Privacy and Fear in the Drone Era: Preserving Privacy Expectations Through Technology

Judith Uchidiuno
Carnegie Mellon University
Pittsburgh, PA 15213
jio@andrew.cmu.edu

Justin Manweiler
IBM Blockchain
Yorktown Heights, NY 10598
jmanweiler@us.ibm.com

Justin D. Weisz
IBM Research AI
Yorktown Heights, NY 10598
jweisz@us.ibm.com

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the Owner/Author.

CHI'18 Extended Abstracts, April 21–26, 2018, Montréal, QC, Canada.
© 2018 Copyright is held by the owner/author(s).
ACM ISBN 978-1-4503-5621-3/18/04.
https://doi.org/10.1145/3170427.3188457

Abstract
The increasing use of unmanned aerial vehicles (i.e. drones) is raising a number of privacy issues. The high-resolution cameras that drones can carry may pose serious privacy hazards to the general public. Numerous media stories highlight incidents of drones spying on people, often with negative consequences (e.g. lawsuits and arrests). Our research seeks to understand how incorporating privacy-preserving technologies in drone design can mitigate privacy fears. We identify several classes of privacy-preserving technological solutions and evaluate their potential efficacy across a variety of situations through a Mechanical Turk survey of 7,200 respondents. Our results inform both drone designers and regulators who wish to develop, operate, and/or regulate novel drone services while assuaging public fears of privacy violations.

Author Keywords
Drones; Privacy

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



Figure 1. DJI S1000 octocopter drone taking off.

Introduction

Unmanned aerial vehicles (UAV or drones) are aircraft flown without human passengers and are piloted by software or by a human pilot via remote control. Today, the nefarious or negligent can easily fly a drone and capture real-time images and videos of persons and physical spaces to which they would not otherwise have access. Incidents of privacy violation are numerous in the media[1], and as drones evolve with greater sensory capabilities and longer battery life, we expect privacy concerns to be all the more acute.

In order to help usher in a new era of ubiquitous UAV applications, we see value in the development of technical means to preserve privacy to improve societal acceptance of drones. We identify several classes of privacy-preserving technologies and evaluate their potential efficacy for alleviating privacy fears through a large-scale survey.

Drones and Privacy in HCI

Drones are starting to become an important area of inquiry in HCI. Drone studies have examined ways in which people can interact and control drones via gestures [2], as well as applications of drones in domains such as sports training [3] and home assistance [1]. Those studies generally identify tensions between the potential benefits of drone technology versus safety and privacy concerns. Recently, researchers have specifically begun examining privacy-preserving methods for drones. Yao et al. conducted multiple studies of drone privacy [78], specifically comparing between drone operators and bystanders. They found that although many bystanders had privacy concerns, operators had fewer concerns because they felt aware that privacy was an issue and operated their drones in a responsible manner [7]. However, although operators did think about whether they flew in public vs. private spaces, their definitions of what constituted public vs. private differed from bystanders. Technology may be able to mediate bystanders' privacy concerns, such as requiring drones to be registered and performing face blurring on captured data [8].

Smith et al. [5] identified four main dimensions of privacy concern: excessive data collection, unauthorized use of collected data, data access by malicious external parties, and improper data access within an authorized organization. While each dimension has clear implications for drones, excessive data collection is arguably the most visible kind of privacy violation. In managing privacy of collected data, Palen and Dourish [4] argue that privacy management is contextual – "a dynamic response to circumstance rather than a static enforcement of rules." Expectations of privacy are thus contextually dependent on who is collecting the data, where and when it was collected, and why and how it was collected [6]. Therefore, our study builds on the results of Yao et al. [78] by examining different classes of privacy-preserving technologies and how they reduce feelings of privacy violation in the presence of different contextual variables.

