Request Summary

Requester: Yang Wang, ,

Title: How Drone Controllers and Bystanders Perceive Different Privacy Mechanisms for Drones

Abstract:

Drones can enable innovative applications but also raise heightened privacy concerns such as surveillance and stalking. To mitigate these concerns, various technology-based and policy-based mechanisms have been proposed. However, most of these mechanisms are voluntary. Therefore, it is unclear how drone controllers and bystanders perceive these mechanisms and whether people intend to adopt them.

We report results from two rounds of online survey with 169 drone controllers and 717 bystanders. When considering individual mechanisms, *drone owner registration* and *face blurring* received most support from both controllers and bystanders. Under specific drone usage scenarios, our respondents suggested using multiple mechanisms together as they may improve different aspects of privacy. Our results also uncover a sense of distrust between controllers and bystanders. We outline a set of important questions for future privacy designs and policies for drones.

Implications for privacy design: Besides the promising results on *face blurring*, future designs should further explore ways to engender trust between drone controllers and bystanders. These may include ways that have helped companies to build consumer trust such as adopting fair information practices and presenting privacy policies as well as ways to improve interpersonal trust such as providing transparency in decision-making (e.g., why use drones to take pictures) and holding people accountable.

We also found that while bystanders valued their privacy, controllers were also concerned about protecting their own privacy. For instance, when considering mechanisms such as owner registration, many controllers did not want bystanders to know their information. This suggests future designs and policies for drones should strike a good balance between the interests (e.g., privacy) of both controllers and bystanders.

Implications for public policy: Many bystander respondents considered these privacy mechanisms ineffective because of their voluntary nature. They suggested making some of these mechanisms (e.g., no-fly-zone) required by laws or enforced automatically via technical means (e.g., implementing in firmware).

Publication:

We have one paper describing this research currently under blind review (attached)

Yaxing Yao, Y. Huang, Y. Wang. Privacy Mechanisms for Drones: Perceptions of Drone Controllers and Bystanders in the U.S. ACM SIGCHI Conference on Human Factors in Computing Systems (CHI2017). Under Review.

A related publication that inspired this research:

Y. Wang, H. Xia, Yaxing Yao, Y. Huang. Flying Eyes and Hidden Controllers: A Qualitative Study of People's Privacy Perceptions of Civilian Drones in the US. Proceedings on Privacy Enhancing Technologies. Volume 2016, Issue 3, 172–190, ISSN (Online) 2299-0984, DOI: 10.1515/popets-2016-0022, May 2016.

Privacy Mechanisms for Drones: Perceptions of Drone Controllers and Bystanders in the U.S.

Yaxing Yao, Yun Huang, Yang Wang
SALT Lab, Syracuse University
yyao08 | yhuang |

ABSTRACT

Drones pose privacy concerns such as surveillance and stalking. To mitigate these concerns, various voluntary mechanisms have been proposed. However, it is unclear how drone controllers and bystanders perceive these mechanisms and whether people intend to adopt them. In this paper, we report results from two rounds of online survey with 169 drone controllers and 717 bystanders. We found that *drone owner registration* and *face blurring* individually received most support from both controllers and bystanders. Under specific drone usage scenarios, our respondents suggested using multiple mechanisms together as they may improve different aspects of privacy. Our results also highlight a sense of distrust between controllers and bystanders. We outline a set of important questions for future privacy designs and policies for drones.

ACM Classification Keywords

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

Author Keywords

Drone; privacy mechanisms; perceptions.

INTRODUCTION

Drones are unmanned aircraft that can be controlled remotely by human controllers or operated autonomously by onboard computers. In recent years, drones have entered the mainstream consumer market. This type of drones often carry cameras and possibly other sensors such as GPS, accelerometers as well as altitude, temperature and infrared sensors. Drones enable innovative applications but also raise privacy issues. For instance, an interview study conducted in the US reported people having various privacy concerns about drones such as staking, video recording and sharing [28].

In the U.S., the National Telecommunications and Information Administration (NTIA) released a document of voluntary best practices for commercial and non-commercial use of drones, for instance, having a privacy policy that explains an organization's use of drones [22]. A number of technical mechanisms for drone privacy have also been proposed. For instance, LightCense uses LED lights on a drone as its ID so that people could identify the drone and its information via a mobile app [21]. However, these technical mechanisms or best practices are voluntary and thus it is unclear whether people will adopt them and even if adopted, whether these mechanisms are effective.

In this paper, we focus on *how drone controllers and bystanders perceive these technology-based or policy-based privacy mechanisms for drones.* This research question is timely and important because if people perceive these mechanisms as requiring too much effort, being impractical or ineffective, they are unlikely to adopt these mechanisms. As a result, people's privacy concerns about drones would remain largely unaddressed, hindering the acceptance and adoption of drones and limiting their benefits to society. Privacy mechanisms that are supported by both drone controllers and bystanders are more likely to be adopted and useful in practice.

To answer this research question, we developed detailed descriptions of a diverse set of representative privacy mechanisms for drones and conducted two rounds of online survey to investigate how drone controllers and bystanders perceive these mechanisms. We denote bystanders as people who do not operate drones but may be surrounded by flying drones. Drone controllers are people who operate drones. In this research, we focus on drones that are used for civilian purposes, excluding military usage. We found that when considering individual mechanisms, drone owner registration and face blurring received most support from both groups. However, under specific drone usage scenarios, our respondents suggested using multiple mechanisms together as they may contribute to different aspects of privacy. Our results also highlight a sense of distrust between controllers and bystanders, which may aggravate the privacy issues of drones.

This paper makes two main contributions. First, it sheds lights into how drone controllers and bystanders think about different types of privacy mechanisms for drones. Second, it discusses ways to improve these specific mechanisms but also outlines important questions for privacy designs and policies of drones.

Related Work

Perceptions of Tracking and Recording Technologies

Since drones are usually equipped with cameras, they can be considered as tracking/recording technologies. Prior studies have identified people's privacy concerns (e.g., leaking personal information) about various tracking and recording technologies, such as Radio-Frequency Identification (RFID) tags [2], credit cards and store video cameras [23].

Prior research has also explored people's perceptions of wearable devices (e.g., glasses or cameras). In a study of Augmented Reality (AR) glasses, Denning et al. find that people expect giving their permissions before being recorded by AR glasses [9]. These wearable devices can also be used for "lifelogging" where photos, audio or video recordings are automatically taken by the devices as a person goes about doing his/her daily activities (e.g., SenseCam [17]). Hoyle et al. find that people have many privacy concerns about lifelogging [19]. 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" [19]. In a follow-up study, Hoyle et al. also discover that "lifeloggers" are motivated to share their "lifelogged" information for impression management purposes [18]. Last but not least, robots when equipped with cameras also have tracking and recording capabilities. In a recent study, Butler et al. find that people desire mechanisms to protect their privacy against remotely tele-operated in-home robots [5].

