Privacy and Unarmed Aerial Systems

David Mberingabo, Emma Rogers, Luka Begiashvili and Kristina Reimer

1 Introduction

Unmanned Aerial Systems (UAS), colloquially known as drones are becoming increasingly capable of autonomously operating near people and animals. As the technology evolves (and safety guarantees increase), it is likely policies will allow systems to operate closer to people. Previous research has observed that drones yield a heightened level of fear and anxiety when operating proximally to people.

Despite the growing public awareness and undeniable privacy implications, the body of literature is scarce when it comes to research on the current public perception of drone privacy. There is literature that supports the idea that priming respondents on specific uses can lead to different perceptions of the overall technologies. However, when looking at sources specific to drone usage, no specific studies that relied on priming users were evident from our research. Much of the research has focused on technical aspects and the use of drones in war zones, while little research to date has been done to explore how civilians perceive drones. To our knowledge, this is a first look at how priming influences perceptions of drone privacy and how the general public plays a role in shaping government regulations of drone privacy laws.

We believe that understanding user perceptions can help with implementation of best practices in terms of drone development as well as effective legislation implementation. When we understand what users and broader society wants, we can tailor drone design and laws to alleviate those concerns. Additionally, understanding the impacts of priming can help these groups anticipate what narratives they need to counter in terms of drone use and which ones might lead to wider acceptance of adoption of drone technology.

Consequently, we focus on the public's perception of privacy regarding drones. We argue that when primed with information on privacy harms, people will be more hesitant to trust drones and will want more regulations. When primed with information presenting drones in a trustworthy manner, we expect people will have less reservations about drones in terms of privacy and be willing to have less strict regulations. We examine the interplay between the public perception of privacy and the perceived benefits of drones. Priming them with information on privacy harms or priming them with information presenting drones in a trustworthy manner this study investigates the following research question: How does priming influence people's perceptions on the privacy violations of drones and the legislation required to regulate them?

This study contributes to existing privacy literature in the domain of drone utilization and related privacy perceptions. Despite a myriad of research about people's privacy perception towards other technologies we identified that there is very little research done about people's privacy perception regarding drones. Therefore we believe that our research can be an interesting source for any interested parties who are working on identifying people's privacy perceptions regarding drones and developing regulations that will take those perceptions into account.

Our paper is divided into the following sections: First, the paper explores the existing literature that looks into the privacy risks which emerge from drone technology, the regulations surrounding privacy and drones, the perceptions people have on privacy with different drone technologies, and general studies on how priming impacts perceptions of technology and their privacy. The second section provides the methodology of the study. In particular it introduces a survey methodology with detailed description of each type of question and the ways we recruited the people for this survey. In the subsequent section we provide an overview of methods, tools, and steps for the analysis and their underlying logic. It is followed by the fourth section about results of survey analysis. Specifically, by examining answers to privacy and regulation questions we are providing findings about how priming impacts a participant's comfortability with drones and affinity to regulate them. Based on the analysis and survey results we then develop policy recommendations in section five. Finally, in the same section we acknowledge survey limitations and suggest avenues for future research in this important but under examined context.

2 Literature Review

In this section we review the current domestic and international privacy regulations on drone technology, the technical foundations of privacy risk from drone technology, the industry best practices for drones about privacy, and the state of current research on people's perceptions of drone privacy. The drones that we discuss include small unmanned aerial systems in complex low-altitude airspace (e.g., personal and delivery drones). This excludes earth-orbit satellites, war drones, water-based drones, helicopter drones, and airplane drones.

2.1 Current Domestic & International Privacy Regulations on Drone Technology

In the US, the Federal Aviation Administration (FAA) has jurisdiction over drones, but privacy-related issues are largely unregulated. In response, most US states have passed legislation that concerns privacy and drones (911 security, 2022). Most of these laws fall under two categories: laws that mandate law enforcement to obtain a search warrant before surveilling a suspect and laws that prevent civilians from invading another person's privacy (911 security, 2022). Drones have many different uses, but we have chosen to focus on civilian use, commercial use, and law enforcement use.

Although the FAA's mission does not touch on privacy issues, other organizations have published privacy guidelines for drone use. In 2016, the National Telecommunications & Information Administration (NTIA) published a document on privacy best practices and included "Guidelines for Neighborly Drone Use" (NTIA, 2016). These guidelines, however, are merely recommendations and not requirements. State legislatures are still debating on how technology should be regulated (DuBois et al., 2021). Many news articles are pushing for more regulations and emphasizing how governments will be unable to keep up with technological innovation (e.g., Brookings, ACLU, and NY Times). Some papers suggest implementing technology that enhances the privacy of the device, such as blockchain technology (Lv et al., 2021) (Rana et al., 2019).

Like the US, the increased use of drones for different applications has presented many countries with regulatory challenges. Such challenges include the need to ensure that drones are operated in a way that protects citizens' privacy. Several countries made efforts to address concerns regarding the privacy issues caused by drones. We will review the experiences in the EU, UK, Japan, and China.

Drone privacy laws are different in these countries and they are at various stages of development. For example, Voss (2013) found that European law provides more protection once data has been obtained from drones. However, there are no specific rules or guidance documents for privacy and drones in EU legislation (Lee et al., 2022). Instead, the General Data Protection Regulation (GDPR) indirectly touches upon privacy issues caused by drones. Specifically, the regulation does not directly discuss drones, but it defines a regulatory framework for managing privacy in the process of digitization. Member states are left to their own devices to develop their regulatory frameworks related to drones that will be consistent with the GDPR (Lee et al., 2022).

Unlike EU countries, there is little discussion of privacy about drones in Japan's privacy regulations. The Civil Aviation Bureau is responsible for establishing rules regarding drone operation, but privacy is not discussed at all in their regulations (Lee et al., 2022).
As for the UK, (Butler, 2019) suggests that the UK requires drones to be operated within a visual line of sight and not over human beings. At the same time, there are additional regulations that prohibit flying near airports and other sensitive areas. The UK presently acknowledges the possibility of privacy risks brought up by drones and apart from developing proper regulation they also plan to raise awareness about drone privacy issues through education (Butler, 2019).

Finally, (Yao, 2021) suggests in his article that while China has gradually come up with clear ideas on how to regulate drones to protect privacy, there is still some leniency and strictness in the implementation process, so China still lacks clear privacy laws regarding drones. It is obvious that drone regulations need a highly effective "parent" law that should be supported by

“Civil Aviation Law” and “General Aviation Law”, but these regulations are missing or fragmented (Yao, 2021). The author also suggests that China should ensure that regulations of drones are combined with the development of the drone industry so that a balance between public safety and technological innovation is achieved.

The experiences in these countries clearly show that national laws and industry regulations regarding drone privacy are still incomplete and more advanced and effective privacy regulations are needed to ensure the proper protection of privacy rights.

2.2 Technical Considerations of Drone Privacy Violations

The foundation for most privacy policies around drones arises from the legislator's varied perceptions on delivery, police, and surveillance drones. With each subcategory comes distinct levels of trust, understanding, and personal opinion that impact the created policies. But regardless of their label, drones as a device are ridden with several technical foundations that truly cause privacy risks. For example, drones of all three aforementioned categories are small, making them easy to be transported, steal, and misused when inactive (Gruhl et al., 2019). Anyone with a technical background would be able to modify a drone’s programming and gain access to the private footage collected during its surveillance (Harri, 2018). This in turn will compromise the confidentiality of the collected information and will lead to severe violation of privacy even if the information was collected with the consent of the object.

A drone’s miniature structure also permits it to travel further than most people can, thus invading passerby’s lives, while still following FAA guidelines (Gruhl et al., 2019). Further, a drone’s storage capacity exceeds that of a cell phone, which in turn makes it capable of recording a multitude of details about anyone it captures. Its primary purpose is to record, thus incurring implicit social and legal intrusions. These recordings process personal data without each subject’s consent simply by constantly video recording. In most drones, this storage technique and location is primarily controlled by its owner, and it becomes a single individual’s responsibility to protect the privacy of many (Supreme Court of the United States, 2022). However, it must be noted that drones still require high levels of technical expertise to properly operate, maintain, and exploit (Harri, 2018).

Furthermore, modern drones are equipped with facial recognition software, infrared technology, and speakers capable of monitoring personal conversations (www.aclu.org, 2022). Consequently, interconnected drones could enable mass tracking of vehicles and people in wide areas. Moreover, without anyone seeing them tiny, drones could peer into the window of a home or place of worship (Rice, 2019). Privacy activists are afraid that this can destroy civil liberties and allow the government access to enormous personal information that they might use against their citizens. Unregulated utilization of drones can lead to a “surveillance society” in which our every

move is monitored, tracked, recorded, and scrutinized by the government (www.aclu.org, 2022). Civil liberties are guaranteed rights and freedoms. For example, the First Amendment was developed to protect freedom of speech and the right to assemble. Also, The Fourth Amendment protects against unreasonable searches and seizures (www.legalscoops.com, 2021). If we will allow the police to use video drones without regulation that may violate constitutional rights under these two amendments.

2.3 Drone Privacy Best Practices and Standards

"*Privacy is independent of the type of technology that's collecting information.*" - Jesse Kallman, Director of Business Development and Regulatory Affairs at Airware, during his congressional hearing on Drone Technology and Safety (Kallman, 2015).

