Privacy Mechanisms for Drones: Perceptions of Drone Controllers and Bystanders

Yaxing Yao, Huichuan Xia, Yun Huang, Yang Wang
SALT Lab, School of Information Studies, Syracuse University
[yyao08, hxia, yhuang, ywang]@syr.edu

ABSTRACT

Drones pose privacy concerns such as surveillance and stalking. Many technology-based or policy-based mechanisms have been proposed to mitigate these concerns. 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 in the U.S. We identified respondents' perceived pros and cons of eight privacy mechanisms. We found that *owner registration* and *automatic face blurring* individually received most support from both controllers and bystanders. Our respondents also suggested using varied combinations of mechanisms under different drone usage scenarios, highlighting their context-dependent preferences. We outline a set of important questions for future privacy designs and public policies of drones.

ACM Classification Keywords

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

Author Keywords

Drone; UAS; UAV; 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 example, the Electronic Privacy Information Center highlights surveillance as a key privacy issue of drones [14].

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 [26]. Many technical privacy mechanisms for drones 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 [25]. However, most of these technical or policy-based mechanisms are voluntary and thus it is unclear whether people will adopt them and even if adopted, whether they would be effective.

In this paper, we focus on *how drone controllers and bystanders perceive these technology-based or policy-based privacy mechanisms for drones.* We define drone *controllers* as people who have operated drones and *bystanders* as people who have not operated drones but could be surrounded by flying 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 may remain largely unaddressed, potentially hindering the acceptance and adoption of drones and limiting their benefits to society. Privacy mechanisms that are supported by both drone controllers and bystanders have great potential to be adopted and useful in practice.

To answer the 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. In this research, we focus on drones that are used for civilian purposes, excluding military usage. We found that when considering individual mechanisms, owner registration and automatic face blurring received most support from both controllers and bystanders. However, under specific drone usage scenarios, our respondents also suggested using multiple mechanisms together as they may contribute to different aspects of privacy. But, the choices of mechanisms varied across different scenarios.

This paper makes three main contributions. First, it sheds lights on how drone controllers and bystanders think about different types of privacy mechanisms for drones. Second, it not only discusses ways to improve these specific mechanisms but also outlines important questions for future privacy designs for drones. Third, it makes a public policy contribution. While most of the studied privacy mechanisms are currently voluntary, they could become mandatory in the future. The findings on people's attitudes towards and perceived effectiveness of these privacy mechanisms can inform the policy development, for instance, mandating certain mechanisms.

CHI 2017, May 06 - 11, 2017, Denver, CO, USA

ACM 978-1-4503-4655-9/17/05...$15.00
DOI: http://dx.doi.org/10.1145/3025453.3025907

RELATED WORK

Perceptions of Tracking and Recording Technologies

Since drones often carry cameras, they are a type of tracking and 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 [27].

Prior research has also studied people's perceptions of wearable devices (e.g., glasses). For instance, Denning et al. find that people expect giving their permissions before Augmented Reality (AR) glasses can record them [10]. These wearable devices can also enable "lifelogging" where photos or videos can be automatically taken by these devices (e.g., SenseCam [20]) in a person's everyday life. Hoyle et al. find that people have various privacy concerns about lifelogging, for instance, sensitive information such as lifeloggers' locations or credit card numbers as well as bystanders' faces or behaviors appearing in the "lifelog" [21]. In addition, robots equipped with cameras can also be considered as a type of tracking and recording technology. For instance, Butler et al. find that people desire mechanisms to help protect their privacy in the presence of remotely tele-operated in-home robots [6]. Our work adds to this literature of tracking and recording technologies but focuses on drones.

Privacy Issues of Drones

Similar to other tracking and recording technologies, legal scholars have argued that drones can infringe on citizens' privacy. For instance, Dunlap posits that when drones are used for surveillance they can violate the Fourth Amendment of the US Constitution, which protects citizens from unreasonable searches and seizures [12]. 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, albeit equipped with high-definition cameras (e.g., "dragonfly drones") [33]. As a result, drones could take detailed pictures of people and it would be difficult for people to notice the drones and to realize they are being recorded by the drones [33].