Privacy Issues of Drones

Legal scholars have argued that drones can infringe on citizens' privacy. For instance, Dunlap posits that drones can violate the Fourth Amendment of the US Constitution that protects citizens from unreasonable searches and seizures when drones are used for surveillance [11]. Therefore, the Fourth Amendment rights should regulate and restrict drone usage [11]. Wright et al. raise heightened concerns about drones 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") [27]. 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 [27].

There are few empirical studies of drone privacy. In a survey study of Australians' perceptions of drones, Clothier et al. find that their respondents did not consider drones to be overly beneficial or risky, but some respondents (less than one fifth) did raise a general privacy concern about drone surveillance or spying [7]. Wang et al. conducted interviews of potential drone bystanders about their perceptions of civilian drones in general and under specific scenarios [28]. They find that bystanders had various privacy concerns about drones and their perceptions of drones varied in different scenarios [28].

Privacy Mechanisms for Drones

A number of technical mechanisms have been proposed that directly or indirectly protect civilians' privacy against 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" [13]. 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 [24]. To provide citizens more information about drones, LightCense is proposed to uses a blink sequence of LED lights on a drone as its ID. People can look up information about the drone by scanning the lights via a mobile app [21]. As an example of a server-side mechanism, Yoohwan et al. propose using a combination of encryption, access control, and image/video transformation [20]. The NTIA recommends a number of voluntary best practices for drone usage, ranging from having privacy policies to informing bystanders before drones taking pictures/videos if possible [22].

Our study aims to investigate how drone controllers and bystanders perceive different privacy mechanisms. People's perceptions can affect the adoption of these mechanisms.

METHODOLOGY

We conducted two rounds of online survey of drone controllers and bystanders. We recruited survey respondents from Amazon Mechanical Turk (MTurk) where workers are based in the US and have at least 95% task acceptance rate. We also recruited respondents from drone user forums such as the DJI forum and Quadcopter.com forum. The first-round survey was conducted during March 2016 and we received a total of 456 valid responses including 385 bystanders and 71 drone controllers. We conducted a second-round survey during August 2016 and received a total of 430 valid responses including 332 bystanders and 98 drone controllers. Each valid response from MTurk was compensated for $2. We had 102 controller respondents from drone forums and administrated a raffle of four $50 gift cards. This research was approved by the IRB.

First-Round Survey

We provided a working definition of drones as "an unmanned aircraft guided by remote control or onboard computers." We also told the respondents to focus on civilian uses and exclude military uses of drones. Next, we asked "Have you ever flew a drone yourself?" If a respondent answered yes, then he or she will answer the controller branch of the survey; otherwise, answer the bystander branch of the survey. For the bystander/controller branch, we explicitly asked the respondents to consider themselves as bystanders/controllers.

Privacy concerns. Informed by Wang et al.'s bystander interviews [28], we developed and asked a set of 5-point Likert scale questions about bystanders' privacy concerns about drones, e.g., "I'm concerned that the drone can fly into my private space." For the controller branch, we framed the above questions from a controller's standpoint, for instance, we changed the wording from "my" to "others' " private space.

Privacy mechanisms. We developed descriptions of six mechanisms that have been implemented or proposed for drones. **No-fly-zone**: I enter my addresses (e.g. home) in a no-fly-zone database so that drones controllers will be warned when they fly the drones near these addresses [24]. **Deletion request**: Drone controllers can receive requests from me to delete photos or videos that capture my family, properties or myself via a mobile app [28]. **Gesture opt-out**: Have gesture recognition technology incorporated in the drone so that I can choose to opt out of being recorded by using certain gestures (e.g., two hands pose as X), and the drone camera can recognize the gesture and the camera will blur my face or figure in the recording (pictures or videos) [6]. **Controller-bystander app**: a mobile app that allows drone owners to provide information about his/her drone such as owner, purpose, drone model and camera/sensor information as well as the current location of the drone. It also lists drones near me and allows me to learn more information about these nearby drones. I can also directly contact drone owners via the app [28]. **Owner registration**: every drone owner must register with the government by providing his or her real name and contact information. Before flying a drone, the owner must mark his/her Registration Number visibly on the drone. I can see the registration number on a drone and then find out its owner information [14]. **LED license**: a drone will use a visible color blink sequence of its LED lights to serve as its unique "license" and I can use a mobile app to capture the color blink sequence, identify the drone, and look up the information about the drone (e.g., its ownership or purpose) [21].

This diverse set of privacy mechanisms vary by their types (e.g., technology-based vs. policy-based, proactive vs. reactive) and by controller and/or bystander effort. We randomized the order of mechanisms. For each mechanism, we asked respondents to rate their levels of agreement (5-point Likert scale) with three statements: "I think this mechanism would be effective in protecting my privacy; I would like to use this mechanism regularly; I think this mechanism is NOT practical." We also asked them to explain their ratings in an open-ended question. For the controllers, these mechanisms were framed from a controller's standpoint, for example, "people enter their addresses (e.g. home) in a no-fly-zone database so that I will be warned when I fly the drone near these addresses."

Second-Round Survey

The first-round survey yield many insights that we will present in the results, but we also learned one important limitation of this survey from respondents' feedback: the descriptions of privacy mechanisms were not detailed enough and thus they raised many questions about the specifics. The second-round survey was similar to the first survey but focused on two aspects: privacy mechanisms with detailed descriptions, and specific drone usage scenarios.

Privacy mechanisms. We decided to remove two mechanisms, deletion request and gesture opt-out, because they were not well supported by both types of respondents and they have not been implemented (also challenging to implement) in practice. We added two new mechanisms: privacy policy and face blurring. The NTIA best practices document recommends organizational users of drones to have a privacy policy that describe their drone uses, particularly the related data practices [22]. The face blurring mechanism was modeled after a Google Street View privacy feature that automatically detects human faces and blur them [16]. For each mechanism, we tried to describe what the mechanism does, how it is implemented, and what controllers and bystanders need to do to use the mechanism. Below are the descriptions.