Some have expressed concerns that the UAS industry and regulators focus on safety at the risk of not taking privacy seriously enough (Department of Homeland Security, 2015). Although no major privacy breaches from drones have yet to hit the news, as UASs become more prominent, they are bound to increasingly cause subjective and objective privacy harm. Creating drones that consider data privacy regulations and standards would require UAS owners, manufacturers, and operators to implement Fair Information Practice Principles and invest in the innovation of industry best practices. Government organizations such as the Federal Trade Commission, enforce consumer and general privacy regulations, but it is up to the industry to decide what are reasonable privacy standards.

Besides well-established information security protocols for data at rest and in transit, such as access control, authentication, and information protection, the industry could reference the Department of Homeland Security and the National Telecommunications and Information Administration's non-prescriptive and voluntary best practices for UAS owners, manufacturers and operators (NTIA, 2016). Manufacturers can apply FIPPs and Privacy by Design principles to their drones, but at the end of the day, owners and operators will hold some responsibility as well. Operators can record personally identifiable data and intrude on the privacy of others, while owners could store, process, and disseminate sensitive data (NTIA, 2016). This does not mean that the industry is absolved of all responsibility, as they can still take further privacy measures. For example, they could require some level of training or contract agreement to operate the drone within legal and ethical bounds before a drone sale, much like how a car dealership requires a Driver's License and other information before the sale (NTIA, 2016).

Government and non-government training courses exist to certify that UAS operators can navigate the privacy-related issues that may arise during a UAS mission. Government agencies and independent organizations such as the Airborne Public Safety Association, the US Department of Interior, and the Federal Aviation Administration offer training courses and

licensing for different types of UAS purposes. This ensures that all UAS operators, including individual hobbyists, can remain updated on privacy rights and regulations about UAS, and that courts can rest assured operators have the minimum knowledge required to navigate any privacy-related situation during a UAS flight mission (Kim et al., 2022).

Some privacy-retaining technologies are still being developed. Although it has yet to be widely adopted by the UAS industry, Geo-Fencing – a form of UAS Traffic Management (or UTM) – is the idea that a UAS can be programmed to only fly over authorized areas (Kim et al., 2022). In the future, this idea can be extended to program UASs to only record authorized areas, objects, and persons.

2.4 Existing Privacy Perceptions of Drone Technology

When it comes to research on the current public perception of drone privacy, the body of literature is much more scarce. (Wang et al., 2016) and a UK report done by a foundation called Nesta appears to be the most applicable research. (Wang et al., 2016) conducted interviews about general drone usage and specific cases, and found that respondents had privacy concerns when drones entered private spaces, when the user's intent was unclear/bad, and when they weren't notified or given the chance to consent to drone usage around them.

In their literature review, the researchers explored privacy perceptions of recording technologies and the privacy mechanisms of drones, noting that existing research on people's perceptions of drone policies didn't exist at the time (in 2016). The UK report states that public confidence is necessary for creating privacy regulations and wide drone usage across the country. The UK recognizes all of the benefits of drone technology but emphasizes that "getting it right" is crucial to maximizing benefits and minimizing privacy and security concerns (Nesta, 2018). In a more experimental setting, (Chang et al., 2017) also looked into privacy perceptions surrounding drones, and found that people tend to have negative perceptions of drone privacy, with notable privacy concerns including spying, recording without consent, and uncertainty surrounding what the drone was recording.

Recent research has worked to break down drone usage and the research participants into smaller subcategories for analysis. A Forbes article explained that there has been an emphasis by respondents on regulation and limited use with explicit purposes when it came to questions on police drones, and in terms of general use there are more privacy concerns when it comes to groups like law enforcement or the military using drones when compared to groups like lobbyists or construction companies (Rice, 2019). A notable conclusion here is that unmarked drones were seen as the most privacy-invasive. The final set of studies Forbes covers is related to user demographics, where it is found that women are more likely to have privacy concerns with drones, as well as those of certain ethnicities, with certain privacy views, or with certain trust in

the police. (Lidynia et al., 2017) furthers this overall line of research by breaking down the usage of drones into the hobby, commercial, and emergency use, and reports on both user privacy perceptions surrounding each use type and their receptiveness to certain regulations as a solution.

Looking at our research question, we also looked into the body of literature on how priming users with different information can lead to different perceptions of the privacy of drone technology. Generally, there is literature that supports the idea that priming respondents on specific uses can lead to different perceptions of the overall technology. The novel *Army of None* (Scharre, 2019) explains two studies in which the views of autonomous weapons (which can include military applications of drones) heavily depended on the information presented surrounding its use.

We could find another interesting example of priming survey participants with different information and then exploring their privacy perceptions in the study "How Textual Priming Affects Privacy Concerns of Email Service Users." Specifically, the authors (Buck & Dinev, 2020) provide an interesting experiment of priming two groups of surveys with different information and when exploring their privacy perceptions. The textual priming and its operationalization were the following: Possible privacy intrusion (I) - Emails sent and received by PROVIDER users may sometimes be read by real people at third-party providers - not just machines. No privacy intrusion (II) - Emails sent and received by PROVIDER users cannot be read by third parties. The researchers got different results about privacy perceptions in two survey groups.

Moreover, in the recent study "Americans' perceptions of privacy and surveillance in the COVID-19 pandemic" respondents who agreed to take the survey were randomized with equal probability into two different survey orders by the authors of the study (Zhang, Kreps, McMurry, & McCain, 2020). Researchers, (Zhang, Kreps, McMurry, & McCain, 2020) hypothesized that direct personal experience with COVID-19, such as having contracted the disease or knowing someone who has, would cause respondents to express higher levels of support for public health measures (ie surveillance through Covid-19 app) intended to limit the spread of the virus. They randomly assigned respondents to a priming treatment in order to test the hypothesis. Those assigned to the priming treatment condition were presented with the section of questions related to their experience with COVID-19 before the section on surveillance and privacy, while those in the control group saw the "Surveillance privacy" section of the survey before the "Experience with COVID-19" section.

Clearly, priming has been explored in technology adoption and privacy concerns as a whole. However, when looking at sources more specific to drone usage, no specific studies that relied on priming their users were immediately evident from our initial research. This is a novel research

question that will inform technology and privacy policy analysts and possibly mitigate some of the challenges of creating effective drone privacy regulations.

3 Methodology

Our work seeks to understand how priming users with different written materials presenting drones in different ways will influence their perception of drone privacy violations and their views on how drones should be regulated. To do this, we designed an online survey to prime the users randomly and then ask them a series of questions pertaining to drone privacy and drone regulations.

3.1 Survey Questionnaire

For our survey, we started by informing users of the potential risks and benefits of the study with our consent form on the front page, before asking for their confirmation that they were willing to start the survey. Once users began the survey, they were directed to fill out a variety of demographics and background information to give us a baseline as to their previous experience with drones.

Then, the survey structure split the users into two groups to determine which user read one of two options of articles. The first group received an excerpt from an article by Matthew Guariglia discussing potential drone abuse by law enforcement in ways that infringe on people's privacy rights (Guariglia 2022). The second group received an excerpt from an article by DJI, a drone company who is highlighting the benefits of their drone technology in saving lives during natural disasters (DJI 2018). Users are randomly assigned to either group to minimize bias and uneven data collection. Both groups are asked to confirm they completed the reading before moving on to the next section of the survey.

Once reading the articles, participants answered questions to gauge their privacy perceptions of drones (Privacy Questions, Q1-12), as well as a set to gauge their opinions on different regulations for drone use (Regulatory Questions, Q1-10). These sets of questions are to determine user opinions specifically pertaining to drones, and would be the answers influenced by the randomly assigned passages if our hypothesis is true. After these questions, users are asked a series of more general questions intended to gather their overall privacy viewpoints. Each set of questions is discussed more in depth below, and the full survey can be found in the appendix.

3.1.1 Demographic Questions

To understand participants and characteristics that might influence their responses to this survey beyond the priming measured in our study, demographic information was collected including age

(within ranges), gender, education level, and major/degree focus. Characteristics are general enough that users are not able to be re-identified by demographic characteristics, and with each demographic question users are offered the chance to opt out of answering with the response "Prefer not to say".

Decisions on which demographics to include were based on the factors that would be of note when it comes to interacting with new forms of technology. Such choices were also influenced by similar bodies of work, including the studies (Emami-Naeini, 2017) and (Bloom et al., 2017).

3.1.2 Background Questions

Additional information pertaining to more specific information pertaining to the user's experience with drones was collected through two additional background questions discussing user's experiences with drones in real-life and whether they have researched or learned about drones before. Such information is intended to help us determine the relative importance of our priming sources, which can differ among individuals who are more or less experienced with drone technology.

3.1.3 Privacy Questions

After reading one of the passages, participants were asked to answer questions about their views of drone use, whether they are comfortable with different actors using drones, and whether drones invade their privacy in a series of multiple choice questions. Participants rated different statements on a five point Likert scale from "Strongly Disagree" to "Strongly Agree." These questions are designed to determine whether users are concerned with potential privacy violations pertaining to drones, as users who are more hesitant would say they are not comfortable with drones in many usage scenarios. As such, questions begin with more benign uses of drones before getting to statements that would likely be disagreed with if users had privacy concerns pertaining to drone use.

Decisions on which privacy violations to include were based on the factors that would be of note based on specific technological features of drone technology. Such choices were also influenced by similar bodies of work on drones like (Lidynia et al., 2016), as well as privacy-oriented studies on different technologies, like the studies (Emami-Naeini 2017) and (Bloom et al., 2017).