There are few empirical studies of drone privacy. A survey of Australians' perceptions of drones 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 [8]. Our previous interview study of drone bystanders find that they had various privacy concerns about drones and their perceptions of drones varied in different scenarios [34]. Unlike these prior studies, we focus on specific privacy mechanisms for drones in this research.

Privacy Mechanisms for Drones

Several mechanisms have been proposed that either directly or indirectly protect people's privacy against drones. For instance, traditional "sense and avoid" systems for drones have been re-designed so that minimum personal data will be retained by the drones [3, 19]. In addition, B4UFLY, a mobile app, was designed to help drone controllers "determine whether there are any restrictions or requirements in effect at the location where they want to fly" [15]. Besides, a type of geo-fencing was proposed to allow individual citizens to designate their addresses as drone no-fly zones, which can be incorporated into the software or firmware of drones and/or honored by drone controllers [28]. LightCense uses a blink sequence of LED lights on a drone as its ID [25]. To learn information about a particular drone, people can use a mobile app to scan the blinking light sequence to identify the drone and look up its information [25]. There are also server-side privacy mechanisms for drones. For instance, Yoohwan et al. propose a system that enables encryption, access control, and image/video transformation of drone recorded data [22]. The NTIA recommends a number of voluntary best practices for drone usage, such as informing bystanders before drones taking pictures/videos if possible [26]. However, it is unclear how people perceive these mechanisms and whether they will be adopted. To fill this gap, we surveyed drone controllers and bystanders, asking them to assess a diverse set of privacy mechanisms for drones.

METHODOLOGY

We conducted two rounds of online survey of drone controllers and bystanders. Both surveys focused on respondents' assessment of specific privacy mechanisms for drones. After conducting survey one, we learned many things that can improve the survey. For instance, many respondents felt the descriptions of privacy mechanisms were not detailed enough and they raised many questions about the specifics. Therefore, we conducted survey two, which was very similar to survey one but differed in three main aspects: making descriptions of privacy mechanisms more detailed, testing a slightly different set of privacy mechanisms, and including specific drone usage scenarios and demographic questions.

We recruited survey respondents from Amazon Mechanical Turk (MTurk) where workers were based in the US and had at least 95% task acceptance rate. We also recruited respondents from drone user forums such as the DJI forum and the Quadcopter.com forum. We conducted survey one during March 2016 and received a total of 456 valid responses including 385 bystanders and 71 drone controllers. We conducted survey two 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 about 100 controller respondents from drone forums and administrated a raffle of four $50 gift cards. This research was approved by the Syracuse University IRB office.

Survey Flow

For both surveys, we first provided a working definition of drones as "an unmanned aircraft guided by remote control or onboard computers" and a photo of a DJI Phantom 2 as an example drone. We also told the respondents to focus on civilian not military uses of drones. Next, we asked "have you ever flown a drone yourself?" If a respondent answered yes, then he or she would answer the controller branch of the survey; otherwise, answer the bystander branch. We told controller and bystander respondents to answer the remaining questions by representing themselves as a controller or a bystander, respectively.

We then provided each respondent descriptions of a set of privacy mechanisms in a randomized order. For each mechanism, we asked respondents to answer three questions (5-point Likert scale): “How practical do you think this mechanism will work? Are you willing to use this mechanism if it is implemented? If this mechanism is implemented, how effective do you think it will protect people’s privacy regarding drones?” Respondents were then asked to provide open-ended answers to explain their ratings. The Likert-scale questions were inspired by our prior interview study of bystanders where the interviewees talked about practicality and effectiveness of, as well as effort/willingness to use a privacy mechanism when they proposed ways to address their privacy concerns [34]. We checked the open-ended answers and found them to be consistent with the corresponding Likert-scale ratings, suggesting the Likert-scale questions were understood correctly.

Survey One

We created brief descriptions of six privacy mechanisms based on the literature and industry proposals. These mechanisms varied by their types (e.g., technology vs. policy, proactive vs. reactive). Below are the descriptions (bystander version). We denote each mechanism in a format of Name (Short name).

Deletion request (Delete): Drone controllers can receive requests from me to delete photos or videos that capture my family, properties or myself via a mobile app [34]. **Gesture opt-out (Gesture)**: 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) [7]. **No-fly-zone (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 [28]. **Owner registration (Register)**: 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 [16]. **Controller-bystander app (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 [34]. **LED license (LED)**: 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) [25].

