territorial solitude is shielded from invasion by unwanted objects or signals" [35]. Drones can be the unwanted objects.

One of the factors that our informants considered when judging the acceptance of a drone usage is whether the drone is operating in a public space or a private space. In general, our informants detested drones flying close to their homes because the drone cameras could peek through the windows to see or record them doing private things, such as bathing as one informant exemplified. This would invade people's bodily privacy. The pictures and video taken by drones about people would obviously affect their information privacy especially when people do not know that they were recorded and how the recordings will be used.

We also note that our informants differed in their delineations of public and private space. Daniel Solove points out that the boundary between individuals' private and public spaces was permeable and pivotal in their privacy concerns [57]. Research has also shown that technologies have been blurring the boundary [27]. A few informants believed that they own their private space within a larger public space, such as parks or shopping malls. Lofland notes that technologies have transformed urban space into a "privatism," because phones, vehicles etc. have "made the withdrawal from participation in the public realm a genuine option" [41]. This is also related to the personal space that people want to maintain [25]. One informant talked about not wanting to be watched by drones if she goes to shopping with an intimate friend. She rejected the drone invading the intimate space between her and her friend while shopping in public places.

This idea of personal space also relates to Lofland's conceptualizations of urban spaces. Lofland differentiates three types of urban spaces: public, private, and parochial spaces [41]. These spaces are characterized by the social relationships therein: strangers (public space), close friends and family members (private space), and people who share commonalities, such as neighbours even if they do not know each other (parochial space) [41]. Accordingly, when a person is doing something personal (e.g., shopping with a close friend) in a public place (e.g., a mall), for that person, however, it is still a private space because of the social relationship (close friendship) that defines the space.

The importance of these different kinds of spaces is also related to the social norms within them. In Erving Goffman's *The Presentation of Self in Everyday Life*, he describes how we present ourselves according to the norms in the different spaces [23]. We argue that the presence of a drone can alter how people perceive the norms in which they are embedded. For instance, a drone can bring a sense of "publicness" into a private space. As a result, the drone creates tensions between expected norms of public and private spaces.

Privacy is also highly contextual. Our informants' perceptions of drones varied across different scenarios. They construed and negotiated their private and public spaces differently across the five scenarios. Helen Nissenbaum's theory of Contextual Integrity underlines the contextual nature of privacy [46]. She identifies two types of contextual norms for privacy: "norms of appropriateness, i.e., what information would be appropriate to be revealed in a context; and norms of flow or distribution, i.e., the flow of personal information in certain context needs to be reasonably justified. If either of these norms has been violated, then users' privacy is considered to be infringed" [46]. The informants paid particular attention to the purposes of the drone uses. For instance, in the friend's party scenario, some informants would accept drone recording only if it is for personal use.

5.2 What makes drones interesting?

Drone is certainly not the first tracking/recording technology that raises privacy concerns. What makes drones particularly interesting or unique compared with other technologies, such as camera phones and CCTV? Our informants identified a combination of factors. First, drones are powerfully mobile. Drones with cameras can be viewed as *flying eyes* that could flexibly and even un-noticeably fly into public and private spaces, watch, record and even share what people are doing. However, it is not the drone that is flying, but rather the controller is flying the drone. Even when a drone is flying autonomously, it is executing a plan programmed by the controller. As such, the flying eyes not only represent the drone camera but also the eyes of the drone controllers.

This leads to the second factor - the *duality* of drone. Citizens are not interacting with the drones in that they are essentially interacting with the (hidden) controller. Moreover, both the drones and their controllers can be invisible and/or inacces-

sible to the people being watched. Compared with other tracking/recording technologies, the invisibility and inaccessibility of drone/controller is exacerbated. People may not be able to detect drones from afar or approach the drone controller to find out what the drone is doing. This lack of awareness and approachability paralyze people's abilities to negotiate and enact their privacy. Acquisti et al. point out that people have considerable uncertainty about their privacy [1]. Such uncertainty is in part due to information asymmetry where technologies have made personal data collection and usage invisible [1]. Information asymmetry is not new but drones aggravate it.

Ryan Calo argues that drones may actually help to waken and restore individuals' privacy awareness because previous privacy violations are hard to visualize, thus giving consent or notification to individuals may not generate a concrete sense [11]. Our informants worried about the invisibility and inaccessiblity of drones/controllers and as a result, the difficulties in getting notification and providing consent. There is currently no standard or a reliable way to enable notice and consent for drones. This makes our informants' suggestions on the design and regulation of drones particularly valuable.