3.1.4 Regulatory Questions

After answering the privacy questions, participants were asked to answer questions about their views on government regulation of drone usage in different ways, ranging from appearance regulations to usage or data collection regulations. Here, participants also rated different

statements about regulations on a five point Likert scale from “Strongly Disagree” to “Strongly Agree.” These questions are designed to determine whether users believe drones need to be more strictly regulated, which is seen as the practical implementation of the privacy concerns measured in the previous section of the survey.

Decisions on which regulations to include were based on the existing and potential regulations discussed within our literature review. Such choices were also influenced by similar bodies of work on drones like (Lidynia et al., 2016), as well as privacy-oriented studies on different technologies, like the studies (Emami-Naeini 2017) and (Bloom et al., 2017).

3.1.5 Baseline Privacy Perception Questions

After completing the privacy and regulatory sections of the questionnaire, users are asked a series of questions from the Internet User’s Information Privacy Concerns (IUIPC) scale, which asks more general questions about privacy to gauge user’s levels of privacy concern (Malhotra 2004). Questions were pulled from the sections Control (Existing Views Q1-3), Awareness of Privacy Practices (Existing Views Q4-6), Collection Attitudes (Existing Views Q7-9), and Opinions on Improper Access (Existing Views Q10-12). Such questions are located at the end of the questionnaire so that they do not influence user’s answers in other sections of the survey. Participants rated different IUIPC statements about privacy on a five point Likert scale from “Strongly Disagree” to “Strongly Agree.” These questions were included to provide a baseline for each user’s privacy concern, so that answers pertaining to drone usage can be analyzed as either being connected to priming or their general privacy concerns.

3.1.6 Justification for Survey Design

We believe that the majority of people have a very vague understanding about privacy implications of drone utilization. At the same time, we thought that their perceptions would highly be dependent upon the information they would receive about drones. Therefore in order to check our hypothesis we decided to ask people the same survey questions but first prime some of the survey participants with positive information about drones and the others with negative information about drones. Only difference between two groups of participants is the type of the information about drones we primed them with. So, if we would find differences about drone privacy perceptions between these groups we could attribute the difference to content of the information they were primed with.

Additionally, we decided to organize the questions on different pages according to the category of the questions (for example, breaking up the privacy-based questions from the regulatory questions). This was done to make it easier for the participants to understand and conceptualize what we were asking them. We used a wide range of questions in each category to give us ample opportunity to do data analysis between a variety of factors.

3.2 Recruitment

Participants were recruited from online advertisements. These advertisements depicted a drone image developed with online AI generators, as well as basic information directing users to a link or QR code leading them to our survey. We marketed through various social networking apps, such as sending it to our respective student organization and major-specific Slacks, to the CMU class discords, and posting on our personal social media accounts. The messaging was standardized throughout all recruitment mediums.

As an incentive to participate in our study, we offered a random drawing for three $50 Visa gift cards to all users who filled out our study. To collect this information without linking users to their specific responses, we included a Google Form at the end of the questionnaire that directed users to fill out the separate form if they wished to be entered in the raffle. This way, we were able to contact the winners of the raffle with their provided email addresses. Winners were chosen via a random number generator that chose three numbers associated with each user's email address. The winners were sent virtual Visa gift cards to thank them for their participation.

The outcome of our recruitment was a total of 128 responses recorded by Qualtrics. Of those responses, 6 were removed from the Qualtrics database because the participants simply opened the form and never made it past the introduction screen. A further 27 were removed during data analysis for not completing the entire survey – of which, there were 16 people who stopped responding during the demographics section before they reached the Survey Body, 1 person who read the priming paragraph but never moved on to the subsequent questions, 4 who left the survey after answering the Privacy section and never moved on to the Regulation section, and 6 who stopped taking the survey after the Regulation section and before the Existing Privacy Views section.

Thus, there were 95 responses that underwent data analysis. Qualtrics assigned all participants randomly to either the positively or negatively primed option, however participants did end up quitting the survey after being assigned one of the readings. Thus, of the 95 participants who completed the survey, 45 were positively primed and 50 were negatively primed. This slight discrepancy is due to the respondents who quit the survey before finishing.

3.3 Data Analysis

Due to our time limits, our analysis focused on the privacy and regulation questions, which are sections 3.2 and 3.3 respectively in the questionnaire. We wanted to find how priming impacts a participant's comfortability with drones and affinity to regulate them. We conducted our analysis by first calculating the total average score and the total average number of responses that were above a 3. For privacy questions, above a 3 is comfortable, and below a 3 is uncomfortable. For

regulations questions, above a 3 is a higher affinity to regulate and below a 3 is a lower affinity. We expect lower levels of comfort to correlate with higher levels of affinity to regulate, as it would indicate individuals who are uncomfortable with drones, in a privacy sense, are also more likely to want to regulate them.

For section 3.2, the privacy questions, on average, the comfortability score was 3.43 for positively primed responses and for negatively primed responses it was a slightly lower 3.22. This did not yield any significant results. On average, the number of comfortable participants (with a score above 3), in the privacy questions, was 8.66 for the positively primed responses, but it dipped to 7.82 for the negatively primed responses. So on average, people were about 10% more uncomfortable with drones when negatively primed than when positively primed.

For section 3.3, the regulation questions, the affinity to regulate score when positively primed was, on average, 3.25, which is slightly lower than the negatively primed average score of 3.44, but not significantly so. The number of participants with a higher affinity to regulate score (above a 3), after being positively primed, was 8.5 and after being negatively primed it was 8.94. Again this was statistically insignificant, although it indicates a slight rise in discomfort and affinity to regulate from negatively priming respondents. We suspected total averages may be hiding deeper differences *amongst the questions themselves*, and so we decided to conduct further analysis with a focus on *the scores for each question*, as we were mostly unsatisfied with the total scores analysis.

We conducted a Mann Whitney U test to compare the distributions of the negatively and positively primed answers against each other to see if there were any significant differences amongst the primed groups. A question would be significantly different if the (1 - p value) of the Mann Whitney U test is above 95%. The tables below show the results of the Mann Whitney U test for both the privacy questions and the regulations questions.

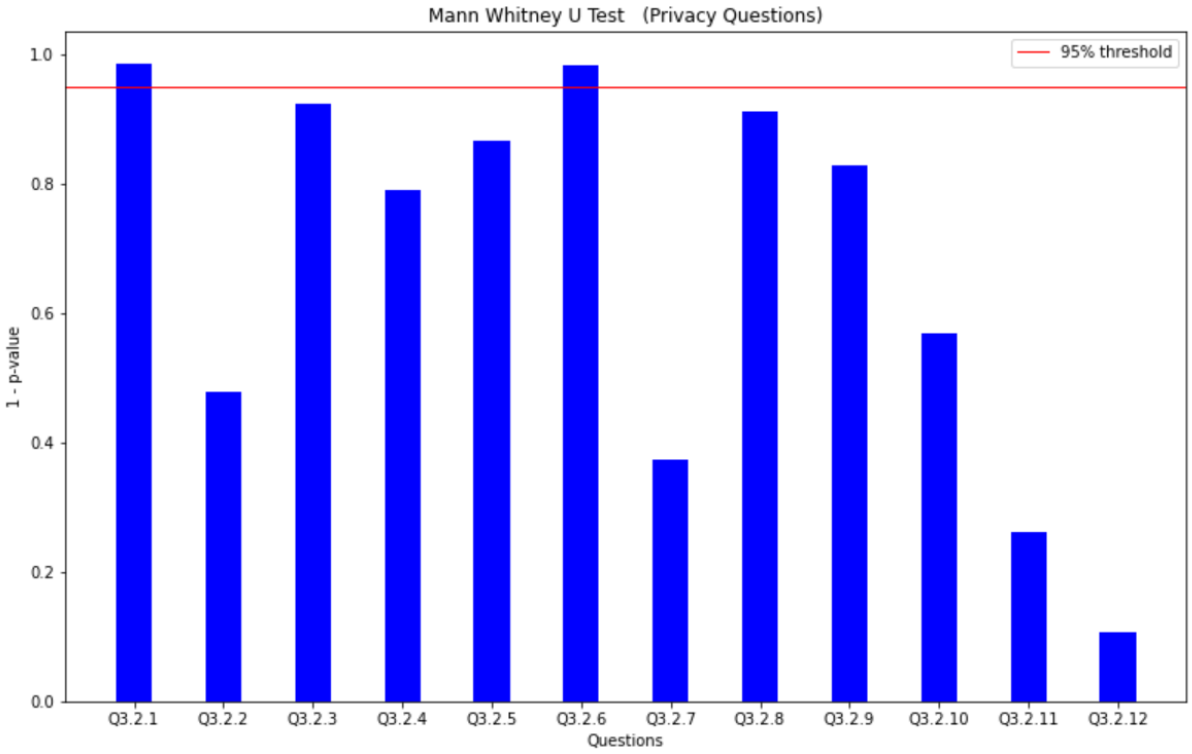

Fig 1. Mann Whitney U test results for privacy questions.