For controllers, these descriptions 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.” Survey one also had many privacy concern questions. Since they are not the focus of this paper, we do not report them here. Besides, we did not ask about demographics due to the survey length.

Survey Two

Privacy mechanisms. In survey two, we removed two mechanisms from survey one, i.e., deletion request and gesture opt-out, because they were not well supported by both groups of respondents, as well as they have not been implemented and are challenging to implement in practice. We added two new mechanisms: privacy policy (Policy) and automatic face blurring (Blur). After survey one, in June 2016, the NTIA recommends organizational users of drones to have a privacy policy that describe their drone uses and the related data practices [26]. The face blurring mechanism was modeled after a Google Street View privacy feature that has been used to automatically detect human faces and blur them [18]. For each mechanism, we tried to describe what it does, how it is implemented, and what controllers and bystanders need to do to use it. To make these mechanisms more comparable, we framed them as administrated/suggested by the US Federal Aviation Administration (FAA). Below are the descriptions.

No-fly-zone (Zone) is implemented using a database maintained by the 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.

Owner registration (Register): Every drone owner in the US must register with the 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.

Controller-bystander app (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 app is operated by the 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 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 areas 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 license (LED): 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 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.

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

We aimed to model these mechanisms realistically. Some mechanisms have 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). The controller-bystander app has been proposed but not implemented [34]. All mechanisms are voluntary except for owner registration, which is required 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 complexities from users' perspective.

Scenarios. Next, we provided respondents three concrete drone usage scenarios, adopted from our prior work [34]. Below are the descriptions.

Neighborhood safety scenario: 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. The drones will be streaming a live video feed to the police department but will not record any photos or videos.

Public park scenario: 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 scenario: A real estate agency company hires a drone controller to shoot photos and videos of a house for sale. When the controller flies the drone to take photos and videos of the house, these recordings might capture your houses and/or your backyard.

These scenarios varied by the type of 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. We finished with demographic questions such as age and gender.

Data Analysis

We computed descriptive statistics of the quantitative data (e.g., 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" [4]. 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 pros (e.g., easy, practical, effortless, similar to existing mechanisms) and cons of 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, restricting access to the controller data). We then used the code book to code the rest of the open-ended data.

RESULTS

We now report drone controller and bystander respondents' quantitative ratings of and qualitative feedback on different privacy mechanisms in both surveys.

Results of Survey One

Figure 1 shows the percentages of controller and bystander respondents who were either "positive" or "very positive" that a privacy mechanism is effective, practical, and that they are willingness to use it. For instance, 51% of bystanders thought owner registration is practical, whereas 42% of bystanders thought so for LED license. Therefore, we say that owner registration received more support than LED license, from bystanders, based on the practicality measure. In general, owner registration and no-fly-zone received more support than the other four mechanisms tested in this survey, from both bystanders and controllers, across all three measures.

Since we removed deletion request and gesture opt-out from survey two, we will focus on people's qualitative feedback on these two mechanisms here. We will discuss the feedback on the other four mechanisms using the data from survey two because it had more detailed mechanism descriptions and a wider range of feedback than survey one. Whenever possible, we report the percentages of bystanders and controllers expressing a main opinion of a mechanism.

Deletion request (Delete). Many bystanders (17%) felt this mechanism can be useful if their requests are honored. Some bystanders also raised two main issues: (1) there is too much work for bystanders (22%), and (2) controllers may ignore/reject the requests (15%). 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."* For controllers, some of them (5.9%) felt this mechanism is unnecessary partly because they only publish photos that they deem safe to post. Besides, some controllers (6%) were concerned that bystanders can abuse this mechanism by sending an overwhelming number of requests.

Gesture opt-out (Gesture). Many controllers (29%) and bystanders (10%) thought this can be a good solution if people know it. The burden is on the bystanders to learn the gesture. However, some bystanders (15%) argued that it is the 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."* On the other hand, some controllers (6%) felt there is really no need for opt-out because drone cameras are usually not good enough to capture people's faces 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.