5.3 Implications for design

High-level principles. Based on our findings, we first propose the following high-level privacy principles for drones:

- making both the drones and their controllers more discoverable, approachable, and accountable;
- enabling communication between drone controllers and ordinary citizens/bystanders;
- making drone designs sensitive to local social and cultural norms.

First, given the duality of drones, designs should make drones and controllers more discoverable, approachable, and accountable. Information about drones and controllers should also be made available. Adopting the notion of "accountabilities of presence," we suggest that the presence of the drone and its controller signifies a participation to a social relationship with the citizens [59]. As a result, the citizens can hold the controller accountable and ease their concerns.

Second, since the invisibility and inaccessibility of drones and drone controllers paralyze some of people's existing privacy practices (e.g., ask the camera controllers not to take or delete photos), we advocate creating channels or platforms to enable direct communication between drone controllers and ordinary citizens/bystanders. This will help build trust and form appropriate social norms over time around drone use that respects citizens.

Third, our results also hinted that the different perceptions and expectations of drone usage are embedded in larger social, cultural, and political contexts. For instance, some of our informants talked about the perceptions of drone usage in the Indian culture. Drone designs should consider the cultures or norms of the country/environment that they operate in. Different pre-defined privacy settings or modes may be used as defaults in certain countries to respect their social norms.

Next, we discuss more specific ideas for designing privacy-friendly drones. Fig. 3 shows example ideas including features from existing privacy-enhancing technologies for drones and other devices as well as suggestions from our informants and ourselves. None of them is a silver bullet to solve all the privacy issues, but collectively they will raise the bar for protecting ordinary citizens' privacy regarding drones. The ideas for drones/controllers may be built by the drone manufacturers and used by drones/controllers.

Designs for drones/controllers. From the standpoint of the drone or controllers, a number of privacy-enhancing techniques can be applied. When a camera is recording, it usually signals the recording with a red light which could be detected by bystanders if the camera is relatively close. However, since drones can fly and record at a distance, people might not detect this signal. Recently, a group of researchers have proposed a system called LightCense that uses flash lights as a drone's ID and people can use their phones to look up the drone by decoding the sequence of lights via a mobile app [40]. While innovative, it does not show what the drone camera sees, which some informants requested. Some of our informants suggested using particular colors to manifest the purpose of a drone (e.g., a police drone). Using standardized color schemes can help ordinary citizens quickly determine, for example, a police drone or a recreational drone.

Besides, there are a large number of citizens with visual impairments who would have difficulties leveraging visual cues. Instead, designers could explore designs that allow people to discover drones on their devices such as smart phones rather than manually searching drones in the sky. For instance, if a drone includes a GPS unit and flies in someone's area, that person can be notified about the drone via an app. If the controller registers with the app, he or she could also provide information about the drone (even including pictures or videos it has taken) and about himself or herself. The app users can approach and interact with the controllers via the app to negotiate their goals and privacy. Drones may also broadcast ultra-frequency sounds (human cannot hear) which encode information about the drones and people's phones or devices can detect these sounds, decode and present these drone information to the citizens/bystanders.

Drone privacy designs should also protect both people's physical privacy and information privacy. The FAA has de-

	Proactive		Reactive
Drone (Controller)	Signal recording Unique ID Provide drone/recording info Inform/enforce rules Detect sensitive location/info Context-sensitive camera control No fly zone	+Signal ownership/purpose *Broadcast notifications *Privacy-friendly defaults *Communication with citizens +Training/best practices	Encryption Access control Transformation of data Logging and audit (accountability)
Bystander	Request drone/recording info (e.g., what the drone sees)	*Detect drones *Receive notification * Signal opt-out *Communicate to controller	Access to collected data Request data filtering and removal

Fig. 3. Concrete ideas of privacy-enhancing drones for drone controllers and ordinary citizens/bystanders, including both proactive and reactive measures. + denotes suggestions from our informants. * denotes the new suggestions that we propose.

veloped B4UFLY, a mobile app that helps drone controllers "determine whether there are any restrictions or requirements in effect at the location where they want to fly" [19]. Besides, the no-fly zones can help keep drones away from sensitive areas. These mechanisms could help prevent safety and security issues as well as protect people's physical privacy.