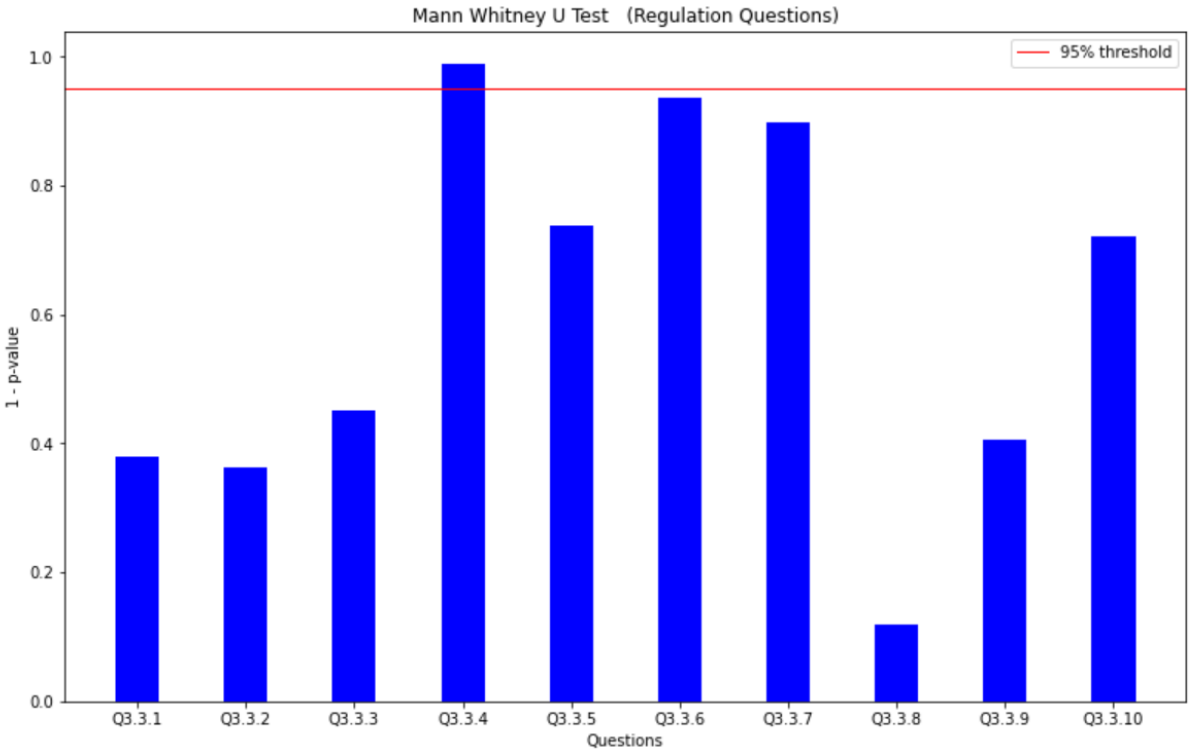

Fig 2. Mann Whitney U test results for the regulation questions.

Only some questions had statistically significant differences, but not all of them. Unfortunately, our hypothesis that there would be a significant difference seems to have fallen short, as a minority of question responses were different, while the majority was not significantly different. This would indicate that the priming had little effect on the participants.

After the Mann Whitney U test, we decided to further analyze the data by displaying the score differences for each question. To measure this difference, we defined the difference score for privacy questions as the *increase in discomfort*. While the difference score for regulations questions is the *increase in affinity to regulate*. If the difference score in the privacy questions is above 0, then the negative priming had more of an effect, but if it is below 0 then the stronger effect came from positive priming. If the difference score in the regulations questions is above 0, then the negative priming had more of an impact on the responses, and if it is below 0 then the positive priming had more of an impact. The results are displayed in the image below.

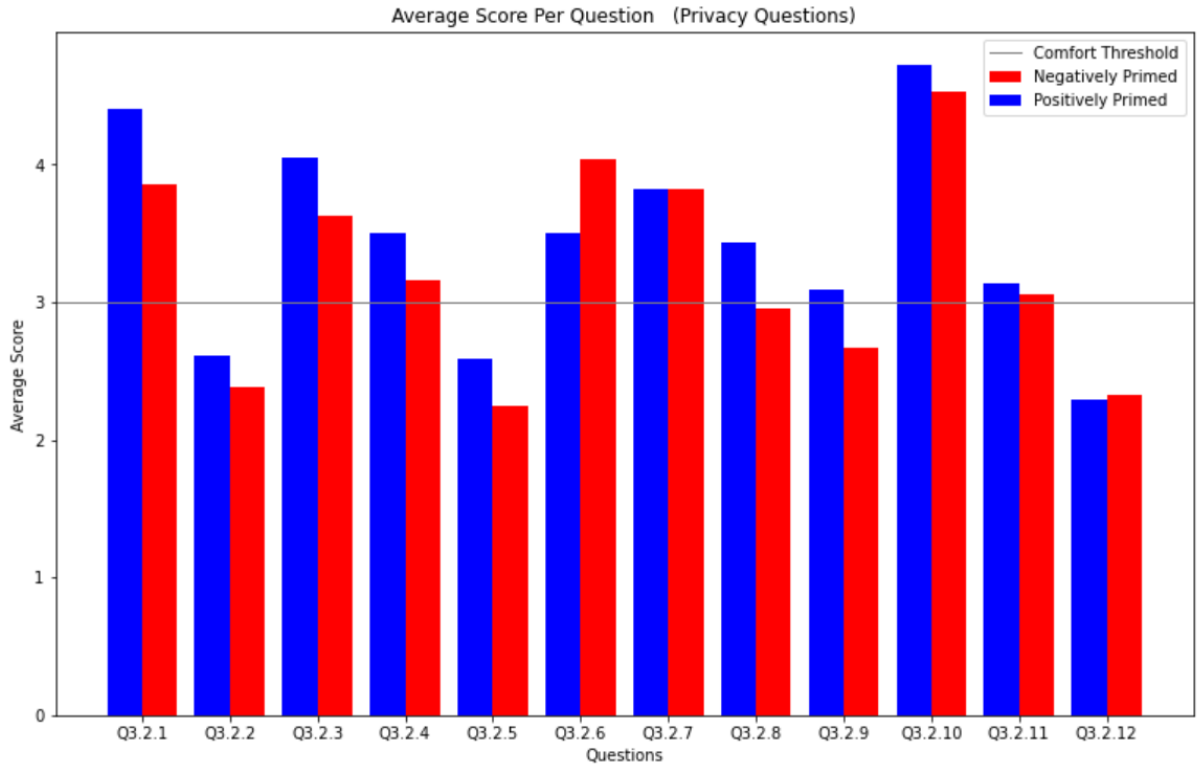

Fig 3. Average score of privacy questions from both response groups.

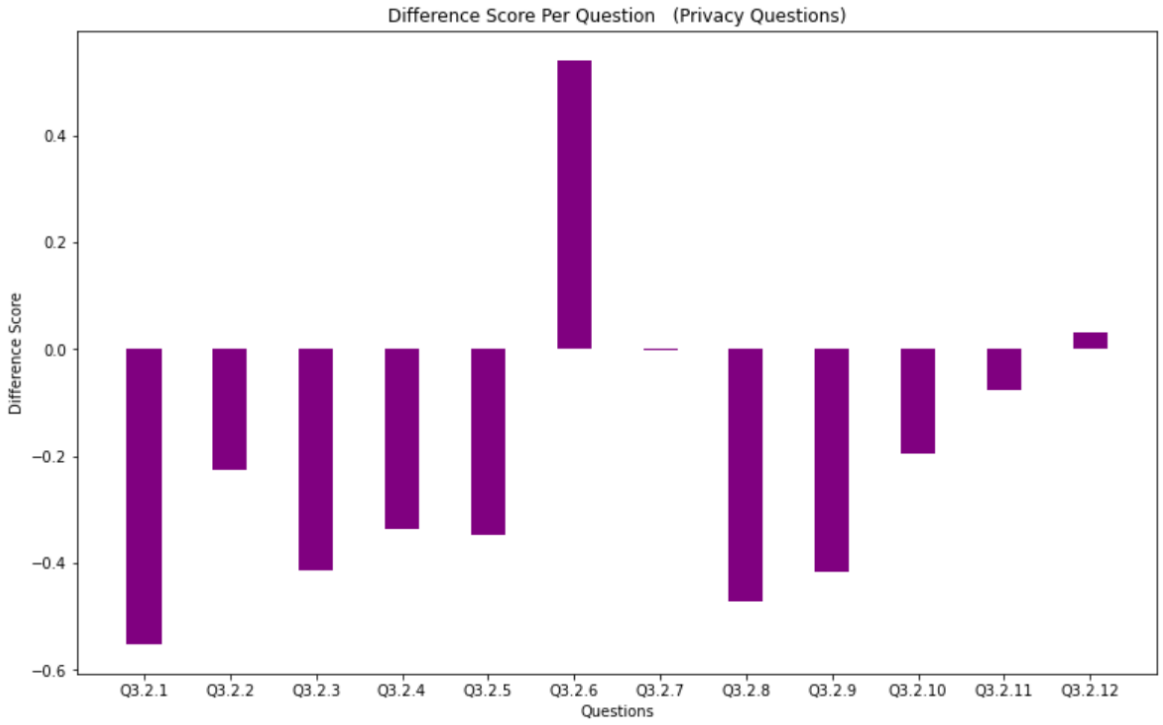

Fig 4. The response difference score of privacy questions from negatively primed participants.