Classes of Privacy-Preserving Technologies

We examine six classes of privacy-preserving technological interventions for drones based on an examination of literature and our own intuitions. We

[1] https://www.nytimes.com/2016/01/28/style/neighbors-drones-invade-privacy.html

Drone Owner
friend
stranger
known business
unknown business
law enforcement

Respondent Location
inside…
  first floor home
  20th floor apartment
  public shopping mall
outside…
  secluded home backyard
  20th floor balcony
  public park

Drone Operator
visible drone pilot
  with remote control
autonomous flight

Drone Technology
prevent recording
physical blur
computational blur
LED indicator
smartphone query
crowdsourced drone rating

Table 1. Independent variables. Twenty responses were collected for all 360 possible combinations of variables yielding 7,200 unique responses.

deployed a Mechanical Turk survey (N=7,200 responses) to evaluate one specific intervention of each class.

Class 1 – Prevent Data Capture. Prevent the physical capture of data by blocking, obstructing, or re-orienting the drone or the data capture apparatus. Examples: no-fly zone [7], pointing the camera away from sensitive areas.

Class 2 – Physical Desensitization. Data are allowed to be captured, but physical means cause it to become desensitized. Example: fly with camera pointed away from sensitive areas.

Class 3 – Computational Desensitization. Data are allowed to be captured, but computational means cause it to become desensitized. Example: Blur detected faces [1].

Class 4 – Indicate Collection. An indication is given for when and/or what kinds of data are being collected. Example: LED to indicate data collection [7].

Class 5 – On-Demand Query. Individuals possess the means to query a nearby drone as to its owner, operator, and/or purpose. Example: drone bystander app [8].

Class 6 – Trusted Indicator. A drone possesses a physical or digital emblem or certification of its trustworthiness. These emblems may be issued by a regulatory agency (e.g. the FAA in the US) or via crowdsourced means. Example: owner registration [8].

Survey Methodology
We constructed a scenario-based survey to examine the effect of several contextual factors on respondents' feelings of privacy violation and the mitigating effects of a privacy-preserving technology. In our design, each respondent was given a base scenario, with additional components populated from three independent variables: *drone owner* (5 options) x *drone operator* (2 options) x *imagined location of the respondent* (6 options) = 60 unique scenarios. Across all respondents, we measured privacy sensitivity to the scenario both before and after presenting one of the six technological interventions. Thus, there were 60 x 6 = 360 unique scenario-intervention combinations. Each respondent was presented with only one such combination, and we prevented any respondent from completing the survey twice. For each combination, we gathered 20 unique responses, yielding 360 x 20 = 7,200 unique total responses. We deployed our survey on Mechanical Turk, compensating $0.20 USD for each response.

Survey respondents were split evenly between male and female. Respondents were aged 18-29 years (47%), 30-49 years (42%), and 50+ years (11%). To minimize culture effects, we only deployed our survey in English to Turk workers residing in the United States or Canada. We also required respondents to be at least 18 years old and have a 95% acceptance rate to reduce the likelihood of bot responses. We embedded a script into our survey to prevent workers from submitting more than one response, and in cases where the script failed (< 1%), we discarded those responses and gathered additional data.

Class 1. You see the drone flip upside down, pointing its camera toward the sky, away from you.

Class 2. You see the drone shaking and spinning itself as it flies, causing all of the images or videos it gathers to be blurry.

Class 3. You see a logo on the drone indicating that the images captured by the drone are post-processed to blur out any human faces. You may assume that the presence of this logo guarantees that the face blurring will occur.

Class 4. You see a red LED light on the drone indicating that it is recording video.

Class 5. You open an app on your smartphone and point the phone towards the drone. In the app, you can see the company that owns the drone and that it is delivering a package.

Class 6. You open an app on your smartphone and point the phone towards the drone. In the app, you see other peoples' ratings and reports of the drone and its operator. You may also leave your own rating and comments, and you can report on undesirable or unsafe drone behavior.

Table 2. Descriptions of privacy-preserving technologies.

Survey Instrument

Respondents were given a description of one of 60 possible scenarios including a specific drone owner, operator, and location. Below is an example scenario with the variable substitutions in **bold**.