In terms of information privacy, the standard best practices, such as encrypting the content, setting up appropriate access control, redacting sensitive content, logging and auditing would be useful. For instance, drone designs can explore existing access control mechanisms for continuous sensing [54]. We advocate that the drone designers and manufacturers consider incorporating these privacy-enhancing designs in their drone products. While incorporating these privacy features might seem as an increase to the cost, the benefits of making drones more privacy-friendly are also competitive advantages in the drone marketplace.

Since privacy concerns were raised by all of our informants, we suggest that techniques such as facial recognition and sensitive information detection may be incorporated into drones for data obfuscation/filtering purposes. Similar techniques have been introduced by previous studies in the wearable camera context for both bystanders and controllers/owners. For bystanders, Korayem et al. introduced ScreenAvoider, a framework that can help users to manage their privacy by protecting users' sensitive images and information on computer screen from wearable cameras [38]. Using deep learning techniques, ScreenAvoider can detect and classify sensitive information on computer monitor, then provide users that ability to control the disclosure of these information [38]. For controllers, prior literature shows that controllers are concerned about the bystanders' privacy [31]. Raval et al. propose PrivacyEye and WaveOff, as their privacy marker system [53]. In this system, sensitive information will be automatically covered by a virtual bounding box from the operators' device, thus protect the bystanders' privacy [53]. However, to our knowledge, these techniques have not been adopted by drones. Future work can explore adapting these existing techniques to drones and developing new techniques to address the specific privacy concerns that people have with drones.

We also value Dourish's perspective that context is not a static representation but is dynamically produced and reproduced in the course of activity [17]. Via our scenario-based questions, we did find that our respondents' sense of private and public spaces, concerns on privacy, as well as opinions about notification were context-dependent. Taking this perspective, we suggest that automatic location or context detection techniques may be explored for drones. One similar system has been introduced in wearable cameras. Templeman et al. proposed PlaceAvoider, a technique for the wearable cameras to identify the current location [58]. If the current location is considered as sensitive (bedroom, bathroom), the images captured by the cameras will be flagged for further review before made available to other applications [58]. We did not find similar techniques developed for drones.

Considering the extreme mobility of drones, we propose that future work can explore and leverage location and context detection for privacy protections in drones. For instance, drones can implement smart privacy-friendly default settings or privacy-friendly camera modes, such as blurring people's faces, or abstain from taking pictures / videos in obviously private/personal locations or spaces such as people's residences. These settings or modes can be applied in recording but also viewing without recording (i.e., controllers can have a live feed of the camera view even when it is not recording).

Since drone technologies are relatively new to the general public, social norms around appropriate use of this technology do not exist. Designers should explore ways to nurture

the formation of these norms. For instance, designs could help strengthen the relationship between citizens and drone controllers so that they can develop trust and expectations for each other. A social platform (e.g., an app) for citizens and drone controllers to meet and mingle could be valuable. For instance, many drone manufacturers already have online forums for drone users/controllers (e.g., forum.dji.com). The manufacturers could extend these platforms into a community that allows drone controllers to provide information about their drones (e.g., where they fly and the purpose of flying/recording), welcome ordinary citizens/bystanders to voice their concerns and support direct communication between controllers and citizens. Similarly, location-based drone picture/video sharing sites can also be extended to help support this type of communication. When best practices and social norms of drones emerge, controllers can be informed or trained about these best practices using educational materials and tools (e.g., games).

Designs for citizens/bystanders. Since it is difficult for citizens to always be able to detect nearby drones and their recording behavior, they should be enabled to pull information about nearby drones. One way to achieve this is to build a database that drone controllers can voluntarily provide information about their drones that citizens can retrieve. If controllers do not provide such information, researchers could also look into ways to help citizens actively detect nearby drones. For instance, the aforementioned mechanism of drones broadcasting information about themselves via sound can be used to allow automatic detection of drones.

In addition, citizens should be able to express their opt out of being recorded by drones. For instance, if users can perform certain pre-defined gesture or the users' devices can broadcast opt-out signals (e.g., color or sound), the drone/camera can potentially capture, interpret and honor the request.

Lastly, citizens should be able to communicate with the drone controllers. For instance, the automatic detection of drones could provide information about the drone controllers (e.g., their email address). The communication platform (e.g., a website or an app) we discussed earlier may also support this communication as well as allowing citizens to request access to the recorded data and request data filtering or deletion. In summary, the key idea is to allow drone controllers and citizens to communicate and negotiate about citizens' privacy.