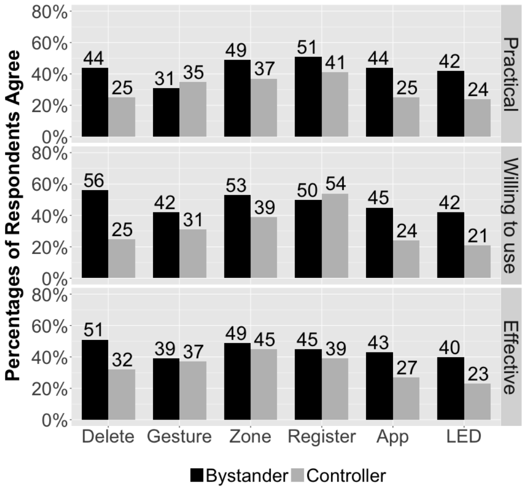

Figure 1. Survey one results: percentages of bystander and controller respondents who were either "positive" or "very positive" that a privacy mechanism is practical, effective, and that they are willing to use it. The six mechanisms include (left to right): Delete request (Delete), Gesture opt-out (Gesture), No-fly-zone (Zone), Owner registration (Register), Controller-bystander app (App), and LED license (LED).

Results of Survey Two

In survey two, 42% of bystanders were male and 58% were female, whereas 66% of controllers were male and 34% were female. In terms of age, controllers (20% 18-25, 52% 26-35) were slightly younger than bystanders (14% 18-25, 42% 26-35). 70% of controllers had less than one year of experience in drone usage and 30% had more than one year of experience. Most bystanders were not familiar with drones.

Recall that survey two also tested six privacy mechanisms, excluding deletion request and gesture opt-out from survey one, but including the other four mechanisms from survey one as well as two new mechanisms: privacy policy and automatic face blurring. Similar to Figure 1 of survey one, Figure 2 shows the rating results of the six mechanisms in survey two. In general, owner registration and automatic face blurring received more support than the other four mechanisms tested in this survey, from both bystanders and controllers, across all three measures. Since the controllers and bystanders differed in their age and gender distributions, we controlled for these demographic differences by taking subsets of the original data set and checking the subset results. For instance, we extracted the data of all female respondents of age 26-35, and compared the controllers and bystanders within this subset. The subset results were in line with the results in Figure 2.

Next, we present respondents' qualitative feedback on each mechanism. Table 1 summarizes the perceived pros and cons of each mechanism in survey one and two. We provide examples of these opinions below.

No-fly-zone (Zone). Both controllers (30%) and bystanders (20%) appreciated this mechanism is simple and requires little 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 from both groups also associated it with

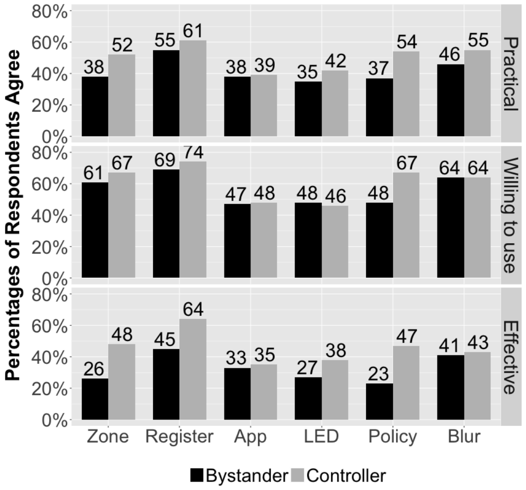

Figure 2. Survey two results: percentages of bystander and controller respondents who were either "positive" or "very positive" that a privacy mechanism is practical, effective, and that they are willing to use it. The six mechanisms include (left to right): No-fly-zone (Zone), Owner registration (Register), Controller-bystander app (App), LED license (LED), Privacy policy (Policy), and Automatic face blurring (Blur).

the do-not-call list that they were already 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, some bystanders thought it will add a layer of control and responsibility over controllers. For instance, one bystander said, *"I think this is effective because it puts the responsibility mostly on the drone operator and allows bystanders to opt in or out."*

However, both controllers (28%) and bystanders (55%) raised concerns about the lack of enforcement because of its voluntary nature. Many respondents from both groups suggested mandating this mechanism by legislation. For instance, a controller said *"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."* This speaks to the concern that some controllers might choose to ignore this mechanism. Besides, both groups (controller: 14%, bystander: 13%) 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?"* Some controllers (5%) 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. For instance, a bystander proposed, *"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 similar to how some drones are configured to stay away from sensitive places such as airports via geo-fencing [11].