No-fly-zone is implemented using a database maintained by the US Federal Aviation Administration (FAA). If a citizen is not comfortable of having drones flying around her house or apartment, she can go to the no-fly-zone website and enter her home address to designate the area within 10ft of her address (including backyard) as a no-fly zone. She needs to submit a document that verifies her residence (e.g., a utility bill). After the no-fly-zone system validates the entered address, the self-designated zone will be stored in the no-fly-zone database.

The drones incorporate the information of this no-fly-zone database either by directly connecting to the database via WiFi or by downloading and updating the database in the drone firmware on a regular basis. These no-fly zones will be highlighted on the map in the drone control interface. In addition, when a drone flies into a no-fly zone indicated by a citizen, the drone operator will get a warning on the drone control interface. Since there are no laws that require drone operators to honor these no-fly-zone requests, the drone operators may or may not choose to honor these requests [24].

Controller-bystander (CB) app is designed to improve communication between drone controllers and bystanders. The app works with three assumptions: (1) drones have a GPS module; (2) drones have a Wi-Fi module; and (3) both drone controllers and bystanders have installed and created an account in this app on their mobile devices. The CB app is operated by the US Federal Aviation Administration (FAA).

By default, GPS and Wi-Fi will be turned on while a drone is flying. The drone will record its location information as well as its recording status (e.g., whether the drone is taking photos or videos). This information will first be transmitted from the drone to the controller's CB app on his or her mobile device through Wi-Fi, and then sent back to a central database on a regular basis.

A drone controller creates an account in the app with information about his or her drone (e.g., drone model, usual flight area and times) as well as optional contact information. An app user can choose a pseudonymous user name in the app. Registered users of the app can send each other private messages via the app. In addition, the controller can choose to share photos, videos, or live video feed taken by the drone in the app so that other registered app users can see.

When a bystander creates an account and then logs into this app on his or her phone, the app will check with the central database on a regular basis. All the updated information, including drones nearby, will show up in the app interface. For example, if there is a drone nearby, the drone will show up on a radar map with the distance and direction from the bystander's current location. If the bystander would like to message the drone controller, the bystander just needs to tap on the drone in the radar map. The bystander will see all public information about the controller and the drone and can send a private message to the controller through the app.

LED drone license: A drone has an array of color LED lights (e.g., blue, green, red) that can be seen by more than 300ft without using any special equipment. These LEDs blink in a particular sequence to help people visually identify the drone. In other words, the blink sequence of LEDs serve as the drone's "license." This system is operated by the US Federal Aviation Administration (FAA).

A drone controller can sign up to use this system by registering an account via the system's website and can optionally provide information about himself or herself as well as information about the drone.

When a bystander spots a drone nearby, he or she can use the companion LED license mobile app to capture the LED blink sequence (with its camera), identify the drone, and look up the information about the drone (e.g., its ownership or purpose) provided by its owner/controller.

Drone owner registration: Every drone owner in the US. must register with the US Federal Aviation Administration (FAA) by providing his or her real name and contact information. Before flying a drone, the owner must mark his or her Registration Number visibly on the drone. In the event that a drone behaves inappropriately, a bystander may report to a law enforcement department. Federal law requires drone operators to show the certificate of registration to any Federal, State, or local law enforcement officer if asked.

Drone privacy policy: The US Federal Aviation Administration (FAA) recommends any organization that uses drones to have a drone privacy policy on their website. The privacy policy should include information about how they use drones, such as what kinds of drones they use; where, when and why they fly the drones; what kinds of data the drones will capture (e.g., pictures or videos) and for what purposes; how long the recorded data will be retained; how the recorded data will be processed and/or shared to others; and if citizens have questions about their drone use, how to contact them.

This drone privacy policy can either be a standalone privacy policy or part of an organization-wide privacy policy. Ordinary citizens can visit the organization's website to find and review its drone privacy policy.

Automatic face blurring: Drones have a built-in feature that can enable automatic identification and blurring of human faces in the pictures and videos taken by the drone camera. By default, this feature is turned on. The US. Federal Aviation Administration (FAA) recommends drone controllers to use this feature unless there is a legitimate reason not to do so.

We attempted to model these mechanisms realistically. Some mechanisms have already been implemented for drones (owner registration, no-fly-zone, and LED license) or used in other domains (privacy policies for websites, and face blurring for Google Street View). Other mechanisms have been proposed but not implemented, including deletion request, gesture opt-out, and the controller-bystander app. All mechanisms are voluntary except for owner registration, which is required by the FAA. To make these mechanisms more comparable, we framed them as administrated or suggested by the FAA. Some mechanism descriptions (e.g., controller-bystander app) were much longer than others (e.g., owner registration), but that reflects their relative complexity from the user's perspective.

Scenarios. Next, we provided three concrete drone scenarios. **Neighborhood safety:** Your neighborhood recently had several public safety incidents (e.g., burglaries). The local police department hires a few drone controllers to fly multiple drones with cameras in the neighborhood for public safety purposes. As a result, the neighborhood will be continuously monitored. These drones will be streaming the live video feed to the police department but will not record any pictures or videos. **Public park:** A drone controller is flying his drone in a public park and taking photos and videos for fun. You and your family, together with several other families with kids are playing in the park. You and your family members may be captured in the pictures and videos taken by the drone. **Real estate photography:** A real estate agency company hires a drone controller to shoot photos and videos of a house for sale. When the controller fly the drone and take the photos and videos of the house, these recordings might capture your houses and/or your backyard.

These scenarios differ by the type of drone controllers (e.g., companies vs. individuals), the purpose of drone usage (e.g., personal enjoyment vs. public safety), the number of drones used (e.g., single vs. multiple), the duration of drone usage (one-time vs. continuous), and the nature of recording (e.g., streaming without recording vs. recording). We randomized the order of scenarios. For each scenario, we asked respondents which privacy mechanism(s) they want to use and why.

Data Analysis

We computed descriptive statistics of quantitative data (e.g., privacy concerns, ratings of privacy mechanisms). We also coded the open-ended answers using a thematic analysis, "a method for identifying, analysing, and reporting patterns (themes) within data" [3]. First, we carefully read through the open-ended answers. Second, we independently open coded a subset of open-ended answers. Third, we discussed and created a code book containing codes that cover the respondent's overall sentiment of the mechanism (e.g., positive), specific reasons of liking (e.g., easy, practical, effortless, similar to existing mechanisms) or disliking the mechanisms (e.g., inaccurate, subject to hack, requiring too much effort, useless, impractical, increasing government surveillance), implementation details of the mechanism (e.g., scope of effective operation, communication channel, mobile app), and suggestions to improve the mechanism (e.g., legal requirement, automatic enforcement, who have access to controller data). We then used the code book to code the rest of the open-ended data.