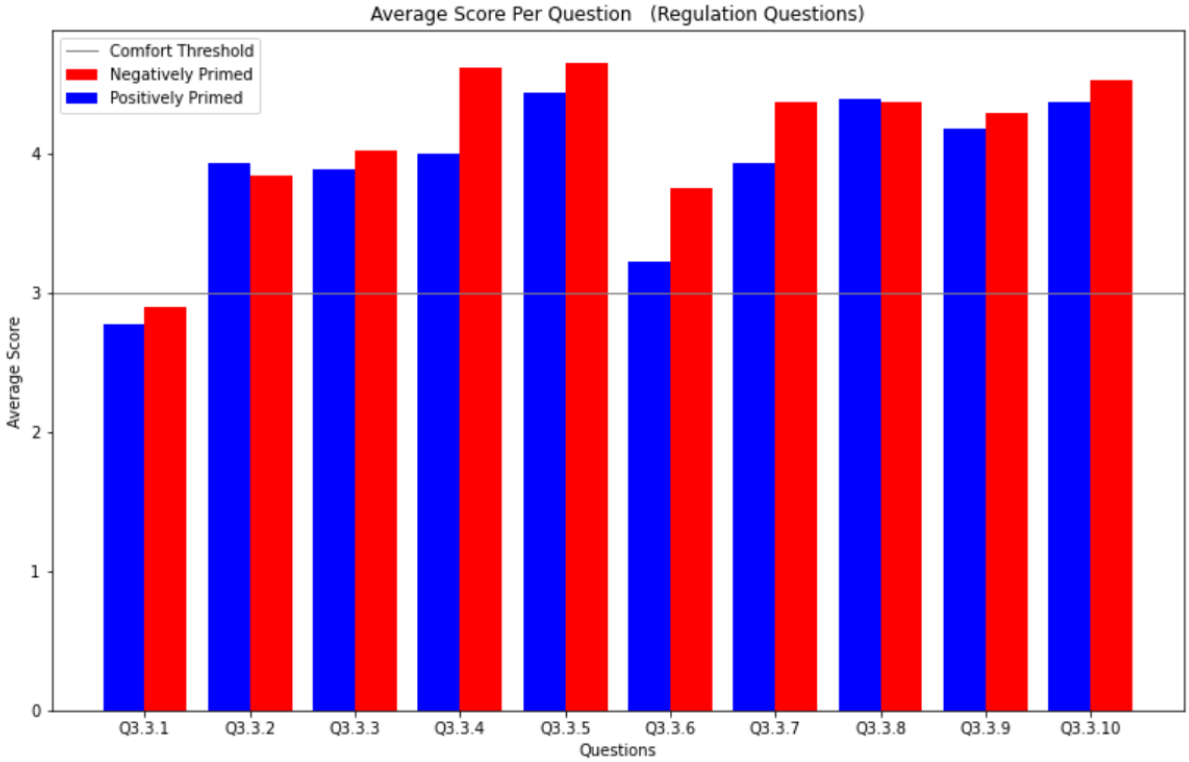

Fig 5. Average score of regulations questions from both response groups.

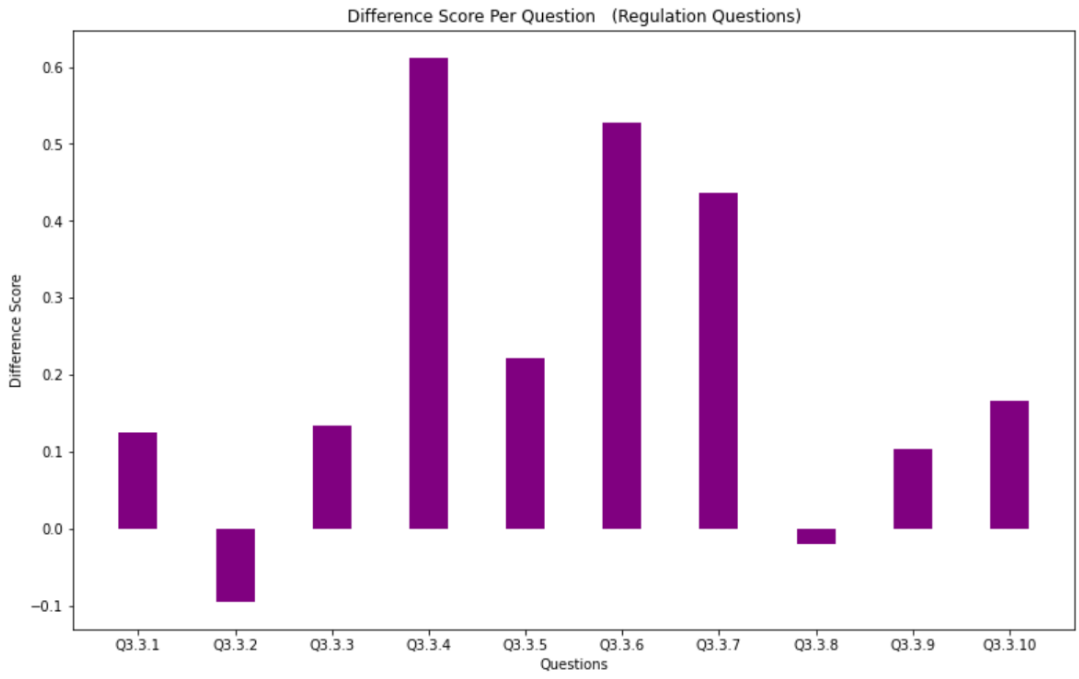

Fig 6. The response difference score of regulations questions from negatively primed participants.

Our python file for the data analysis can be found at https://colab.research.google.com/drive/1DKmxSmcNj8oV4NYVXLn5qOWAqTpNsset?usp=sharing

4 Results

Overall, the results seem to promote our hypothesis that participants would become less comfortable and have an increased affinity to regulate drones when presented with negatively priming material. However, the impact of negative priming was not as significant as expected, with a decrease in comfort of only 10%. Despite minimal overall results in support of our hypothesis, additional conclusions can be drawn when looking specifically at the data analysis for the respective Privacy and Regulation questions.

4.1 Analysis on Privacy Questions

Analysis can be done with each method of looking at the data we collected.

Starting with the Mann Whitney U Tests for the Privacy Questions, there were two questions that passed the threshold as being statistically significantly different among the two differently primed groups. The first is question 3.2.1, which has users rate the statement “I believe drone technology is useful”. The second is question 3.2.6, which has users rate the statement “I am

comfortable with people using drones for personal use". What becomes clearer when looking at the average score per question for the differing groups is the fact that, for Question 3.2.1, people who were positively primed were more likely to believe the technology is useful (with a higher average score), while for Question 3.2.6 people who were negatively primed were more likely to be comfortable with the technology. When it comes to question 3.2.1, this makes sense because the priming materials showed positive uses of drones to save lives, while the negative priming showed misuse with minimal context on situations where drones would be useful. This result is also in line with our hypothesis, because the difference in priming pertaining to drone uses and privacy harms led to a difference between the two groups. For question 3.2.6, it is less clear what made the negatively primed group more comfortable with personal drone use compared to the positively primed group. A possible explanation is that the priming mainly dealt with law enforcement and other large organizations misusing drones, which means that by contrast the privacy harms of personal use could seem less problematic. This difference might be statistically significant, but it goes against what we would expect with our hypothesis – however it can still be explained by further surveying.

There are a few additional questions that had differences in average answers that were close to the threshold but did not pass it for the Mann Whitney U Test. These questions showed similarly large bars for the double bar graphs marking the differences between the positively and negatively primed groups. This included questions 3.2.3 and 3.2.8, which ask participants to rate the following statements, respectively: "I am comfortable with drones using GPS technology" and "I am comfortable with companies using drones for security". This is also in line with our hypothesis, because it shows nearly statistically significant differences for statements that show a feature of drones that could be privacy invasive (by showing user locations) and a use of drones that could lead to participant harm (security). This also has ties to the priming materials. For question 3.2.3, the positively primed participants would be more likely to recognize the benefits of location tracking technology because their materials talked about finding people who are in peril from natural disasters, while the negatively primed individuals would find this information invasive because of the law enforcement connotations. For question 3.2.8, there are less connections to the positively primed participants' reading, but the negatively primed individuals might connect this usage of drones with the police usage and chilling effect from their priming materials.

There are also interesting differences that can only be seen when looking at the averages graph. This includes questions where the averages for the positively and negatively primed groups straddle the dividing bar at 3. This occurs for questions 3.2.8 and 3.2.9, which also have similarly sized differences when looking at Figure 4. Question 3.2.8 asks participants to rate the phrase "I am comfortable with companies using drones for security", while question 3.2.9 asks participants to rate the phrase "I am comfortable with the government using drones for law enforcement aid". While neither of these questions showed statistically significant differences between the

positively and negatively primed groups, I still think it is notable that the averages for the respective groups ended with the positively primed participants above the "comfort threshold" at 3 and the negatively primed participants below that threshold. This meant that via our established definition, positively primed participants are comfortable with security drones while negatively primed participants are not (albeit by a slim margin), and that positively primed participants are comfortable with law enforcement drones (once again by a slim margin) while negatively primed participants are not. This is a notable result for this study because the priming materials were specifically about drones used by law enforcement for either helpful or privacy invasive activities, so seeing a difference right around the "comfort threshold" for questions that are closely related to the priming materials could indicate that (at least on the qualitative level) the articles that primed the individuals had some measure of an effect.