Owner registration (Register). Many bystanders (43%) 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 driver's license."* This mechanism was also positively received by the controllers (42%). In fact, many of them self-reported having done the registration, which is required in the US by the FAA.

However, many bystanders (39%) and controllers (28%) felt this mechanism does little to directly protect people's privacy. One bystander expressed, *"It seems like a good basic requirement, but would not necessarily protect people much."* Another controller believed it is more for safety than privacy, saying *"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 (5%) were concerned about who can access their registration information and explicitly mentioned that only the government can access that information. Furthermore, some controllers worried that this mechanism can increase the government's ability to track their activities. One controller summarized the pros and cons, saying *"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."*

Controller-bystander app (App). Both controllers (19%) and bystanders (21%) commended that this app can enable or enhance the communication between bystanders and controllers. For example, one controller said, *"Controller-bystander app is a very effective way of using Drone. It provides a direct way of communication between drone controllers and bystanders."* Some respondents (controller: 3%, bystander: 10%) also felt it can increase the accountability of controllers. For example, one bystander expressed, *"I think the app will provide better protection to bystanders 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, some controllers (12%) and bystanders (2%) raised a potential privacy violation of controllers since their drone practices are tracked. One controller complained, *"I feel that this is a huge invasion of privacy for the drone owner him/herself. It seems that it will record all activities 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 challenge of making drone usage transparent while protecting controllers' privacy.

In addition, many bystanders (27%) complained that this mechanism demands too much effort. One bystander commented,

Mechanisms	Pros	Cons
1. Deletion request (Delete)	+ Helpful if requests are respected (both)	- Too much work for bystanders (both) - Controllers can ignore or reject requests (both) - Too many requests (controller)
2. Gesture opt-out (Gesture)	+ Good solution if people know about it (both)	- Too much work for bystanders (both) - Have to learn the gesture (both) - No need for opt-out (both)
3. No-fly-zone (Zone)	+ Simple and requires little effort (both) + Add control over controllers (bystander) + Similar to do-not-call list (both)	- No law enforcement (both) - Practical issues due to proximity of homes (both) - Large amount of data (controller)
4. Owner registration (Register)	+ Practical in tracking down controllers (both) + Similar mechanisms in other domains (both) + Discourage irresponsible use (bystander) + This mechanism is already in use (controller)	- Not directly protect privacy (both) - Privacy issue for controllers (controller)
5. Controller-bystander app (App)	+ Enhance controller-bystander communication (both) + Improve controller accountability (both)	- Too much work for bystanders (both) - Privacy issues for controllers (both) - Responses not guaranteed (bystander)
6. LED license (LED)	+ Help identify controllers (both)	- LED patterns can be changed or hacked (both) - Phone camera cannot recognize the pattern (both) - Not directly protect privacy (both) - Too many possible patterns (controller)
7. Privacy policy (Policy)	+ Give bystanders peace of mind (controller) + Provide information about drone use (controller) + Hold organizations more accountable (bystander)	- People rarely read privacy policies (both) - Not directly protect privacy (bystander) - Policy not followed (bystander)
8. Automatic face blurring (Blur)	+ Effective in hiding people's identity (both) + Make people feel more secure (bystander) + Need little effort, turn on by default (both)	- Conflict with controllers' purpose of use (both) - Slow or inaccurate facial recognition (controller) - Can be turned off (both)

Table 1. The pros and cons of each mechanism suggested by controllers and bystanders. We denote each point as raised by bystanders only, controllers only, or both. Mechanisms 1-6 and 3-8 were studied in survey one and two, respectively. Data about mechanisms 1-2 was from survey one, while data about mechanisms 3-8 was from survey two because it had more detailed mechanism descriptions and a wider range of feedback than survey one.