RESULTS

We will focus on the privacy concerns of drone controllers and bystanders in the first-round survey and people's perceptions of different privacy mechanisms in the second-round survey.

First-Round Survey Results

Privacy concerns

We asked a set of eight 5-point Likert scale privacy concern questions in a randomized order: (Private space) "I'm concerned that the drone can fly into my private space." (Peeking) "It bothers me that the drone can peek into my windows." (Stalking) "I'm concerned that the drone can be used to stalk me." (Surveillance) "I think that it's acceptable to use the

Items	Md Bys	Md Ctr	W-value	P-value (adjusted)
Private space	4.0	3.0	18,754	0.000**
Peeking	4.0	2.0	22,020	0.000**
Stalking	4.0	3.0	18,508	0.000**
Surveillance	3.0	3.0	13,575	1.000
Invisible controller	4.0	2.0	20,104	0.000**
Public space	3.0	2.0	20,419	0.000**
Disclosure	4.0	3.0	20,712	0.000**
Registration	3.0	3.0	16,757	0.008

Table 1. Eight Mann-Whitney U tests on privacy concerns of controllers and bystanders (first-round survey). Md Bys and Md Ctr stand for median values of each item for bystanders and controllers, respectively.

drone for surveillance." (Invisible controller) "It bothers me if the drone controllers are out of sight." (Public space) "I'm fine with the drone taking pictures or videos that may capture me in a public space." (Disclosure) "The drone owners should disclose how they would use, share, or distribute the drone-recorded pictures or videos that may capture me." (Registration) "It's important to me that the drone can only be operated by people who have registered with the government."

To compare drone privacy concerns of controllers and bystanders, we conducted eight Mann-Whitney U tests with a Bonferroni correction (adjusted cutoff p value .005) for each question between the two groups of respondents. We used this non-parametric test because of the unequal sample sizes of controllers and bystanders. Table 1 shows the test results. The results indicate that our bystander respondents were significantly more concerned about drone privacy than their controller counterparts across all of these aspects except for surveillance and registration.

Privacy mechanisms

For each of the six mechanisms, we asked respondents to rate its effectiveness in privacy protection, their willingness to use it, and how practical it is. We also asked respondents to explain their ratings in free text. Figure 1 shows the percentages of controller and bystander respondents who either "agree" or "strongly agree" that a privacy mechanism is effective, practical, and that they are willingness to use it. Amongst the mechanisms, no-fly-zone and owner registration received most support from both groups across all three measures. Since we removed deletion requests and gesture opt-out from the second survey, we will mainly focus on people's feedback on these two mechanisms. We will discuss the results on the other four mechanisms using the data from the second-round survey.

Deletion request. Bystander respondents felt this mechanism can be useful if their requests are honored, but raised two main issues: (1) there is too much work for bystanders, and (2) controllers may ignore/reject the requests. One bystander summarized both points, saying *"This requires too much effort, and there doesn't seem to be any consequences if the drone owner chooses to do nothing."* Another bystander highlighted his concern about malicious controllers: *"A drone that is trying to spy on me or, otherwise, has ill intentions is not going to cooperate anyway."* From the controllers' perspective, some controllers felt this mechanism is unnecessary because they only publish photos that they deem safe to post. Besides, some controllers were concerned about bystanders abuse this mechanism and send an overwhelming number of such requests.

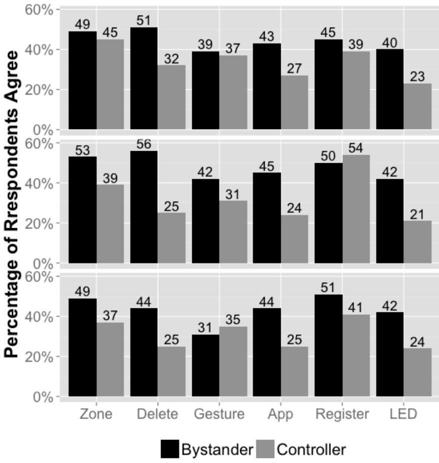

Figure 1. Survey 1 results on privacy mechanism: percentages of respondents who either "agree" or "strongly agree" that a privacy mechanism is effective, practical, and that they are willingness to use it. The mechanisms include: no-fly-zone (zone), delete request (delete), gesture opt-out (gesture), controller-bystander app (app), owner registration (register), and LED license (LED).

Gesture opt-out. Some controllers and bystanders thought this can be a good solution if people know it. The burden is on the bystanders to learn the gesture. However, some bystanders argued that it is controllers' responsibility to protect bystanders' privacy. One bystander explained, *"I feel like I shouldn't have to make gestures to protect my own privacy and that I would have to constantly be watching out for drones for this to be effective."* Some controllers felt there is really no need for opt-out because drone cameras are usually not good enough to capture people's in the air. One controller explained, *"There is a real lack of knowledge about the cameras on drones. Unless it is a large octo-copter being used by a professional operator with a high priced DSLR camera, then the images/videos you get would be grainy, and if taken from more then about 15ft up unable to identify faces."* This quote also suggests that an information asymmetry about drones' capabilities exists between controllers and bystanders.

Second-Round Survey Results

We used the second-round survey to further investigate people's perceptions about privacy mechanisms for drones (with more detailed descriptions), and their preferences of these mechanisms under three concrete scenarios.

Privacy mechanisms

Similar to the first survey, we asked respondents to rate each mechanism on three dimensions: effectiveness, willingness to use, and practicality. Figure 2 shows the results of each mechanism from the second survey. Owner registration and face blurring received more support from both controllers and bystanders across all three measures than other mechanisms. Next, we will present people's perceptions of each mechanism

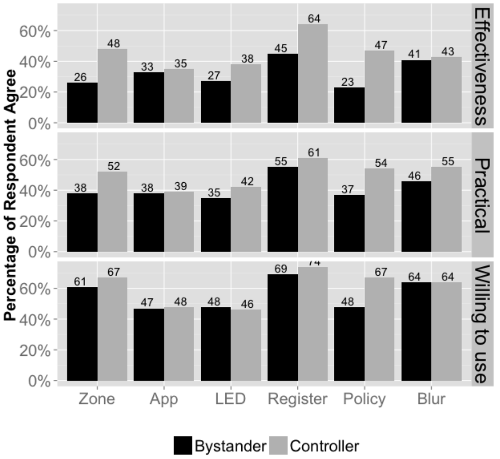

Figure 2. Survey 2 results on privacy mechanism: percentages of respondents who either "agree" or "strongly agree" that a privacy mechanism is effective, practical, and that they are willingness to use it. The six mechanisms include: no-fly-zone (zone), controller-bystander app (app), owner registration (register), and LED license (LED), privacy policy (policy), and automatic face blurring (blur).

based on their open-ended answers. Table 2 summarizes the perceived pros and cons of each mechanism.