5.4 Implications for policy

In terms of public policy, both federal regulation and industry self-regulation of drones should take privacy protection as a priority. The FAA drone policy and the code of conduct of drone associations (e.g., Association for Unmanned Vehicle Systems International) barely touch on privacy protection. However, all informants raised privacy questions without any priming. This finding provides the timely empirical evidence that privacy concerns of drones are real and they need to be addressed.

The FAA launched a required drone controller registration in December 2015 [39]. The registration requires information about a drone controller's name, address, and a credit card, but not any information about the drones that this person owns. But, any registered drone controller should post his or her registration sticker on any drone he or she wants to fly outdoor. By early January 2016 over, 180,000 drone controllers had registered [44]. However, if a citizen is concerned about a drone taking pictures at distance, the citizen is unlikely to see the drone controller information on the sticker/drone and know who the controller is. As such, it is unclear how much this registration enables to protect people's privacy against drones in practice. In February 2016, the FAA announced that they will set up a committee to propose rules to govern how close drones can get to bystanders, mostly for safety reasons [2].

Based on our preliminary review of state-level legislation, 24 states in the US have passed drone-related legislation. We have three important observations. First, there is no consensus on the definition of "drone" among these state drone laws. Some states equate drone with Unmanned Aircraft Vehicle (UAV) such as Oregon, whereas other states separate the two, such as Idaho. Moving forward, a standardized definition is desirable. Second, only some states regulate the drone controllers in addition to the drones. For instance, North Carolina requires drone controllers to pass a knowledge test and get a permit issued by the The Division of Aviation of the Department of Transportation. Given the duality of drone, we advocate for regulations that cover both drones and their controllers. Third, few states have detailed rules on privacy. One exception is Iowa, which has rules on three aspects of privacy: (1) trespassing, (2) invasion of privacy (intrusion upon seclusion, public disclosure of private facts, and sexually motivated privacy invasion), and (3) harassment and stalking. We urge drone laws to include detailed privacy rules.

Some of our informants expected prior consent, however, practically consent would be difficult to implement. Imagine you plan to fly a drone in a park where there are one hundred people. It would be difficult, costly, or even unrealistic to get everybody's permission or consent before flying the drone and/or recording videos in that park. Instead of relying on getting people's prior consent, we suggest considering the ideas of *accountability* and audit. Drone controllers would be held accountable and receive audits for their drone operations.

5.5 Study limitations

Our study is a first step towards a deep understanding of people's perceptions of drones, and it has many limitations.

First, our study scope focused on civilian uses of lightweight drones operated by human controllers. As such, we did not explore military uses of drones.We separated military and civilian uses because they serve distinct purposes, have different implications on society, and thus require separate treatments (e.g., the FAA in th US only regulates civilian use of drones). We also did not study fully autonomous drones (FADs). To our knowledge, FADs are mostly used for military purposes. FADs and military uses may lead to perceptions of drones that are different from what we reported on civilian uses. Since military uses were excluded, our study also did not explore the entanglements between military and civilian uses of drones (e.g., some drone manufacturers have both military and civilian drones).

Second, the list of our scenarios is by no means comprehensive. We chose realistic scenarios that are already happening in the real world because they would be easier for people to understand. All of our scenarios might be perceived as having a "positive" purpose (e.g., searching criminals). We did not have a scenario that have a clearly controversial or "negative" intention (e.g., surveillance or mission creep). Having futuristic and/or "negative" scenarios may solicit different (and presumably more negative) perceptions of drones. In addition, we did not design the scenarios for highlighting the different affordances between drones and other tracking technologies (e.g., camera phones and CCTV). This limitation means that our study may miss some perceived differences between drones and other tracking technologies. Furthermore, each scenario presented a one-off drone use and thus did not highlight the possibility of continuous, repeated or multiple drone uses over an extended period of time. These long-term uses of drones and down-stream data analyses can evoke perceptions that we did not uncover. While some of our scenarios represented organizational uses of drones (e.g., Amazon package delivery, or the police uses drones for searching criminals), our informants seemed more cognizant of individual controllers than what organizations can do with drones and what data they can collect and use over time.

Third, our results are based on a limited sample size and the majority of our informants were university students in the US. This means that our findings might not be generalizable to the general population. University students can be more accepting of new technologies. Therefore, the general population may have even more privacy concerns over drone use than what we reported. In addition, we did not explicitly recruit for informants with varying social-economic status (e.g., minorities, vulnerable populations, or people with low incomes). People with these backgrounds may have different perceptions or concerns that we did not uncover.