Beyond the analysis that can be done when looking at the differences between the primed groups, there are also some general trends that occur in both groups. One such trend is the fact that the average scores for certain questions are notably far into the positive or negative sides. For questions 3.2.2, 3.2.5, and 3.2.12, both the positively and negatively primed groups have averages that are fairly low, because they are fairly below the neutral number 3. Question 3.2.2 asks respondents to rate the statement "I believe information collected by drones will be used only for intended purposes". Question 3.2.5 asks respondents to rate the statement "I am comfortable with drones using facial recognition technology". Question 3.2.12 asks respondents to rate the statement "I do not worry about drones infringing on my privacy". When taken together, these questions are ones that very clearly have privacy implications, mentioning the data collected by drones, invasive features, and simply asking whether privacy concerns pertaining to drones are a worry for participants. This seems to indicate that overall, regardless of the priming, there is general hesitation surrounding drones, and people have concerns about their privacy implications. However, the fact that we only see these dual low ratings for questions that are very clear in terms of their privacy violations seems to indicate that people won't take the extra steps to determine how different drone features and behaviors can invade privacy, but are willing to express doubts when the initial connection between the behavior/feature and privacy is done for them.

4.2 Analysis on Regulation Questions

The regulation question data also yields results when looking at both methods of data analysis.

Starting with the Mann Whitney U Test for the regulation questions, there was only one question that surpassed the threshold for this test, which was question 3.3.4. Question 3.3.4 had participants rate the following regulation on a scale from Unnecessary to Necessary: "Requiring physical indicators for drone's uses (for example, specific icons for personal vs commercial vs government drones)". In line with our hypothesis, the negatively primed group found the

regulation to be more necessary than the positively primed group, and in this case it was by a significant amount. This is likely to alleviate concerns as to who is collecting information via drones, which could be linked to the negatively primed participants' reading, which dealt with drones that individuals did not want or know about identifying them in a protest crowd. In contrast, the positively primed participants' reading dealt with a drone use that didn't emphasize who was using the drones, as saving people's lives is a context where the people being saved do not care as much about who operates the drone so long as it provides aid.

Similar to the privacy questions section, the regulation questions also had a few questions that had difference scores close to the significance level for the Mann Whitney U Test. This included questions 3.3.6 and 3.3.7, which corresponded with the following regulations, respectively: "Limits on the altitude above the earth that drones can fly" and "Limits on locations where drones can be used". These regulations likely saw higher "necessary" ratings from negatively primed individuals because they want to ensure that drone uses aren't abused, due to the law enforcement abuses mentioned in the negatively primed participants' reading. This is especially true for question 3.3.7, because of the use of drones outside a person's window that was mentioned in the reading, and the clear protection from privacy harms that can be seen by individuals who have that context.

Additional trends can be obtained from looking at the graphs for the average score per question for the positively and negatively primed groups, as opposed to just the Mann Whitney U Test graphs. One of these features is the fact that there is only one regulation where the average scores are below the "Comfort Threshold" at 3, with all other regulations being seen as necessary by both the positively and negatively primed groups. This regulation is the most innocuous of all of the regulations, and has averages that are only slightly below the "comfort threshold" for both the positively and negatively primed groups. This is question 3.3.1, which asks participants to rate the regulation statement: "Limits on the colors of drone bodies". Such a regulation was included by us as a starting point for regulations, that is, from the perspective of us as researchers based on the literature review we conducted, fairly unnecessary and not really viewed as necessary by drone regulators. It is of note that even for a relatively unnecessary regulation, the average score for the negatively primed group was still higher than the positively primed group, showing that they were slightly more willing to regulate drones, even when the regulations wouldn't have obvious privacy benefits. The overall trend that the rest of the questions shows, though, by all having averages that indicate that participants viewed the regulations as necessary, is that regulation is something generally preferred by participants.

Furthering this analysis is the fact that the averages for the remaining questions were all significantly higher than the "comfort threshold", either above or only slightly below a value of 4. The only exception to this trend was question 3.3.6, which had participants rate the regulation "Limits on the altitude above the earth that drones can fly". This is in line with the overall trend

that participants want regulations, because this question describes a regulation that can't be easily extrapolated into how it affects the people interacting with the drone. Limits on flight altitude doesn't have clear risks to privacy, so people aren't as likely to view it as a necessary regulation. This can be directly contrasted with the consistent high averages among both positively and negatively primed participants on questions 3.3.8, 3.3.9, and 3.3.10, which are more clearly tied to privacy concerns. The regulations discussed by these questions are "Limits on types of information that drones can collect", "Limits on the technologies that drones can be equipped with (for example, facial recognition technology)", and "Mandates that any information collected by drones must be protected from unauthorized access", respectively.

The final overall trend that is clear from the dual bar graph on the averages of the positively and negatively primed participants is that for all questions except 3.3.2 and 3.3.7, the negatively primed participants are more likely to view specific regulations as necessary. Questions 3.3.2 and 3.3.7 also only show slightly higher averages in favor of the regulations among positively primed participants, and are for the regulations "Limits on the level of sound drones can make while in flight" and "Limits on locations where drones can be used". There is no clear indicator within our data for why this exception exists. However, the overall trend is still in favor of priming causing participants to view regulations as more necessary, due to the consistently higher averages for negatively primed individuals.

5 Discussion

Finally, we will discuss the meaning of our findings and the privacy implications for the drone industry and regulators, and present future research paths or improvements.

5.1 Limitations

While this study provides informative views on drone privacy, it has three limitations. Convenience sampling and recruitment bias may have affected our results because survey participants only came from Carnegie Mellon and contacts close to the authors. This limits the generalizability of the study to other populations and countries. This limitation was the result of convenience and time constraints due to our course schedule. We wanted to obtain respondents quickly, which meant recruiting other students on campus and contacting friends and relatives. Future studies on the subject should be extended and diversified to other populations as well as to other nations.

Second, we did not include a control group in our study. Both groups were "treated" in the sense that they read priming excerpts on drone privacy before they filled out the survey. An additional group that read no priming excerpt may have enabled us to view current perceptions of drone privacy without "nudging" participants in a certain direction. This would require an even larger number of respondents, as we would effectively divide our dataset into three groups. This

affected our analysis, however we believe there is much to learn from even from this limited study, and would encourage others to pick up where we left off. Despite this, any previous knowledge on drones and privacy that helps form personal opinions on the technology could be considered “priming” and should be accounted for in these types of studies.

The third limitation is the survey format. Although our online survey allowed us to reach over 100 participants and learn about their opinions on drone privacy, it was shortened in length and limited in depth in order to decrease the survey completion time. Another format limitation was the lack of emotional incentive for the participants as the questions were abstract and no real risk of privacy harm was introduced in the survey. We suspect that respondents would provide more meaningful answers if they were given or placed in specific scenarios of privacy harm. This is further proven by simple review of some of the survey responses– at least three of the respondents completed the survey in short times and didn’t change any of the questions from their default values, suggesting that they simply clicked through the pages to reach the rewards slide. We left them in the dataset because there is no way to confirm our suspicions. Additionally, there are potentially many other variables that could explain drone privacy perceptions and help inform public policy, but are currently unknown or not being studied. Research that is more in depth could also explore the privacy costs and societal benefits that people think come from drone technology.

5.2 Policy Recommendations

It is incredibly challenging for regulators to balance drone technology innovation with privacy. Like many other new technologies, drone use has outpaced government regulations. We have created a set of policy prescriptions that are necessary to prevent this from continuing.

1. Implement industry-specific self-regulation, increase federal regulations by the FAA, or implement state and local laws to protect the public.
2. Regulators must take the public perceptions, expectations, and concerns of privacy into account by furthering research to develop legislations accordingly.
3. Regulators must take into account the information the public is being presented about drones as it impacts their receptiveness to policies.
4. Raise public awareness towards privacy issues of drones.
5. Create a regulatory regime that will be capable of keeping up with technological innovations.
6. Companies that produce and operate drones must have privacy policies and be transparent about their data collection practices.

These policy recommendations are based on the research done for our literature analysis as well as the results of our study. There seems to be some indication that the manner in which drone information is presented impacts the perceptions that people have about how drones are or are not privacy invasive, as well as what regulations they want as a result. Thus, some of our recommendations are from the perspective that policymakers need to take into account the

impact of the narrative that policy information is presented in.

A comprehensive set of policy prescriptions will help ensure that citizens are protected and can decrease the occurrence of privacy harms. Drone technologies will undoubtedly change our lives in the near future, which makes this a time-sensitive issue. The sooner that governments act, the more likely the public will be adequately protected.

5.3 Future Research Areas

Data on the public opinions of drone privacy and use are scarce. The wide applications of drone technologies also necessitate sector-specific research to help inform policy. Currently, governments don't have a good idea on what drone regulations the public expects. We believe that continuous research on public perceptions of drone privacy will be necessary to create a comprehensive regulatory regime. Preferences of the public are an extremely important consideration when drafting legislation. As drones will inevitably become a larger part of our lives, it will be increasingly important for governments to keep up with the speed of drone technology adoption.

Further, we believe that additional research pertaining to how priming impacts the acceptance of drone technology or drone regulations is similarly important. The public will have different opinions on drones depending on what information they have about drone technology. Some additional methods to test priming could include priming participants on different usage scenarios, as both of our example passages pertained only to use by law enforcement. Additionally, priming can be done with more damaging contexts of drone use, like drones used in warfare, or with more explicit mentions of privacy violations.