No-fly-zone. Both controllers and bystanders appreciated its simplicity and low effort. One bystander highlighted, *"I think the concept of a no-fly database is simple enough, and practical enough because little is required to get your property included in it."* Many respondents also associated with the do-not-call list that they are familiar with. One controller said, *"I like this system and I think it's a unique idea. This would give bystanders the option of "opting out" of having drones around their space in much the same way as the "no call list" works for telemarketers."* In addition, bystanders mentioned that it will add a layer of control and responsibility over controllers. One respondent commented on this, *"I think this is effective because it's puts the responsibility mostly on the drone operator and allows bystanders to opt in or out"*.

However, both controllers and bystanders raised concerns about the lack of enforcement because of its voluntary nature. Many respondents suggested a law, for instance, *"I don't think the 'no fly zones' will be respected. There would have to be a law requiring the zones to be respected or it probably won't work."* Besides, both groups also raised practical issues due to proximity of addresses. One controller questioned, *"If my neighbor didn't want a drone flying near their house would that keep me from flying my drone ten feet away above my yard?"* Controllers also raised a practical concern about maintaining the large amount of data this mechanism may generate, as one controller noted, *"That would be a massive geographic database, with all the design, operation, and maintenance problems such a thing has."*

In addition to laws, some bystanders suggested making drones respect these no-fly-zone signals automatically. One respondent proposed a concrete strategy, *"Like, the drone operator gets a warning that they are within so many feet of a no-fly zone, and warnings up until they reach it, then the drone be deactivated if they ignore the warnings and enter the zone."* While completely automatic deactivation of drones might be unsafe, configuring the drones not to enter a no-fly zone is doable just like how some drones are configured to stay away from sensitive places like airports via geo-fencing [10].

Controller-bystander app. Both controllers and bystanders commended that it can enable or enhance the communications between bystanders and controllers. For example, one controller commented, *"Controller-bystander app is very effective way of using Drone.It provides direct way of communication between drone controllers and bystanders.So it gives ideal responses and accurate responses."* In addition, some controllers also felt it can increase the accountability of controllers. For example, one respondent expressed, *"I think the app will provide better protection to bystander and make the controller more accountable."* Allowing bystanders to see nearby drones and information about their usage would hold the associated controllers responsible for their behaviors.

However, both groups raised a potential privacy violation of controllers since their drone practices are tracked. One bystander put it vocally, *"I feel that this is a huge invasion of privacy for the drone owner him/herself. It seems that it will record all activity and where the drone is and where it has been and if it was used for pictures/video. This is worse than someone accidentally having their face recorded."* This highlights the trade-off between making drone usage transparent while protecting the controller's privacy.

In addition, many bystanders complained that this mechanism demands too much effort. One respondent commented, *"This requires a lot of work for the bystander. Some people will not know about this app and the fact that they can use it."* Even if they are aware of the app, they still need to install, learn how to use, and use the app. Another bystander expressed another common sentiment that this voluntary mechanism would fail to detain malicious controllers, *"This seems like an honor-system thing and I don't think that would solve much with people who are using drones inappropriately. They've already proven they won't follow an honor system."* To improve this mechanism, many bystanders mentioned that it needs to be mandatory. One respondent explained this point, *"I think maybe it would have to be mandatory to install and use this app to fly a drone or the operator could face federal charges. Maybe a live feed of what the drone is recording could be useful to bystanders"*. He suggested that installing and using the app should be required by regulation with penalties for not doing so.

LED license. Both controller and bystander respondents felt this mechanism can help identify drones and their controllers, as one bystanders simply noted, *"I think it would help in identifying the drones owner."* However, both groups also raised practical issues about this mechanism. One concern was that the LED lights can be obscured or altered by the controllers. For instance, one bystander said, *"there are some less honest people out there would be obscure the lights to prevent detection."* This comment also highlights his or her distrust to some drone controllers. Another respondent also talked about distrust and further suggested making the mechanism manda-

Mechanisms	Pros	Cons
1. Deletion request	+ Helpful if requests respected (bystander)	- Too much work for bystanders (bystander) - Controllers reject requests (bystander) - Too many requests (controller)
2. Gesture opt-out	+ Good solution if people know it (both)	- Too much work for bystanders (bystander) - Have to learn the gesture (both) - No need for opt-out (controller)
3. No-fly-zone	+ Simple and requires little effort (both) + Add control over controller (bystander) + Similar to no call list (both)	- No law enforcement (both) - Practical issues due to proximity (both) - Large amount of data (controller)
4. Drone owner registration	+ Practical in tracking down controllers (both) + Similar mechanism in other domains (both) + Discourage irresponsible use (bystander) + Mechanism already in use (controller)	- Not directly protect privacy (both) - Privacy issue for controllers (controller)
5. Controller-bystander app	+ Enhance communication (both) + Controller accountability (controller)	- Too much work for bystanders (both) - Privacy issues for controllers (both) - Responses not guaranteed (bystander)
6. LED license	+ Help identify controllers (both)	- LED patterns easy to change or hacked (both) - Camera not recognize the pattern (both) - Not directly protect privacy (both) - Too many possible patterns (controller)
7. Privacy policy	+ Peace of mind to bystanders (controller) + Information about drone use (controller) + Accountability for organizations (bystander)	- No one reads privacy policy (both) - Not directly protect privacy (bystander) - Policy not followed (bystander)
8. Automatic face blurring	+ Effective hiding people's identity (both) + Make people fell more secure (bystander)	- Conflict with drones' original purpose (both) - Inaccurate facial recognition (controller) - Can be turned off (bystander)

Table 2. Summary of the pros and cons of each mechanism suggested by drone controllers and bystanders. Each point is raised by bystanders, controllers, or both (denote in brackets). Mechanisms 1-6 and 3-8 were studied in the first and second survey, respectively. Data about mechanisms 1-2 was from the first survey, while data about mechanisms 3-8 was from the second survey because it had more detailed mechanism descriptions.