Fourth, while we showed our informants an actual drone, flew it and showed them its live video feed when the weather permitted, it might be still difficult for them to think about this relatively unfamiliar technology. Since most of our informants were not very familiar with drones, they may have been focused more on undesirable aspects (e.g., new technology can bring privacy risks) than their actual perceptions. However, we did ask the perceived benefits of drones at the beginning of the interviews, so our informants were not biased to only consider the risky aspect of drones.

Fifth, we asked our informants to compare drones with camera phones and CCTV, two familiar tracking technologies, as references. We could have included other tracking technologies such as wearable cameras, which may elicit additional insights. However, people are generally less familiar with wearable cameras, making them less ideal as references.

Lastly, we used a specific drone in our study. This might limit our results as other examples of drones may elicit different perceptions.

6 Conclusion

Once a military technology, civilian drones are rapidly moving into the daily lives of people in the US and other countries. Our interview study is a first step towards understanding people's nuanced perceptions of drones. Our informants identified both potential benefits and promising applications of drones, but also safety, security and privacy issues. Our results also suggest that drone is more than just another tracking and recording technology. Its potential for surveillance and impact on people's physical and information privacy is almost unparalleled. The duality of drone implies that, metaphorically, the flying eyes (drones and their controllers) can enter and peek into people's private spaces and lives together. As a result, drone controllers should be held accountable for what they and drones do. Lastly, while the FAA has proposed drone rules to focus primarily on safety and security issues, our study provides timely empirical evidence that people's privacy concerns of drones are real, nuanced, and must be addressed.

7 Acknowledgments

We thank our informants for sharing their insights. We are also grateful to Jason Dedrick, Bryan Semaan, Seda Gürses and anonymous reviewers for their thoughtful feedback on earlier

versions of this paper. This work was supported in part by a Syracuse University internal research grant.

References

[1] Alessandro Acquisti, Laura Brandimarte, and George Loewenstein. 2015. Privacy and human behavior in the age of information. *Science* 347, 6221 (2015), 509–514.

[2] Alan Boyle. 2016. FAA panel will decide how drones and people mix. (Feb. 2016). http://www.geekwire.com/2016/faa-creates-panel-to-come-up-with-rules-for-letting-drones-come-near-innocent-bystanders/

[3] Anita Allen. 2015. Privacy and Medicine. In *The Stanford Encyclopedia of Philosophy* (fall 2015 ed.), Edward N. Zalta (Ed.). http://plato.stanford.edu/archives/fall2015/entries/privacy-medicine/

[4] Amazon. 2014. Amazon Prime Air. (2014). http://www.amazon.com/b?node=8037720011

[5] Rebecca Angeles. 2007. An empirical study of the anticipated consumer response to RFID product item tagging. *Industrial Management & Data Systems* 107, 4 (2007), 461–483.

[6] Melissa Barbee. 2014. Uncharted Territory: The FAA and the Regulation of Privacy via Rulemaking for Domestic Drones. (2014).

[7] Richard E. Boyatzis. 1998. *Transforming Qualitative Information: Thematic Analysis and Code Development*. SAGE.

[8] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology* 3, 2 (Jan. 2006), 77–101. DOI: http://dx.doi.org/10.1191/1478088706qp063oa

[9] Daniel J. Butler, Justin Huang, Franziska Roesner, and Maya Cakmak. 2015. The Privacy-Utility Tradeoff for Remotely Teleoperated Robots. In *Proceedings of the Tenth Annual ACM/IEEE International Conference on Human-Robot Interaction (HRI '15)*. ACM, New York, NY, USA, 27–34. DOI: http://dx.doi.org/10.1145/2696454.2696484

[10] John Travis Butler and Arvin Agah. 2001. Psychological effects of behavior patterns of a mobile personal robot. *Autonomous Robots* 10, 2 (2001), 185–202.

[11] Ryan Calo. 2011. The drone as privacy catalyst. *Stanford Law Review Online* 64 (2011), 29–33.

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

[13] Reece A Clothier, Dominique A Greer, Duncan G Greer, and Amisha M Mehta. 2015. Risk perception and the public acceptance of drones. *Risk analysis* (2015).

[14] Consumer Electronics Association (CEA). 2015. *U.S. Consumer Electronics Sales and Forecasts*. Technical Report. Consumer Electronics Association (CEA). https://www.cta.tech/News/News-Releases/Press-Releases/2015-Press-Releases/New-Tech-to-Drive-CE-Industry-Growth-in-2015,-Proj.aspx

[15] Kathleen Bartzen Culver. 2014. From battlefield to newsroom: Ethical implications of drone technology in journalism. *Journal of Mass Media Ethics* 29, 1 (2014), 52–64.