6 Conclusion

Our study investigated the underdeveloped research area of priming and technology, specifically looking at whether priming individuals influences their perceptions on privacy violations of drones and the legislation options to regulate them. We found that priming did indeed have an impact on participants in terms of their privacy and regulation viewpoints, but that the areas that this was seen were not as widespread as we initially hypothesized. Instead of seeing clear results across the majority of the questions, we only saw them in a few key questions discussed in the above results section. One of the notable statistics from this section was that the negative priming made individuals 10% less likely to be above the "comfort threshold" when it came to questions pertaining to privacy and drones.

Drone regulations are set to be a significant area for lawmakers in the upcoming years as drones continue to develop technologically and become more integrated in society. Keeping in mind the narratives that surround drone use is an important factor when it comes to rolling out drone

regulations, as the information that people have already learned regarding drones, and the information that accompanies that legislation during the law implementation will affect how they view drones and the new regulations. Understanding people's tendencies when it comes to perceiving technological advancements like drones is important not only to guide legislation creation, but also its adoption in society. Further research in priming and perceptions is key to help facilitate these processes.

Bibliography

1. Security, 911. “Drone Laws and Regulations in the USA.” 911, 2022. https://www.911security.com/learn/airspace-security/drone-laws-rules-and-regulations.
2. “Drone Laws in the U.S.A.” UAV Coach, June 13, 2022. https://uavcoach.com/drone-laws-in-united-states-of-america/.
3. Martin, Caroline Wimbly, and Ethan Barr. “Drone Privacy Law: Get out of My Space.” Lutzker & Lutzker, September 24, 2020. https://www.lutzker.com/get-out-of-my-space-drones-and-privacy-law/.
4. “Voluntary Best Practices for UAS Privacy, Transparency, and Accountability.” NTIA, May 18, 2016. https://www.ntia.doc.gov/files/ntia/publications/uas_privacy_best_practices_6-21-16.pdf.
5. FindLaw Staff. “Drone Laws by State.” Findlaw, July 12, 2021. https://www.findlaw.com/consumer/consumer-transactions/drone-laws-by-state.html.
6. DuBois, Gretchenn, and Jonathan Bates. “Current Unmanned Aircraft State Law Landscape.” National Conference of State Legislatures, August 3, 2021. https://www.ncsl.org/research/transportation/current-unmanned-aircraft-state-law-landscape.aspx.
7. Voss, Gregory W. “Privacy Law Implications of the Use of Drones for Security and Justice Purposes.” International Journal of Liability and Scientific Enquiry. www.researchgate.net, https://www.researchgate.net/publication/264822950_Privacy_Law_Implications_of_the_Use_of_Drones_for_Security_and_Justice_Purposes. Accessed 5 October 2022.
8. Lee, D., Hess, J. D., & Heldeweg, M. (2022, August 13). Safety and privacy regulations for unmanned aerial vehicles: A multiple comparative analysis. Technology in Society. Retrieved from https://www.sciencedirect.com/science/article/pii/S0160791X22002202
9. Butler, D. (2019). Drones and Invasions of Privacy: An International Comparison of Legal Responses. University of New South Wales Law Journal. Retrieved from http://classic.austlii.edu.au/au/journals/UNSWLawJl/2019/37.html
10. Yao, J. (2021, April 12). The Practice and Problems of UAVs Regulation and Legislation in Local China from the Perspective of Public Safety. Open Journal of Social Sciences. Retrieved from https://www.researchgate.net/publication/350758581_The_Practice_and_Problems_of_UAVs_Regulation_and_Legislation_in_Local_China_from_the_Perspective_of_Public_Safety
11. Harri, K. '. -. (2018). DRONES: PROPOSED STANDARDS OF LIABILITY. Santa Clara High Technology Law Journal, 35(1), 65-109. Retrieved from https://www.proquest.com/scholarly-journals/drones-proposed-standards-liability/docview/2135080353/se-2

12. Gruhl, J., & Combs, M. (2019). Police drones: Coming to a neighborhood near you. *National Political Science Review, 20*(1), 56-72. Retrieved from https://www.proquest.com/scholarly-journals/police-drones-coming-neighborhood-near-you/docview/2502254782/se-2
13. Kallman, Jesse. (2015) *Airware Testifies Before Congress on Commercial Drone Technology & Safety*. Youtube. https://www.youtube.com/watch?v=SuVcCX2lu60&t=746s.
14. *Best Practices for Protecting Privacy, Civil Rights & Civil Liberties In Unmanned Aircraft Systems Programs*. (2015, December 18). Department of Homeland Security https://www.dhs.gov/publication/best-practices-protecting-privacy-civil-rights-civil-liberties-unmanned-aircraft-systems.
15. *Voluntary Best Practices for UAS Privacy, Transparency, and Accountability*.(2016, May 18). National Telecommunication and Information Administration. https://www.ntia.doc.gov/files/ntia/publications/uas_privacy_best_practices_6-21-16.pdf.
16. Airborne Public Safety Association. https://publicsafetyaviation.org/events/uas-training.
17. *DOI UAS Privacy*. Department of the Interior. https://www.doi.gov/aviation/uas/privacy.
18. *UAS Collegiate Training Initiative Program.* (2020, April). Federal Aviation Administration. https://www.faa.gov/sites/faa.gov/files/uas/educational_users/collegiate_training_initiative/UAS_CTI_Program.pdf
19. Stevens, N. Mia. *Geofencing for Small Unmanned Aircraft Systems in Complex Low Altitude Airspace*. (2019). University of Michigan Library, Deep Blue Repositories. https://deepblue.lib.umich.edu/bitstream/handle/2027.42/153391/minist_1.pdf?sequence=1.
20. Kim, J.; Atkins, E. *Airspace Geofencing and Flight Planning for Low-Altitude, Urban, Small Unmanned Aircraft Systems*. (2022, January 7) Appl. Sci. 2022, 12, 576. https://doi.org/ 10.3390/app12020576.
21. Chang, V., Chundury, P., & Chetty, M. (2017, May 1). *Spiders in the Sky: Proceedings of the 2017 CHI conference on human factors in computing systems*. ACM Conferences. Retrieved October 7, 2022, from https://dl.acm.org/doi/abs/10.1145/3025453.3025632?casa_token=6voLSt0RdYsAAAAA%3AUHUBEbhS5x9GEx8M8jauukMRtOgFH_d7hE_Y4raBj0B2RPH-1yXdPflqtsZ2h523tAQMmuxQt3mc
22. Rice, S. (2019, February 4). *Eyes in the sky: The public has privacy concerns about drones*. Forbes. Retrieved October 7, 2022, from https://www.forbes.com/sites/stephenrice1/2019/02/04/eyes-in-the-sky-the-public-has-privacy-concerns-about-drones/?sh=68cda2166984
23. Scharre, P. (2019). Robots on Trial: Autonomous Weapons and the Laws of War. In *Army of none: Autonomous Weapons and the future of war* (pp. 250–270). essay, W. W. Norton & Company.

24. Wang, Y., Xia, H., Yao, Y., & Huang, Y. (2016, July). *Flying Eyes and Hidden Controllers: A Qualitative Study of People's Privacy Perceptions of Civilian Drones in The US*. ResearchGate. Retrieved October 7, 2022, from https://www.researchgate.net/publication/302065844_Flying_Eyes_and_Hidden_Controllers_A_Qualitative_Study_of_People's_Privacy_Perceptions_of_Civilian_Drones_in_The_US
25. Lidynia, C., Philipsen, R., Ziefle, M. (2017). Droning on About Drones—Acceptance of and Perceived Barriers to Drones in Civil Usage Contexts. In: Savage-Knepshield, P., Chen, J. (eds) Advances in Human Factors in Robots and Unmanned Systems. Advances in Intelligent Systems and Computing, vol 499. Springer, Cham. https://doi-org.cmu.idm.oclc.org/10.1007/978-3-319-41959-6_26
26. *Supreme Court of the United States*. (n.d.). Retrieved October 8, 2022, from https://www.supremecourt.gov/opinions/13pdf/13-132_8l9c.pdf
27. Serafinelli, E. (2022). Imagining the social future of drones. Convergence, 28(5), 1376–1391. https://doi.org/10.1177/13548565211054904
28. Z. Lv, L. Qiao, M. S. Hossain and B. J. Choi, "Analysis of Using Blockchain to Protect the Privacy of Drone Big Data," in IEEE Network, vol. 35, no. 1, pp. 44-49, January/February 2021, doi: 10.1109/MNET.011.2000154.
29. T. Rana, A. Shankar, M. K. Sultan, R. Patan and B. Balusamy, "An Intelligent approach for UAV and Drone Privacy Security Using Blockchain Methodology," 2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence), 2019, pp. 162-167, doi: 10.1109/CONFLUENCE.2019.8776613.
30. "Flying High: Shaping the Future of Drones in UK Cities." nesta, July 23, 2018. https://www.nesta.org.uk/event/flying-high-shaping-future-drones-uk-cities/.
31. www.aclu.org. (2022, September 22). www.aclu.org. Retrieved from www.aclu.org: https://www.aclu.org/issues/privacy-technology/surveillance-technologies/domestic-drones
32. Rice, S. (2019, February 4). www.forbes.com. Retrieved from www.forbes.com: https://www.forbes.com/sites/stephenrice1/2019/02/04/eyes-in-the-sky-the-public-has-privacy-concerns-about-drones/?sh=1dbf8f776984
33. www.legalscoops.com. (2021, November 10). Retrieved from www.legalscoops.com: https://www.legalscoops.com/how-to-protect-civil-liberties-from-video-drones-and-modern-technology/
34. Guariglia, Matthew. How are police using drones? Electronic Frontier Foundation. January 6, 2022. https://www.eff.org/deeplinks/2022/01/how-are-police-using-drones
35. Public Safety Drones Save Four Lives In One Day. Shenzhen DJI Sciences and Technologies Ltd. June 6, 2018. https://www.dji.com/newsroom/news/drones-save-lives-public-safety-search-rescue-four-one-day.