tory, *"That seems kind of silly, because people who are using drones maliciously will simply not sign up to register their drone. It needs to be made mandatory somehow upon purchase of a drone/built into all new drones."* Some controllers and bystanders suspected that cameras on phones are not good enough to capture the blinking sequence correctly. For instance, one response reads, *"it would be hard for a camera to pick up blinks with a phone camera."*

Some bystanders were also concerned about the effort needed including learning about, finding and downloading and then using the app. One respondent summarized, *"It's not practical to the every-day bystander. It's too much work for the average person to go through and they shouldn't have to go through such lengths to ensure their right to privacy."* In addition, some controllers complained that this mechanism can violate their privacy because people can see their information via the app. One respondent said, *"I wouldn't want just any bystander with an app to have the ability to look my info up."*

Drone owner registration. Bystanders generally praised that this mechanism can help make controllers more accountable for their drone practices. Some even suggested that people need to take lessons and get a license before they can operate drones. For example, one bystander suggested, *"This will help to hold flyers accountable for their actions while flying a drone and could be extended to require lessons and certification in the actual flight of the drone just like a drivers license."* This mechanism was also positively received by the controllers. In fact, many of them self-reported that they have already done the registration, which is required in the U.S.

However, many bystanders and controllers felt this mechanism does little to directly protect privacy. One bystander expressed, *"It seems like a good basic requirement, but would not necessarily protect people much."* Another controller believed this mechanism is more for safety than privacy, *"Owner registration is a good idea but it will not have any effect on "privacy". It will be more useful in identifying the owner in case of an accident with the drone.* In addition, some controllers were concerned about who can access their registration information. Many controllers felt their registration should only be accessible to the government. Furthermore, some controllers worried that this mechanism can increase the government's ability to track their activities. One respondent succinctly summarized both sides, *"I think it's a good and a bad thing. Good in that if someone is using their drone for illegal activity it would be easy to identify their drone information if they are reported. It's a bad thing because it's another way for the government to monitor people's activities."*

Privacy policy. Controllers noted that privacy policy can provide bystanders information about drone practices. One controller expressed, *"I think it is a decent policy. It would be easy to implement and would be good for bystanders who want to know what you're doing with the drone."* In addition, controllers also think that privacy policy can provide bystanders a peace mind, like a controller highlighted, *"I think it gives people more peace of mind about drones knowing they can request information on why they're being used."* However, others felt the policy does not directly protect privacy, as one respondent suggested *"it doesn't protect people of prevent anything"*. Other issues were brought up such as people usually do not read privacy policies. One controller said, *"I think this is a necessary feature, although I'm not sure how effective it will be. Most people do not pay attention to privacy policies in general."* This suggests that they felt this mechanism is needed but not sufficient by itself.

Bystanders generally appreciated this mechanism, feeling it will help hold controllers accountable. One bystander commented on this, *"This could help with accountability and discourage inappropriate behavior."* However, they also questioned whether organizations will follow their policies. One respondent was pessimistic about privacy policies, saying *"It's highly debatable how many organizations actually even follow their own privacy policies. This would do ZERO, literally ZERO to help curb privacy violations and privacy concerns."* This highlights the need for enforcement. In the US, the Federal Trade Commission can prosecute companies that do not follow their own privacy policies as deceptive practices.

Automatic face blurring. Both controller and bystander respondents valued this mechanism's potential in hiding people's identities. One controller commented, *"Auto blur would absolutely protect privacy."* Another bystander said, *"Seems practical enough because it's turned on by default. I would feel more safe should this feature be implemented."*

However, respondents also had reservations about this mechanism. One concern is that this mechanism can be useless because controllers can easily turn it off. One bystander said, *" If you can disable the setting, it is worthless. People all like to spy and see things so they won't care about privacy if they can disable the setting."* This quote also suggests that some bystanders had a lack trust of controllers. Another issue is that bystanders do not have an easy way to know whether this feature is turned on or off. Even if this feature is used, some respondents questioned whether this mechanism can be reversed. One controller believed, *"I'm sure any half way decent hacker can un-blur this picture."* Some controllers even criticized this mechanism. For instance, while this feature can be turned off, one respondent said *"It sounds stupid. And what if I'm trying to identify someone? I don't want anything blurred."* Some controllers also questioned the capability of this mechanism. For example, one controller said, *"I just don't think the facial recognition software can work fast enough to block out all faces as soon as they appear."* He suggested that he worried about the speed of face recognition, which would affect the effectiveness of the mechanism, or make *"false recognition"*. While this mechanism might not be able to blur faces during the recording, it has been shown to work on recorded images/videos.

Drone Usage Scenarios

We asked respondents to select the mechanism(s) they want to use in three concrete drone usage scenarios and explain why.

Real estate scenario. The largest percentages of bystanders selected these three mechanisms: no-fly-zone (64%), face blurring (61%), and privacy policy (38%). For controllers, it is the same set of mechanisms but in a different order: face blurring (51%), privacy policy (49%), and no-fly-zone (45%).

Bystander felt no-fly-zone can at least signal bystanders' privacy preferences. One bystander said, *"The no-fly zone mechanism would hopefully prevent the filming of your house and yard, or at least let the real estate company know that you are uncomfortable with those being filmed."* 45% of controllers indicated they would respect no-fly zones. One of them said, *"It would show which houses to avoid, as in, shoot from a different angle if a neighbor is on the list."*

Both groups also valued the face blurring mechanism as it can protect people's identity. One bystander explained, *"If it accidentally captures me, no identifying information will be shared."* Some controllers thought this mechanism might be able to extend to cover more than people's faces. For instance, one controller believed, *"It would hide those people and objects that might be picked up in the close proximity."*

Since this scenario is related to organizational use of drones, several bystanders and controllers thought privacy policy would be helpful. One bystander wrote, *"It would make me feel more secure about how they are using the information."* The information can increase the transparency of drone practices. One controller spoke about combining these mechanisms for better privacy protection, *"Given the purpose and who is controlling it, I think the privacy policy would be effective, but added protection of face blurring and, if I was so inclined, respecting my no-fly zone would be beneficial."*

Neighborhood safety scenario. In this scenario, the three most chosen mechanisms by bystanders were: privacy policy (48%), automatic face blurring (36%), and no-fly-zone (34%). Controllers instead chose: drone owner registration (49%), privacy policy (41%), and automatic face blurring (39%).