[16] Tamara Denning, Zakariya Dehlawi, and Tadayoshi Kohno. 2014. In situ with bystanders of augmented reality glasses: Perspectives on recording and privacy-mediating technologies. In *Proceedings of the 32nd annual ACM conference on Human factors in computing systems*. ACM, 2377–2386.

[17] Paul Dourish. 2004. What we talk about when we talk about context. *Personal and ubiquitous computing* 8, 1 (2004), 19–30.

[18] Travis Dunlap. 2009. We've got our eyes on you: When surveillance by unmanned aircraft systems constitutes a Fourth Amendment search. *S. Tex. L. Rev.* 51 (2009), 173.

[19] FAA. 2015a. B4UFLY Smartphone App. (2015). https://www.faa.gov/uas/b4ufly/

[20] FAA. 2015b. Unmanned Aircraft Systems. (2015). https://www.faa.gov/uas/

[21] Adrienne Porter Felt, Serge Egelman, and David Wagner. 2012. I've got 99 problems, but vibration ain't one: a survey of smartphone users' concerns. In *Proceedings of the second ACM workshop on Security and privacy in smartphones and mobile devices*. ACM, 33–44.

[22] Baruch Fischhoff, Paul Slovic, Sarah Lichtenstein, Stephen Read, and Barbara Combs. 1978. How safe is safe enough? A psychometric study of attitudes towards technological risks and benefits. *Policy Sciences* 9, 2 (April 1978), 127–152. DOI: http://dx.doi.org/10.1007/BF00143739

[23] Erving Goffman. 1959. *The Presentation of Self in Everyday Life* (1 ed.). Anchor.

[24] Erving Goffman. 1971. Relations in public. microstructure of the public order. *Hannondsworth: Penguin* (1971).

[25] Edward Twitchell Hall. 1966. The hidden dimension . (1966).

[26] Steve Hodges, Emma Berry, and Ken Wood. 2011. SenseCam: a wearable camera that stimulates and rehabilitates autobiographical memory. *Memory (Hove, England)* 19, 7 (Oct. 2011), 685–696. DOI: http://dx.doi.org/10.1080/09658211.2011.605591

[27] Joachim R Höflich. 2006. The mobile phone and the dynamic between private and public communication: Results of an international exploratory study. *Knowledge, Technology & Policy* 19, 2 (2006), 58–68.

[28] Jason Hong. 2013. Considering privacy issues in the context of Google glass. *Commun. ACM* 56, 11 (2013), 10–11.

[29] Mohammad Alamgir Hossain and Yogesh K Dwivedi. 2014. What improves citizens' privacy perceptions toward RFID technology? A cross-country investigation using mixed method approach. *International Journal of Information Management* 34, 6 (2014), 711–719.

[30] Roberto Hoyle, Robert Templeman, Denise Anthony, David Crandall, and Apu Kapadia. 2015. Sensitive Lifelogs: A Privacy Analysis of Photos from Wearable Cameras. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. ACM, 1645–1648.

[31] Roberto Hoyle, Robert Templeman, Steven Armes, Denise Anthony, David Crandall, and Apu Kapadia. 2014. Privacy behaviors of lifeloggers using wearable cameras. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing*. ACM, 571–582.

[32] Ira Lamcja. 2015. Canada's police forces take to the sky with drones | Metro News. (2015). http://goo.gl/ITh2Nu http://www.metronews.ca/news/canada/2015/03/19/canadas-police-forces-taking-to-the-sky-with-drones.html.

[33] Jeremy Diamond. 2015. Obama: We need more drone regulations. (2015). http://www.cnn.com/2015/01/27/politics/obama-drones-fareed/

[34] Jonathan Kaiman. 2015. Chinese film star Zhang Ziyi is proposed to – by drone. *The Guardian* (Feb. 2015). http://goo.gl/kxo4lh http://www.theguardian.com/world/2015/feb/09/chinese-film-star-zhang-ziyi-is-proposed-to-by-drone.

[35] Jerry Kang. 1998. Information Privacy in Cyberspace Transactions. *Stanford Law Review* 50, 4 (April 1998), 1193–1294. DOI:http://dx.doi.org/10.2307/1229286

[36] Kathy Baxter and Catherine Courage. 2005. *Understanding Your Users: A Practical Guide to User Requirements Methods, Tools, and Techniques* (1 edition ed.). Morgan Kaufmann, San Francisco, CA.

