Whose Privacy? The Case of Drone Controllers and Bystanders

Yang Wang
Syracuse University
Social Computing Systems (SALT) Lab
ywang@syr.edu

Yaxing Yao
Syracuse University
Social Computing Systems (SALT) Lab
yyao08@syr.edu

Abstract
Much of the networked privacy scholarship has focused on individual users' privacy, which is often the main or only goal. Drawing from our research on privacy issues of drones, this paper aims to highlight the complexity of achieving privacy in a messy social environment where multiple stakeholders exist and may have competing interests. Which group's interests take precedence often reflects power imbalances and raises important ethical questions. In our case study, we highlight that both drone controllers and bystanders have privacy concerns in the context of drone operations, and privacy-enhancing mechanisms that benefit one group may hurt the other group. We discuss the importance of and potential directions in making sensible and ethical privacy trade-offs that affect different stakeholders.

Author Keywords
Privacy; Ethics; Unmanned Aircraft Systems; Drones

ACM Classification Keywords
H.5.m [Information interfaces and presentation (e.g., HCI)]: Miscellaneous

Introduction
Unmanned Aircraft Systems (UAS) or drones are unmanned aircraft controlled remotely or operated autonomously. Drones have a long history of military applications, but also

have recently been introduced to the mainstream consumer market. As an emerging technology, drones can enable numerous innovative applications such as aerial photography, news reporting, disaster responses, and package delivery. However, drones' maneuverability and capability in taking high-definition pictures/videos and sensing the environment have raised heightened privacy concerns such as surveillance and stalking [4].

Example interview quotes

"People can't tell it's there and will not be aware that they are being watched by such a tiny drone and the footage by drone may be used for whatever purposes without their consent or knowledge."
- A bystander interviewee

"It was not required in any way whatsoever, you're not required to get permission."
- A controller interviewee

To mitigate these concerns, various technology-based and policy-based mechanisms have been proposed. For example, LightCense is a drone identification system that uses LED array on a drone as its identifier [1]. People who want to know more about a drone or its controller can use a mobile app to scan the LED array to identify the drone and obtain its details, such as ID and controller information [1]. On the policy front, the drone-related regulations in the U.S. (e.g., FAA drone controller registration and FAA rules on small drones, a.k.a., Part 107) have focused on safety. The National Telecommunications and Information Administration (NTIA) recommended a list of voluntary best practices for commercial and non-commercial use of drones which could help protect ordinary citizens' privacy [3]. However, most of these mechanisms are voluntary. Thus, it is unclear how drone controllers and bystanders perceive these mechanisms and whether people intend to adopt them.

Drawing from our studies of drone controllers and bystanders, we highlight the often competing privacy needs of these two groups and discuss the importance of and potential directions in balancing the needs of both groups.

Drone Controllers vs. Bystanders

Most of the extant research on privacy issues of drones focuses on privacy concerns from the perspective of ordinary citizens or drone bystanders. For instance, a survey conducted in Australia found that people had an overall neutral attitude toward drone, but less than one fifth of the participants showed concerns about drone surveillance or spying [2]. Our interviews of drone bystanders also found that they were concerned about drones invading their physical and informational privacy [4]. In addition, some of our bystander interviewees expected to be notified and asked for explicit consent before a drone taking pictures/videos if they were nearby. The interviews also expressed the concerns that it can be hard to recognize drones and/or know what the drones are doing, whether the drones are taking pictures/videos that might capture them, and how these recordings will be used. In addition, they were also concerned about the remoteness of the drone controllers as they cannot see or find the controllers and the fact that they do not know who the controllers are. All of these uncertainties or difficulties make protecting their privacy challenging.

We conducted a follow-up interview study of drone controllers [5]. The results painted a different picture. In general, our drone controllers had less privacy concerns about using drones than what we found in the bystander interviews. Many controller interviewees felt the privacy issues of drones were exaggerated in part because of the media's sensational coverage of controversial drone uses [5]. In terms of notice and consent, the controller interviewees generally considered it was not necessary to ask consent from the bystanders before flying a drone if they fly the drone in public spaces. In fact, some of the controller interviewees believed that they have the Constitutional rights (citing the First Amendment) to fly drones and take pictures/videos in public spaces. Most controller interviewees said that to be polite, they would be willing to share information about what they are doing with their drones if bystanders ask [5].