Many respondents desired both privacy policy and face blurring. In their views, privacy policy provides information and serves as notice, whereas face blurring protects their identities. For instance, one bystander explained, *"Considering the drone privacy policy, I would like to know how and to what extent the police will be using this footage. Since they will be on constant patrol, I would like to have all faces blurred to protect anonymity and privacy."* One controller raved about face blurring because it needs little effort, *"Because it's the best one. Most people won't bother with the others, and that would automatically protect the identities of people."* Some bystanders also selected no-fly-zone, despite the potential public safety issues, believing it is easy to enforce. One bystander said, *"we can advocate for our home to be no fly despite this being law enforcement and the street around the home is still* *being viewed"*. Besides, some controllers voted owner registration as a way for bystanders to contact controllers. One respondent suggested, *"People could also check the drone's registration in case they need to contact the drone operator."*

Public park scenario. Bystanders preferred face blurring (82%), controller-bystander app (31%), and drone owner registration (31%). Controllers preferred face blurring (71%), drone owner registration (39%), and privacy policy (29%).

Many bystanders and controllers considered face blurring the most effective mechanism partly because its protection for children. One bystander explained, *"The face blurring thing is the best option to protect their children and the families at the park since there is nothing else that can be done about it."* Some bystanders liked the combination of owner registration and controller-bystander app. For instance, one respondent said, *"It would be helpful to know the drone is registered with the FAA and the controller-bystander app would be perfect in this case. It would make the bystander feel safer and may even help to make friends."* Using these two mechanisms together both ease bystanders and could also help them socialize with others. Another bystander further illustrated the use of the app, *"I believe in asking for something. "Please do not record myself or my family, thank you." would send a polite and clear message."* Privacy policy was also favored by some controllers. One controller believed, *"It will allow the family to know who I am and what I'm up to."* This information could also help mitigate the privacy concerns that the family might have.

DISCUSSION

Our results suggest that our bystander respondents had more privacy concerns about drones than their controller counterparts. In addition, the two groups' perceptions of privacy mechanisms for drones often differed. The differences between controllers and bystanders are perhaps not surprising because of their roles. Their behaviors can be thought as the in-group (controllers) versus out-group (bystander) behavior in an inter-group process (drone operations) [4]. In drone operations, controllers directly operate the drones and they presumably focus on utilizing and enjoying drones, whereas bystanders do not participate in drone operations and thus mainly consider protecting their welfare such as safety and privacy against drones.

Privacy Mechanisms for Drones

While the privacy mechanisms that we explored are not exhaustive, they cover a wide range of designs ranging from technical mechanisms (e.g., LED license and face blurring) to policy mechanisms (e.g., own registration and privacy policy). These privacy mechanisms can be roughly categorized into three groups based on our respondents' ratings of and feedback on each mechanism.

While no mechanism was perceived as a silver bullet, owner registration and face blurring) gained most support from both bystanders and controllers than other mechanisms. This matters because the results suggest these two mechanisms are more likely to be adopted by controllers and to mitigate bystanders' privacy concerns. In other words, they are more likely to succeed in practice. Owner registration is already in use and is well received by both groups. Face blurring has not been applied for drones but should be considered by drone manufacturers as a useful privacy feature. Privacy policy and no-fly-zone also received support, albeit more controllers perceived them to be practical and effective than bystanders. This result suggest while controllers may adopt these two mechanisms, bystanders may consider these mechanisms ineffective in addressing their privacy concerns.

The remaining four mechanisms received less support than the previous mechanism. This does not mean they are completely useless. For instance, in the public park scenario, the second most selected mechanism by bystanders was the controller-bystander app because it allows them to directly communicate with controllers about their privacy concerns about the drone. Prior research shows that bystanders are concerned about drone controllers being invisible or inaccessible that they could not communicate with [28]. The FAA has promulgated new drone safety rules, such as prohibiting flight over people and night operations, and requiring drones to be in visual line of sight of the drone controllers [15]. These new rules do not require drones nor drone controllers to be visible to bystanders. Therefore, bystanders' concern about invisible controllers remains unaddressed. The controller-bystander app can allow bystanders to contact controllers, but our controller respondents did not value this mechanism as much.

The scenario-based results also suggest that respondents' desires of using multiple mechanisms. For instance, privacy policy and owner registration were often considered helpful but not sufficient because they do not directly protect people's privacy as many respondents put it. Therefore, our respondents often combined multiple mechanisms such as privacy policy, owner registration, and face blurring since they can improve different aspects of privacy. For instance, privacy policy can provide notice about drone usage, owner registration can help hold controllers accountable, and face blurring can hide bystanders' identities.

Important Privacy Design Questions for Drones

Many bystander respondents perceived voluntary mechanisms as ineffective because some controllers would simply ignore the mechanisms. For instance, controllers can ignore the no-fly-zone signals and deletion requests or turn off the automatic face blurring. In the case of LED license, some bystanders even suspected that controllers may hack the lights so that people cannot capture the correct "light" license. These perceptions surface a general lack of trust that bystanders have for controllers. This distrust might be attributed to the lack of information/transparency about drones and their controllers, and the lack of required privacy standards for drones. Similarly, our controller respondents sometimes distrusted bystanders too. For instance, in the case of deletion requests, some controllers felt that bystanders may abuse this mechanism by sending them an overwhelming number of requests.

The lack of trust between controllers and bystanders highlights an important privacy design question for drones - how to nurture the trust between the two groups? Prior research has shown that lack of trust is an antecedent to privacy concerns [25]. One direction to mitigate privacy concerns about drones is to improve bystanders' perceived trust to controllers. When controllers are organizations, we can learn from the e-commerce literature, which has shown that companies can build consumer trust and thus reduce consumer privacy concerns by a number of measures such as adopting fair information practices (e.g., notice and consent) [8], presenting privacy policies [12], and displaying privacy notices or seals [26]. The mechanisms we studied cover some of these ideas, for instance, privacy policy and gesture opt-out (user consent). Displaying privacy notices or seals directly on a drone might be hard for people to see or read, but they could be shown on the information page of the drone once people have identified a drone by the LED license or controller-bystander app for instance. When the controllers are individual users, we can learn from ways to increase interpersonal trust such as providing transparency in decision-making (e.g., why use drones to take pictures) and holding people accountable [1]. Many respondents commanded that the controller-bystander app and owner registration help hold controllers accountable.

In addition, our respondents suggested using laws or technical methods to enforce these voluntary mechanisms. For instance, some controllers suggested "hard coding" no-fly-zone into drones that automatically block them from flying into the no-fly-zone. This is known as geo-fencing, which currently works for sensitive locations such as airports and does not include people's homes. Other respondents suggested making laws to require and enforce mechanisms such as no-fly-zone, privacy policies, and face blurring.