[37] Yoohwan Kim, Juyeon Jo, and Sanjeeb Shrestha. 2014. A server-based real-time privacy protection scheme against video surveillance by Unmanned Aerial Systems. In *Unmanned Aircraft Systems (ICUAS), 2014 International Conference on*. IEEE, 684–691.

[38] Mohammed Korayem, Robert Templeman, Dennis Chen, David Crandall, and Apu Kapadia. 2014. Screenavoider: Protecting computer screens from ubiquitous cameras. *arXiv preprint arXiv:1412.0008* (2014).

[39] Les Dorr and Alison Duquette. 2015. Press Release – Unmanned Aircraft Registration System Takes Flight. (Dec. 2015). http://www.faa.gov/news/press_releases/news_story.cfm?newsId=19874

[40] LightCense. 2016. LightCense. (2016). http://www.lightcense.co/

[41] Lyn H. Lofland. 1998. *The Public Realm: Exploring the City's Quintessential Social Territory*. Transaction Publishers.

[42] Aleecia M. McDonald and Lorrie Faith Cranor. 2010. Americans' attitudes about internet behavioral advertising practices. ACM Press, 63. DOI:http://dx.doi.org/10.1145/1866919.1866929

[43] David H. Nguyen and Gillian R. Hayes. 2010. Information Privacy in Institutional and End-user Tracking and Recording Technologies. *Personal Ubiquitous Comput.* 14, 1 (Jan. 2010), 53–72. DOI:http://dx.doi.org/10.1007/s00779-009-0229-4

[44] Jack Nicas. 2016. U.S. Drone Users Number At Least 181,000. (Jan. 2016). http://blogs.wsj.com/digits/2016/01/06/u-s-drone-users-number-at-least-181000/

[45] Helen Nissenbaum. 2004. Privacy as contextual integrity. *Washington law review* 79, 1 (2004), 119–158.

[46] Helen Nissenbaum. 2009. *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.

[47] NoFlyZone. 2016. NoFlyZone. (2016). https://www.noflyzone.org/

[48] Wanda J. Orlikowski. 1992. The Duality of Technology: Rethinking the Concept of Technology in Organizations. *Organization Science* 3, 3 (Aug. 1992), 398–427. http://www.jstor.org/stable/2635280

[49] George Orwell. 1949. *1984*. Signet Classic.

[50] Leysia Palen and Paul Dourish. 2003. Unpacking "privacy" for a networked world. In *Proceedings of the SIGCHI conference on Human factors in computing systems*. ACM, Ft. Lauderdale, Florida, USA, 129–136. DOI:http://dx.doi.org/10.1145/642611.642635

[51] Pensacola News Journal. 2015. Drone video: Pensacola Grand Mardi Gras Parade. (2015). http://www.pnj.com/videos/entertainment/events/mardi-gras/2015/02/15/23444447/

[52] Katerina Pramatari and Aristeidis Theotokis. 2009. Consumer acceptance of RFID-enabled services: a model of multiple attitudes, perceived system characteristics and individual traits. *European Journal of Information Systems* 18, 6 (2009), 541–552.

[53] Nisarg Raval, Landon Cox, Animesh Srivastava, Ashwin Machanavajjhala, and Kiron Lebeck. 2014. Markit: privacy markers for protecting visual secrets. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication*. ACM, 1289–1295.

[54] Franziska Roesner, David Molnar, Alexander Moshchuk, Tadayoshi Kohno, and Helen J Wang. 2014. World-driven access control for continuous sensing. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 1169–1181.

[55] Bruce Schneier. 2015. Is it OK to shoot down a drone over your house? - CNN.com. (2015). http://www.cnn.com/2015/09/09/opinions/schneier-shoot-down-drones/index.html

[56] H Jeff Smith, Tamara Dinev, and Heng Xu. 2011. Information privacy research: an interdisciplinary review. *MIS quarterly* 35, 4 (2011), 989–1016.

[57] Daniel J Solove. 2006. A taxonomy of privacy. *University of Pennsylvania law review* (2006), 477–564.

[58] Robert Templeman, Mohammed Korayem, David Crandall, and Apu Kapadia. 2014. PlaceAvoider: Steering first-person cameras away from sensitive spaces. In *Network and Distributed System Security Symposium (NDSS)*.

[59] Emily Troshynski, Charlotte Lee, and Paul Dourish. 2008. Accountabilities of presence: reframing location-based systems. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 487–496.