"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 actually use the app. Another bystander felt this voluntary mechanism would fail to detain malicious controllers, saying *"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."* This highlights the concern that some controllers may intend to bypass this mechanism. To improve this mechanism, many bystanders proposed that controllers should be required to use it by regulations. For instance, one bystander suggested, *"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."*

LED license (LED). Many controllers (22%) and bystanders (16%) felt this mechanism can help identify drones and their controllers, as one bystanders noted, *"I think it would help in identifying the drones owner."* However, both groups (controller: 38%, bystander: 50%) also raised practical issues, such as 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 underlies the concern that some controllers may intend to circumvent this mechanism. Another bystander further suggested mandating this mechanism, *"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."* In addition, a few controllers (8%) and bystanders (11%) suspected that cameras on phones are not good enough to capture the blinking sequence correctly. For instance, one controller said, *"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 bystander 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 controller said, *"I wouldn't want just any bystander with an app to have the ability to look my info up."*

Privacy policy (Policy). Many controllers (16%) noted a privacy policy can provide bystanders information about drone practices. One controller said, *"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."* Besides, some controllers (12%) thought it can provide bystanders peace of mind, as one controller explained, *"I think it gives people more peace of mind about drones knowing they can request information on why they're being used."* However, some respondents from both groups (controller: 4%, bystander: 21%) felt it does not directly protect privacy, as one bystander put it, *"it doesn't protect people of prevent anything."* Another issue was that people rarely read privacy policies (controller: 14%, bystander: 16%). 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. Some bystanders (8%) also felt it will help hold controllers accountable. One bystander said, *"This could help with accountability and discourage inappropriate behavior."* However, many bystanders (32%) also questioned whether organizations will follow their policies. One bystander was pessimistic, 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 (Blur). Many controllers (22%) and bystanders (18%) valued this mechanism's potential in hiding people's identities. One controller commented, *"Auto blur would absolutely protect privacy."* One bystander said, *"Seems practical enough because it's turned on by default. I would feel more safe should this feature be implemented."*

However, both groups also had reservations about this mechanism. Some controllers (27%) and bystanders (48%) were concerned that this mechanism can be useless because controllers can easily turn it off. For instance, 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."* Another issue was that bystanders do not have an easy way to know whether this feature is on or off. Even if it is on, some controllers and bystanders suspected that it can be reversed. One controller commented, *"I'm sure any half way decent hacker can un-blur this picture."* This comment highlights the concern that some controllers may have the ability to circumvent the mechanism. Some controllers complained that this mechanism is on by default. For instance, one controller said *"It sounds stupid. And what if I'm trying to identify someone? I don't want anything blurred."* A few controllers (8%) 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."* While this mechanism might not be able to blur faces during the recording, it has been shown to work well on recorded images/videos [18].

Drone Usage Scenarios

We next asked respondents to select the mechanism(s) they want to use under three concrete scenarios and explain why. They all chose their preferred individual mechanisms and many also suggested using multiple mechanisms together. Their choices of mechanisms varied across scenarios, showing their context-dependent preferences.

Neighborhood safety scenario. In this scenario, the largest percentages of bystanders chose the following three mechanisms: 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. They felt that a privacy policy provides information and serves as a notice and 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."*

Public park scenario. In this 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 bystander explained, *"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."* This comment also suggests that the app can help people socialize. Another bystander added, *"I believe in asking for something. 'Please do not record myself or my family, thank you.' would send a polite and clear message."*

Real estate scenario. In this scenario, the three most chosen mechanisms by bystanders were: no-fly-zone (64%), face blurring (61%), and privacy policy (38%). For controllers, it was the same set of mechanisms but in a different order: face blurring (51%), privacy policy (49%), and no-fly-zone (45%). Bystanders felt no-fly-zone can at least signal their intent to opt out. 45% of controllers indicated they would respect no-fly zones. One controller 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 identities. Since this scenario was related to organizational uses of drones, several bystanders and controllers thought that a privacy policy would be helpful. One controller also suggested combining multiple 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."*

DISCUSSION

We discuss respondents' perceptions and relative preferences of different mechanisms as well as important questions for how to address privacy challenges of drones.