We also conducted two rounds of online survey with both drone controllers and bystanders about their perceptions of several kinds of privacy-enhancing mechanisms for drones, such as no-fly-zone, owner registration, privacy policy, LED license, and a controller-bystander app [6]. In general, we found drone controllers were less positive about all the privacy mechanisms than their bystander counterparts.

Example survey quotes

"I think the app will provide better protection to bystander and make the controller more accountable."
- A bystander respondent

"Again, you are suggesting trading the privacy of one for the privacy of another."
- A controller respondent

In addition, the controller respondents raised privacy concerns about some of these privacy mechanisms violating their own privacy. For example, the controller-bystander app is designed to support direct communication between bystanders and controllers. Controllers can provide information about the drone model, owner information, the purpose of use, and the camera/sensor information of the drone. Nearby controllers can opt in to be listed on a map in the app. Bystanders can directly check these information, and contact controllers via the app. Many bystander respondents found value in this mechanism as it would provide some degree of transparency of drone practice that they do not currently have. However, some controller respondents worried that the drone controllers could be unnecessarily tracked and thus violate their privacy.

Another example was the controller registration mechanism. The FAA requires drone controllers to register themselves with the government agency. The registration number must be visible on the drone, and drone bystanders could use the number to track down the controller of a drone. Some survey respondents suggested that the controller registration information should only be made available to the government but not to the general public. If the later happens, then it could violate controllers' privacy.

For more details about these studies and their results, we refer interested readers to the following papers [4, 5, 6].

Discussion

The results above highlight that the drone controllers and bystanders have quite different perceptions of drones and different kinds of privacy mechanisms for drones. More importantly, they call attention to the sometimes competing privacy interests of both groups. A important ethical question is whose privacy we ought to protect or prioritize.

The current discourse around privacy protection in drones is centered around ordinary citizens, or drone bystanders as we studied in our research. However, as we observed in our studies, if technical or policy-based privacy mechanisms only consider the privacy needs of bystanders, these mechanisms might negatively affect the drone controllers and given most of these mechanisms are voluntary controllers are unlikely to adopt these mechanisms, making them practically useless. Even if the mechanisms are required, if they do not consider the needs of both groups, the mechanisms can backfire. More broadly, we believe that it is unethical to not consider different stakeholders' interests. In the world of privacy, consumers or citizens usually are more vulnerable because of the powerfulness of the companies and government. However, we argue that it is not ethical to only consider the citizens' privacy. The technology users' privacy should also be considered.

The next logical question is how to balance the privacy needs of drone controllers and bystanders and more broadly different stakeholders in other contexts. We believe this is an important area for future research. We offer some initial thoughts here. First, a methodology or process that can fairly acknowledges and considers different stakeholders' privacy needs is desirable. The NTIA multi-stakeholder process on drones seems to be a promising example. However, whether and what improvements can be made to better represent different stakeholders' interests (e.g., that of

the citizens) is an open question. Second, similar to the multi-stakeholder process, a participatory design approach that can take into account various stakeholders' privacy needs would be valuable. Lastly, the current privacy impact assessment (PIA) is often used to focus on one stakeholder (e.g., the company). We advocate that future development of privacy risk analysis methodologies should be able to model and analyze the privacy risks for all stakeholders.

More broadly, this is just a concrete example that highlights the complicated challenge of achieving or balancing privacy and/or other values for the different stakeholders. This is an important direction for future research.

References

[1] 2016. LightCense. (2016). http://www.lightcense.co/

[2] 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.

[3] National Telecommunications and Information Administration. 2016. Multistakeholder Process: Unmanned Aircraft Systems. (2016). https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-unmanned-aircraft-systems

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

[5] Yaxing Yao, Huichuan Xia, Yun Huang, and Yang Wang. 2017a. Drone Controllers' Privacy Perceptions and Practices. In *Proceeding of the annual SIGCHI conference on Human factors in computing systems (CHI2017). To appear.*

[6] Yaxing Yao, Huichuan Xia, Yun Huang, and Yang Wang. 2017b. Privacy Mechanisms for Drones: Perceptions of Drone Controllers and Bystanders. In *Proceeding of the annual SIGCHI conference on Human factors in computing systems (CHI2017). To appear.*