While bystanders valued their privacy, controllers were also concerned about protecting their own privacy. For instance, when considering owner registration and controller-bystander app, many controllers did not want bystanders (in theory, almost anyone can be a bystander) to know their information. Some controllers also expressed concerns about these mechanisms could increase government's abilities to track them. Therefore, another important privacy design question for drones is - how to balance the privacy of bystanders and controllers. For instance, one idea to help protect controllers' privacy against bystanders is that bystanders can only report problematic drones to the government using the controller's registered ID but cannot access other controller information. Alternatively, bystanders can only view a controller's information when they are physically close to the operating drone.

Another important question is how much effort a mechanism requires a bystander or controller. If people think a mechanism demands a lot of effort, then they are unlikely to use it because privacy is often not their main or immediate goal. Deletion request, gesture opt-out, and controller-bystander app were not rated higher partly because they were considered as requiring too much effort from bystanders. In addition, many bystanders believed that it is the controllers' responsibilities to protect the bystanders' privacy. However, this can be a risky belief because controllers may protect their own privacy at the cost of bystanders' privacy. One reason that face blurring was highly rated is because it requires minimum effort from controllers and no effort from bystanders.

Many common privacy strategies are challenging to implement in the context of drones. For instance, it is hard to implement user consent when a drone is operating in a public space (e.g., a park) where there are many people present. Do we require the drone controller to get consent from each person before flying the drone or using the drone to take pictures/videos? What if bystanders have conflicting preferences? Another example is providing privacy notice. Since drones are flying in the air, it is difficult for people to see or read any privacy notice on the drones. How to help bystanders identify/locate drones' privacy policies or notices, and understand what privacy mechanisms have been applied is also important for future privacy designs.

Lastly, privacy has been a key research theme in the HCI history and the CHI community. Our research highlights that the design of human-drone interaction should not only consider controller-drone interaction but also the indirect involvement of bystanders, as their privacy can be intentionally or inadvertently violated by drone operations. Identifying privacy mechanisms that are supported by both controllers and bystanders will inform the development of public policies and future designs of drone technologies.

Study Limitations

First, we cannot guarantee that all controller respondents are actually drone controllers. However, we double checked with the open-ended question on what brand/model of drones they have and they had reasonable answers.

Second, our sample cannot generalize to all drone controllers and bystanders. We recruited respondents from Amazon Mechanical Turk and multiple drone forums. We also focused on the U.S. Thus, our results may not apply in other countries.

Third, the privacy mechanisms studied in our research are by no means exhaustive, but we chose a diverse set of technology-focused and policy-focused mechanisms. While we attempted to provide detailed and realistic descriptions of these mechanisms, some descriptions are hypothetical because the described mechanisms have not been fully implemented in practice and we had to imagine their implementations. Besides, the drone usage scenarios are hypothetical, but they were modeled largely after real-world uses of drones.

Lastly, our study focused on people's perceptions of drone privacy mechanisms rather than people's real adoption behavior. However, we note that people's perceptions or behavioral intentions (e.g., willingness to use a mechanism) is important to study because they can influence people's real behaviors.

CONCLUSION

While drones can enable many innovative applications, their usage may also infringe on ordinary citizens' privacy. We conduct a series of survey to investigate how drone controllers and bystanders perceive a diverse set of privacy mechanisms for drones. Our respondents raised various pros and cons of each mechanism. While drone owner registration and face blurring received most support individually by both groups, respondents preferred to use a combination of mechanisms. We highlight a number of important questions for future privacy designs and policies of drones.

REFERENCES

1. Lisa C. Abrams, Rob Cross, Eric Lesser, and Daniel Z. Levin. 2003. Nurturing interpersonal trust in knowledge-sharing networks. *The Academy of Management Executive* 17, 4 (Nov. 2003), 64–77. DOI: http://dx.doi.org/10.5465/AME.2003.11851845

2. 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.

3. 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

4. Rupert Brown and Sam Gaertner (Eds.). 2002. *Blackwell Handbook of Social Psychology: Intergroup Processes*. Wiley-Blackwell, Malden, MA etc.

5. 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

6. Jessica R. Cauchard, Jane L. E, Kevin Y. Zhai, and James A. Landay. 2015. Drone & Me: An Exploration into Natural Human-drone Interaction. In *Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp '15)*. ACM, New York, NY, USA, 361–365. DOI: http://dx.doi.org/10.1145/2750858.2805823

7. 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).

8. Mary J. Culnan and Pamela K. Armstrong. 1999. Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. *Organization Science* 10, 1 (Jan. 1999), 104–115. DOI: http://dx.doi.org/10.1287/orsc.10.1.104

9. 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.

10. DJI. 2015. DJI Introduces New Geofencing System for its Drones. (2015). http://www.dji.com/newsroom/news/dji-fly-safe-system

11. 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.

12. Mary Ann Eastlick, Sherry L. Lotz, and Patricia Warrington. 2006. Understanding online B-to-C relationships: An integrated model of privacy concerns, trust, and commitment. *Journal of Business Research* 59, 8 (Aug. 2006), 877–886. DOI: http://dx.doi.org/10.1016/j.jbusres.2006.02.006

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

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

15. FAA. 2016. *Summary of the Small UAS Rule*. Technical Report. https://www.faa.gov/uas/media/Part_107_Summary.pdf

16. A. Frome, G. Cheung, A. Abdulkader, M. Zennaro, B. Wu, A. Bissacco, H. Adam, H. Neven, and L. Vincent. 2009. Large-scale privacy protection in Google Street View. In *2009 IEEE 12th International Conference on Computer Vision*. 2373–2380. DOI: http://dx.doi.org/10.1109/ICCV.2009.5459413

17. 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

18. 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.

19. 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.

20. 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.

21. LightCense. 2016. LightCense. (2016). http://www.lightcense.co/

22. National Telecommunications and Information Administration. 2016. *Voluntary Best Practices for UAS Privacy, Transparency, and Accountability*. Technical Report. https://www.ntia.doc.gov/files/ntia/publications/voluntary_best_practices_for_uas_privacy_transparency_and_accountability_0.pdf

23. 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

24. NoFlyZone. 2016. NoFlyZone. (2016). https://www.noflyzone.org/

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

26. Sijun Wang, Sharon E. Beatty, and William Foxx. 2004. Signaling the trustworthiness of small online retailers. *Journal of Interactive Marketing* 18, 1 (2004), 53–69. DOI:http://dx.doi.org/10.1002/dir.10071

27. 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.

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