Perceptions and Preferences of Privacy Mechanisms

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 two 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 relatively more support from both bystanders and controllers than other mechanisms. This matters because this result suggests these two mechanisms are more likely to be adopted and to help mitigate bystanders' privacy concerns. In other words, they have great potential to succeed in practice. Owner registration was already in use and was perceived by both controllers and bystanders as useful but insufficient by itself. Face blurring was perceived by both groups as useful and something that requires little effort. It 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 some support, albeit more controllers perceived them to be practical and effective than bystanders. This suggests that while controllers may adopt these two mechanisms, bystanders may consider them ineffective. The remaining four mechanisms received even less support, but 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. Our prior research shows that bystanders are concerned that drone controllers can be invisible or cannot be reached for communication [34]. 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 [17]. These new rules do not require drones nor drone controllers to be visible to bystanders. Therefore, bystanders' concern about invisible controllers remains largely unaddressed. The controller-bystander app can allow bystanders to contact controllers, but our controller respondents did not value this mechanism as much partly because its usage might infringe on their own privacy.

Important Questions for Addressing Drone Privacy Issues

We now discuss important questions and suggestions for designing future privacy mechanisms and policies for drones.

Improving individual privacy mechanisms

How to improve individual privacy mechanisms? We suggest to consider three aspects: effort, practicality, and effectiveness.

Effort. One important question is how much effort a mechanism demands from a bystander or controller. If people think a mechanism requires too much 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 should be the controllers' responsibilities to protect the bystanders' privacy. However, this can be a risky belief because controllers may care more about protecting their own privacy rather than the bystanders' privacy. One reason that face blurring was highly rated is because it requires minimum effort from controllers and bystanders.

Practicality. Another question is how practical a mechanism is in reality. 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 notices. When drones are flying in the air, it would be difficult for people to see or read any privacy notice on the drones. How to help bystanders identify drones' privacy policies or notices, and understand what privacy mechanisms have been applied is important for future privacy designs and policies for drones.

Effectiveness. The third question is how effective a mechanism is in practice. This is particularly important in the context of drones because most of the existing privacy mechanisms for drones are voluntary. Both controllers and bystanders believed some controllers have the *ability* and/or *intention* to circumvent these mechanism. For instance, un-blurring face blurred images highlights not only the potential technical weakness of the face blurring mechanism but also controllers' *ability* to reverse it. In contrast, malicious controllers who spy people would intentionally ignore no-fly-zone requests, speaking more about controllers' *intention* to avoid the mechanism.

Our respondents suggested using laws and/or technical means to enforce these voluntary mechanisms. For instance, some controllers suggested "hard coding" no-fly-zone information into drones that automatically prevent them from flying into a 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 mandate and enforce mechanisms such as no-fly-zone, privacy policies, and face blurring.

Combining multiple mechanisms

Our scenario-based results suggest that respondents from both groups had desires of using a combination of 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 suggested combining 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. Our respondents' choices of mechanisms also varied across different scenarios, suggesting that they had context-based preferences of privacy mechanisms. Future research can explore packages of mechanisms based on the changing scenario or context.

Bridging the bystander-controller mismatch

Our results also indicate that our bystander and controller respondents often had different perceptions of the same privacy mechanisms (e.g., the effectiveness of privacy policy). In the case of deletion requests, some controllers were concerned that bystanders may abuse this mechanism by sending them an overwhelming number of requests. These 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) behaviors in an inter-group process (drone operations) [5]. In drone operations, controllers directly operate drones and presumably focus on utilizing and enjoying drones, whereas bystanders do not directly participate in drone operations and thus prioritize their welfare such as safety and privacy against drones.

One way to bridge the bystander-controller mismatch is to improve the trust between them. Prior research has also shown that lack of trust is an antecedent to privacy concerns [30]. 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 using a number of measures such as adopting fair information practices (e.g., notice and consent) [9], presenting privacy policies [13], and displaying privacy notices or seals [32]. We studied some of these ideas, for instance, privacy policy and gesture opt-out (a form of user consent).

Prior literature has also proposed different ways of providing notice and consent to users in ubiquitous computing environments in order to improve users' privacy awareness [24, 23, 29]. Future work can explore these ideas (e.g., broadcasting a user's privacy preferences [23] in a physical location) for drones. 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 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 commended that the controller-bystander app and owner registration help hold controllers accountable.