*We live in an era of ubiquitous drones in which individuals, companies, and governments continuously operate numerous unmanned drones in our skies. Drones are everywhere, performing a variety of tasks such as delivering goods, fighting crime, and recording significant events. You are **inside your house, on the first floor, looking outside a window**. You see a drone fly overhead, pause, and move on. You see a camera on the drone. A **person with a remote control** is flying the drone. You know that **your friend** owns the drone.*

Respondents rated the extent to which the drone violated their expectations of privacy on a 5-point Likert scale (strongly disagree to strongly agree). Respondents also identified the extent to which they felt the following parties were responsible for maintaining their privacy: the government, the drone itself, the drone manufacturer, the drone operator, or they themselves. Next, respondents read a description of one technological intervention and were asked to respond to the same questions. This within-subjects methodology allowed us to test the effect of the intervention. The descriptions of the technological interventions used in the study are shown in Table 2.

Effect of Privacy-Preserving Technologies

Across all scenarios, 53% of respondents agreed (strongly or otherwise) that the drone had violated their privacy; 27% disagreed and the rest were neutral.

Many respondents felt that the operator of the drone, the owner of the drone, and they themselves were responsible for protecting their privacy (Figure 2).

"I am responsible for protecting my privacy. The government nor the drone are responsible for protecting my privacy. There is no way for a drone to protect my privacy, it is a machine, manned by a man who has no respect for my privacy or he would not be using the drone." (female, 18-29, location = shopping mall, operator = remote pilot, owner = law enforcement, tech = class 2, physical desensitization)

"Blinds exist for a reason. Someone doesn't want anything to see in their window? Close the blinds!" (female, 30-49, location = first floor, operator = autonomous, owner = stranger, tech = class 5, query)

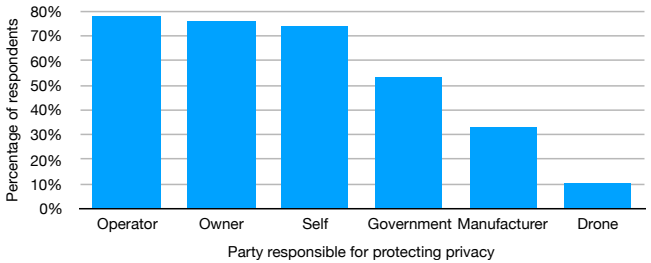


Figure 2. Percentage of respondents who felt that the given parties were responsible for protecting their privacy (N=7,200).

Respondents were also sensitive to drones that operated in both indoor and outdoor settings, with 58% agreeing that their privacy was violated in indoor scenarios and 62% agreeing that their privacy was violated in outdoor scenarios. Roughly half of respondents felt that their privacy was violated no

matter who owned the drone: their friend (49% agreed), a stranger (55% agreed), a known business (51% agreed), an unknown business (56% agreed), or law enforcement (50% agreed). Female respondents were more likely to agree that the drone had violated their privacy (57%) than male respondents (52%).

Reducing Feelings of Privacy Violation

Figure 3 shows how perceptions of privacy violation changed with the introduction of a technological intervention. Overall, the percentage of respondents that agreed the drone violated their privacy decreased from 53% to 38% after being introduced to the technological intervention. The percentage of respondents who disagreed that the drone violated their privacy consequently increased from 27% to 41%. We ran a Wilcoxon signed rank test to determine whether this observed difference was significant, and it showed a statistically significant median improvement in feelings of privacy violation after presentation of a technological intervention (Wilcoxon $z = -27.577$, $p < .001$).

To address the impact of technological interventions on feelings toward privacy violation, we considered the difference of the initial privacy rating (P_0) and the rating after presentation of the technological intervention (P_T). A change in privacy rating was coded as positive if $P_T - P_0 > 0$. Figure 4 shows the percentage of respondents that indicated a positive shift in privacy ratings after presentation of a technological intervention, as well as whether the technology should be included in all drones. Technological interventions that prevent the capture of sensitive data (Class 1) or inform people of the drone's purpose (Class 5) were most likely to have a positive impact on privacy. Interestingly, technologies that did not impact privacy ratings were requested for inclusion on all drones (Classes 3 & 6).