[60] Janice Tsai, Patrick Kelley, Lorrie Cranor, and Norman Sadeh. 2010. Location-Sharing Technologies: Privacy Risks and Controls. *I/S: A Journal of Law and Policy for the Information Society* 6, 2 (2010), 119–152. http://ssrn.com/abstract=1997782

[61] Blase Ur, Pedro Giovanni Leon, Lorrie Faith Cranor, Richard Shay, and Yang Wang. 2012a. Smart, useful, scary, creepy: perceptions of online behavioral advertising. In *Proceedings of the Eighth Symposium on Usable Privacy and Security (SOUPS '12)*. ACM, New York, NY, USA, 4:1–4:15. DOI:http://dx.doi.org/10.1145/2335356.2335362

[62] Blase Ur, Pedro Giovanni Leon, Lorrie Faith Cranor, Richard Shay, and Yang Wang. 2012b. Smart, useful, scary, creepy: perceptions of online behavioral advertising. In *Proceedings of the Eighth Symposium on Usable Privacy and Security*. ACM, 4–19.

[63] Samuel Warren and Louis Brandeis. 1890. The Right to Privacy. *Harvard Law Review* 4, 5 (1890), 193–220.

[64] Alan F. Westin. 2003. Social and Political Dimensions of Privacy. *Journal of Social Issues* 59, 2 (July 2003), 431–453. DOI:http://dx.doi.org/10.1111/1540-4560.00072

[65] David Wright, Rachel Finn, Raphael Gellert, Serge Gutwirth, Philip Schütz, Michael Friedewald, Silvia Venier, and Emilio Mordini. 2014. Ethical dilemma scenarios and emerging

technologies. *Technological Forecasting and Social Change* 87 (2014), 325–336.

[66] WUSA9. 2015. Drone video goes inside abandoned White Flint Mall. (2015). http://goo.gl/Akndp2 http://bethesda.wusa9.com/news/news/2664031 -drone-video-goes-inside-abandoned-white- flint-mall.

A Interview Questions

A.1 General questions about drones

1. Have you heard of drones? What is the first thing that comes to your mind when you hear about drones?
2. What have you heard about drones?
3. How do you feel about drones?
4. Do you see any benefits or issues of drones?
5. What information do you think drones can collect about you?
6. Did you know that you can record video with drones?
7. Why do you think someone would want to have a drone?
8. How would you compare recording by a drone with recording by a cell phone with a camera? Why?
9. How would you compare recording by a drone with recording by a CCTV camera? Why?
10. How do you feel about being around with a flying drone? Why?
11. Would you want someone who plans to fly a drone near you to ask for your permission before recording a video?

A.2 Context-based questions

12. Are there situations in which you would be more willing to let drone flying round you and recording?
13. For each of the following scenarios, please indicate if you would accept this drone usage. Please explain the reasoning behind your decisions.
    (a) Imagine you are in a shopping mall where a promotion event is going on, like on the Black Friday. The store owner decides to use a drone to monitor and record this event, and you happen to be in that event.
    (b) Imagine you are at your friend's party, and your friend decides to use a drone to record the party.
    (c) Imagine that Amazon decides to use drones to deliver goods that you have bought in its online store to your house.
    (d) Imagine you are in a parade. Some news agency decides to use a drone to record the parade.
    (e) Imagine that there are some suspects or criminals lurking in your residential area. The police department decides to use drones to search for these people in your residential area.

    Do you have any other thought about drones' possible applications?
14. Have any of your expectations changed on drones?
15. Are there any circumstances in which you would NOT like drones to collect data about you?
16. Are you aware of any laws dealing with drones?
17. Do you have any additional comments?

A.3 Expected notification and control

The following questions were inspired by: Drone Aircraft Privacy and Transparency Act of 2013 (proposed but not enacted in the US).

18. Do you expect to have the list of individuals who have the authority to operate or who are operating drones?
19. Do you expect to be notified about the exact locations of the operating drones?
20. Do you expect to be notified about the time periods during which drones can/will be operated?
21. Do you expect to be notified about the types of information that the operating drones might collect?

The following questions were adapted from a RFID user study [29].

22. Do you expect to be asked for any kind of "explicit consent" to allow drones to fly near you? Why?
23. Do you expect to see detailed explanations if a drone takes pictures or videos that can capture you? Why?
24. Do you expect to have any control over your privacy regarding drones operated or owned by others? Why? If you do have such expectations of control, could you give me an example?