Protecting the privacy of both bystanders and controllers

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 that these mechanisms could increase the 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 flying drone.

Lastly, privacy has been a key research theme in the HCI community. Our research highlights that the design of human-drone interaction should not only consider controller-drone interaction but also the indirect involvements 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 is thus important to inform the development of public policies and future designs of drone technologies.

Study Limitations

First, we cannot completely guarantee that all controller respondents were 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 US. Thus, our results may not apply to other countries.

Third, the privacy mechanisms studied in our research are by no means exhaustive, but we chose a diverse set of technology-based and policy-based 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 privacy mechanisms rather than their actual adoption behavior. We only collected self-reported data, which can divert from actual behavior, as shown in the privacy paradox literature (e.g., [31]). 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 behavior.

CONCLUSION

As drones continue to be adopted and used by governments, organizations, and ordinary consumers, how to protect people's privacy against drones is a critical and timely question. We conducted two surveys 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 owner registration and face blurring received most support individually by both groups, many respondents also suggested using a combination of mechanisms, which varied across different drone usage scenarios. We highlight a number of important questions for future privacy designs and policies of drones.

ACKNOWLEDGEMENTS

We thank Xingzhi Guo and anonymous reviewers for their helpful feedback. This research is in part supported by an internal grant from Syracuse University.

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. Anirudha Majumdar and Russ Tedrake. 2016. *Funnel Libraries for Real-Time Robust Feedback Motion Planning*. Technical Report. Massachusetts Institute of Technology. http://groups.csail.mit.edu/robotics-center/public_papers/Majumdar16.pdf

4. 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

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

6. 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

7. 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

8. Reece A Clothier, Dominique A Greer, Duncan G Greer, and Amisha M Mehta. 2015. Risk perception and the public acceptance of drones. *Risk analysis* 35, 6 (2015), 1167–1183.

9. 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

10. 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.

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

12. 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.

13. 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

14. Electronic Privacy Information Center (EPIC). 2016. EPIC - Domestic Unmanned Aerial Vehicles (UAVs) and Drones. (2016). https://epic.org/privacy/drones/

15. Federal Aviation Administration (FAA). 2015a. B4UFLY Smartphone App. (2015). https://www.faa.gov/uas/b4ufly/

16. Federal Aviation Administration (FAA). 2015b. Unmanned Aircraft Systems. (2015). https://www.faa.gov/uas/

17. Federal Aviation Administration (FAA). 2016. *Summary of the Small UAS Rule*. Technical Report. https://www.faa.gov/uas/media/Part_107_Summary.pdf

18. Andrea Frome, German Cheung, Ahmad Abdulkader, Marco Zennaro, Bo Wu, Alessandro Bissacco, Hartwig Adam, Hartmut Neven, and Luc 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

19. Future of Privacy Forum, Intel, and PrecisionHawk. 2016. *Drones and Privacy by Design: Embedding Privacy Enhancing Technology in Unmanned Aircraft*. Technical Report. https://fpf.org/wp-content/uploads/2016/08/Drones_and_Privacy_by_Design_FPF_Intel_PrecisionHawk.pdf

20. 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

21. 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.

22. 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.

23. Bastian Könings, Sebastian Thoma, Florian Schaub, and Michael Weber. 2014. Pripref broadcaster: Enabling users to broadcast privacy preferences in their physical proximity. In *Proceedings of the 13th International Conference on Mobile and Ubiquitous Multimedia*. ACM, 133–142.

24. Marc Langheinrich. 2002. A privacy awareness system for ubiquitous computing environments. In *international conference on Ubiquitous Computing*. Springer, 237–245.

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

26. 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

27. 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

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

29. 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.

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

31. Sarah Spiekermann, Jens Grossklags, and Bettina Berendt. 2001. E-privacy in 2Nd Generation E-commerce: Privacy Preferences Versus Actual Behavior. In *Proceedings of the 3rd ACM Conference on Electronic Commerce (EC '01)*. ACM, New York, NY, USA, 38–47. DOI:http://dx.doi.org/10.1145/501158.501163

32. 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

33. 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.

34. 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.