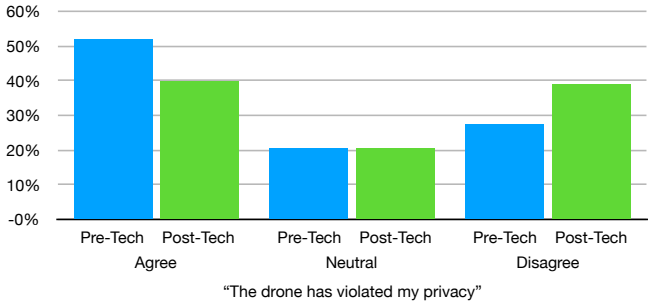


Figure 3. Percentage of respondents rating their feelings of privacy violation before vs. after the presentation of a technological intervention – aggregated across all interventions.

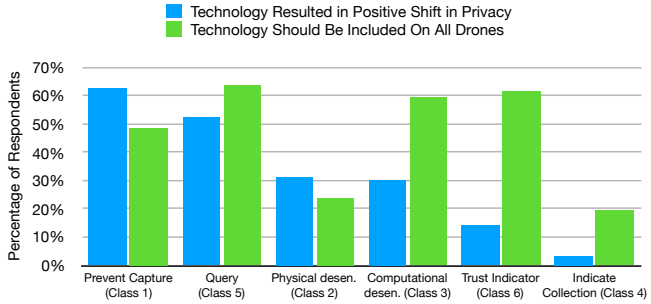


Figure 4. Percentage of respondents that reported a positive shift in privacy ratings when presented with different technological interventions, as well as whether the technology should be included on all drones.

Discussion

Our most notable finding is that privacy-preserving technologies can reduce privacy-related drone fears. Technologies that prevent the capture of data in

sensitive situations (Class 1) had the greatest impact, and technologies that allow individuals to query a drone for its owner, purpose, and data being collected (Class 5) also helped significantly. Deploying these technologies in practice might involve the use of transmitters, such as beacons, that inform drones of the specific data capture policy of a given area. Although the technologies most requested to be included with drones weren't the ones that produced the greatest effect on privacy, we note the general overall desire for inclusion of *some* privacy-preserving technology. Our findings differ slightly from the findings of Yao et al. [7,8]. In their study, they found that "owner registration and face blurring gained relatively more support from both bystanders and controllers than other mechanisms." These mechanisms roughly correspond to our Trust Indicator (Class 6) and Computational Desensitization (Class 3). Although methodological differences in how technological preference was indicated may account for inconsistencies in specific findings, our general conclusion is the same: technologies ought to be developed and included on drones to reduce privacy fears. Ultimately, we believe that technical means present a fruitful path for greater societal acceptance of drones.

References

1. 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.
2. 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.
3. Florian 'Floyd' Mueller and Matthew Muirhead. 2015. Jogging with a Quadcopter. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (CHI '15). ACM, New York, NY, USA, 2023-2032.
4. Leysia Palen and Paul Dourish. 2003. Unpacking "privacy" for a networked world. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI '03). ACM, New York, NY, USA, 129-136.
5. H. Jeff Smith, Sandra J. Milberg, and Sandra J. Burke. 1996. Information privacy: measuring individuals' concerns about organizational practices. *MIS quarterly:* 167–196.
6. H. Jeff Smith, Tamara Dinev, and Heng Xu. 2011. Information privacy research: an interdisciplinary review. *MIS quarterly* 35, 4: 989–1016.
7. Yaxing Yao, Huichuan Xia, Yun Huang, and Yang Wang. 2017. Free to Fly in Public Spaces: Drone Controllers' Privacy Perceptions and Practices. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (CHI '17). ACM, New York, NY, USA, 6789-6793.
8. Yaxing Yao, Huichuan Xia, Yun Huang, and Yang Wang. 2017. Privacy Mechanisms for Drones: Perceptions of Drone Controllers and Bystanders. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (CHI '17). ACM, New York, NY, USA, 6777-6788.