36. Lidynia, C., Philipsen, R., Ziefle, M. (2017). Droning on About Drones—Acceptance of and Perceived Barriers to Drones in Civil Usage Contexts. In: Savage-Knepshield, P., Chen, J. (eds) Advances in Human Factors in Robots and Unmanned Systems. Advances in Intelligent Systems and Computing, vol 499. Springer, Cham. https://doi.org/10.1007/978-3-319-41959-6_26
37. Emami-Naeini, Pardis, Sruti Bhagavatula, Hana Habib, Martin Degeling, Lujo Bauer, Lorrie Faith Cranor, Norman Sadeh. Privacy Expectations and Preferences in an IoT World. 2017. https://users.ece.cmu.edu/~lbauer/papers/2017/soups2017-iot-privacy-prefs.pdf
38. Cara Bloom, Joshua Tan, Javed Ramjohn, Lujo Bauer. Self-Driving Cars and Data Collection: Privacy Perceptions of Networked Autonomous Vehicles. 2017. https://users.ece.cmu.edu/~lbauer/papers/2017/soups2017-self-driving-fleets-privacy-prefs.pdf
39. Malhotra, Naresh & Kim, Sung & Agarwal, James. (2004). Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. Information Systems Research. 15. 336-355. 10.1287/isre.1040.0032.
40. The Regulatory Review. “Regulating Domestic Drone Use.” The Regulatory Review, November 10, 2021. https://www.theregreview.org/2021/10/23/saturday-seminar-regulating-domestic-drone-use/.
41. West, Jonathan P., Casey A. Klofstad, Joseph E. Uscinski, and Jennifer M. Connolly. “Citizen Support for Domestic Drone Use and Regulation.” *American Politics Research* 47, no. 1 (2018): 119–51. https://doi.org/10.1177/1532673x18782208.
42. Buck, C., & Dinev, T. (2020). Low Effort and Privacy – How Textual Priming Affects Privacy Concerns of Email Service Users. Retrieved from https://pdfs.semanticscholar.org/a325/ebf28be90b9b615b5a2ae9978e4cdda91a53.pdf?_ga=2.147614644.2041726850.1670650010-1008577789.1670650010
43. Zhang, B., Kreps, S., McMurry, N., & McCain, M. R. (2020). Americans’ perceptions of privacy and surveillance in the COVID-19 pandemic. Retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7757814/

Appendix

1 Full Questionnaire

Please read survey information carefully. This survey explores opinions about drone technology. It is NOT intended to test or judge your knowledge of drone technology.

Section 1: Demographics

1. What is your age?
    a. Under 25
    b. 26-40
    c. 41-55
    d. Over 55
    e. Prefer not to say
2. What is your gender?
    a. Male
    b. Female
    c. Nonbinary
    d. Prefer not to say
3. What is your educational level?
   (Note: select the highest degree level you have completed)
    a. High School Diploma
    b. Associate's Degree
    c. Bachelor's Degree
    d. Master's Degree
    e. PhD
    f. Prefer not to say
4. If applicable, what was the focus of your degree?
    a. Computer Science
    b. Engineering
    c. Science
    d. Humanities
    e. Arts
    f. Not applicable
    g. Prefer not to say

Section 2: Background Information

Section 2.1: Encountering Drones in Real Life

The following questions are intended to gain context as to where you have interacted with drones in person in different use settings.

1. What is your highest level of real-life experience with drones?
    a. Never encountered a drone in real life
    b. Have seen a passive, non-flying drone
    c. Have encountered a drone in use
    d. Have operated a drone

Section 2.2: Past Knowledge of Drones

The following questions are intended to gain context as to your past knowledge of drones in different use settings.

2. What is your highest level of background knowledge of drones?
    a. No background knowledge on drones
    b. Have discussed drones with others, but not looked into the subject myself
    c. Have read articles on drones
    d. Have learned about drones in an academic or professional context

Section 3: Survey Body

The intent of this survey is to collect information on the privacy-related opinions people have pertaining to drone technology. Please proceed to the next page to read a short passage and answer some survey questions.

*(Randomly send users to one of two articles here)

Priming for the privacy harms of drones:

"We've spent years seeing police drones being deployed in more and more mundane policing situations and in punitive ways. After the New York City Police Department accused one racial justice activist, Derrick Ingram, of injuring an officer's ears by speaking too loudly through his megaphone at a protest, police flew drones by his apartment window—a clear act of intimidation. The government also flew surveillance drones over multiple protests against police racism and violence during the summer of 2020. When police fly drones over a crowd of protestors, they chill free speech and political expression through fear of reprisal and retribution from police. Police could easily apply face surveillance technology to footage collected by a surveillance drone that passed over a crowd, creating a preliminary list of everyone that attended that day's protest. As we argued back in May 2020, drones don't disappear once the initial justification for purchasing them no longer seems applicable. Police will invent ways to use their invasive toys–which means that drone deployment finds its way into situations where they are not needed, including everyday policing and the surveillance of First Amendment-protected activities."

Priming for drones in a trustworthy manner by telling the respondent that drones are capable of saving lives:

"At least 133 people have now been rescued from peril by drones. [...] Police, fire and rescue services, as well as bystanders in the right place at the right time, have used drones to find missing people and deliver supplies to people stranded in water, forests, ditches, mountains and fields. Drones can cover far more area than searchers on land or

water, and can use thermal imaging cameras to peer through smoke, fog, darkness or vegetation to find unconscious people. Drones also allow public safety agencies to reduce the risk of injury to rescuers, who might otherwise place themselves in peril on search and rescue missions. DJI [a drone technology company] tracks drone rescues reported on traditional and social media to illustrate the lifesaving value of drone technology and demonstrate how wider access to drones has helped improve public safety."

Section 3.1: Informational Material

1. Did you read the short text?
    a. Yes, I read and understand the text
    b. No, I did not read the text (please read)

Section 3.2: Privacy Questions

Indicate agreement with the following statements on a scale of 1-5, where 1 represents “Strongly Disagree” and 5 represents “Strongly Agree”

1. I believe drone technology is useful.
2. I believe information collected by drones will be used only for intended purposes.
3. I am comfortable with drones using GPS technology.
4. I am comfortable with drones using audio-visual recording technology.
5. I am comfortable with drones using facial recognition technology.
6. I am comfortable with people using drones for personal use.
7. I am comfortable with companies using drones for package and food delivery.
8. I am comfortable with companies using drones for security.
9. I am comfortable with the government using drones for law enforcement aid.
10. I am comfortable with the government using drones for natural disaster response.
11. I believe anyone should be able to own a drone.
12. I do not worry about drones infringing on my privacy.

Section 3.3: Regulatory Questions

Governments have the ability to regulate certain aspects of drone usage. Indicate agreement with the following potential regulations on a scale of 1-5, where 1 represents “Highly Unnecessary” and 5 represents “Highly Necessary”

1. Limits on the colors of drone bodies
2. Limits on the level of sound drones can make while in flight
3. Requiring uniform appearance for drones of specific uses
4. Requiring physical indicators for drone’s uses (for example, specific icons for personal vs commercial vs government drones)
5. Requiring physical indicators when drones are collecting information (for example, a light to show they are recording)
6. Limits on the altitude above the earth that drones can fly
7. Limits on locations where drones can be used

8. Limits on types of information that drones can collect
9. Limits on the technologies that drones can be equipped with (for example, facial recognition technology)
10. Mandates that any information collected by drones must be protected from unauthorized access

Section 4: Existing Views on Privacy

The following questions are about your views on privacy. Indicate agreement with the following statements on a scale of 1-5, where 1 represents "Strongly Disagree" and 5 represents "Strongly Agree"

1. Consumer data privacy is really a matter of consumers' right to exercise control and autonomy over decisions about how their information is collected, used, and shared.
2. Consumer control of personal information lies at the heart of consumer privacy
3. I believe that data privacy is invaded when control is lost or unwillingly reduced as a result of a marketing transaction.
4. Companies seeking information online should disclose the way the data are collected, processed, and used.
5. A good consumer online privacy policy should have a clear and conspicuous disclosure.
6. It is very important to me that I am aware and knowledgeable about how my personal information will be used.
7. It usually bothers me when online companies ask me for personal information.
8. When online companies ask me for personal information, I sometimes think twice before providing it.
9. I'm concerned that online companies are collecting too much personal information about me.
10. Online companies should devote more time and effort to preventing unauthorized access to personal information
11. Computer databases that contain personal information should be protected from unauthorized access – no matter how much it costs.
12. Online companies should take more steps to make sure that unauthorized people cannot access personal information on their computers.

Section 5: Reward Lottery

Thank you for completing our survey! The following is a link to a separate google form to collect your email address so we can contact the winners of our raffle for three $50 Visa gift cards. This information cannot be connected to your responses on this survey, however the choice to enter the raffle is still voluntary.

<link here>