Advocating for Users' Privacy Protections: A Case study of COVID-19 apps

Tanusree Sharma
tsharma6@illinois.edu
University of Illinois at Urbana-Champaign
Champaign, Illinois

Tian Wang
tianw7@illinois.edu
University of Illinois at Urbana-Champaign
Champaign, Illinois

Masooda Bashir
mnb@illinois.edu
University of Illinois at Urbana-Champaign
Champaign, Illinois

ABSTRACT

Mobile apps are being utilized in different regions around the world for contract tracing during this COVID-19 pandemic and many of these apps require personal information to be shared. The COVID-19 crisis has demonstrated how critical it is that we embrace virus-response opportunities given to us through technology, but we should also keep in mind that while we use these novel technologies to combat the pandemic, we must also ensure that users' privacy and security is contained. Therefore, in this project we assessed privacy controls that are offered in COVID-19 apps and what users are identifying to be their preferences if they were to adopt a COVID-19 app. Our results show that while the majority of the apps did not provide adequate privacy controls, users do consider these to be important factors in their decision making. In addition, we believe our preliminary findings can provide foundation for inclusive privacy features that is human-centered.

CCS CONCEPTS

• **Security and privacy** → **Privacy protections**.

KEYWORDS

Privacy, Human-Centered Design, Trust, Security, Mobile apps

ACM Reference Format:
Tanusree Sharma, Tian Wang, and Masooda Bashir. 2020. Advocating for Users' Privacy Protections: A Case study of COVID-19 apps. In *22nd International Conference on Human-Computer Interaction with Mobile Devices and Services (MobileHCI '20 Extended Abstracts), October 5–8, 2020, Oldenburg, Germany.* ACM, New York, NY, USA, 4 pages. https://doi.org/10.1145/3406324.3410711

1 INTRODUCTION

As the COVID-19 outbreak spreads all over the world, governments in multiple countries are pushing for location (GPS) and Bluetooth proximity technology as a form of digital contact tracing in response to the pandemic via mobile applications. A large number of applications have been developed in the past few months and many of these apps has been published under government/state support [6]. For example, a digital contact tracing app called COVIDSafe has been developed and announced by Australian Government to help with the COVID-19 outbreak [1]. While it is vital to contain the virus spread by using digital tracing as an effective approach, security and privacy concerns need to be carefully addressed to avoid harm of users' personal or sensitive information when developing and applying such applications [4]. Our literature review reveals that there is still a lack of guided-control in deploying context-based privacy controls that are needed as countermeasures of users' data [1], [5]. Therefore, there is much work to be done for improving the scope of privacy protections and placing applicable measures to minimize users' security and privacy susceptibility. The United State is still in an early stage of developing a framework for managing public health safety while preserving users' privacy, and thus it is essential and timely to consider privacy protections when designing COVID-19 apps that involve the use of sensitive and personal information. Therefore, we sought to assess COVID-19 associated apps to examine their privacy design and to determine if there are unanticipated privacy risks and compare these to users' expectations within those risks.

More specifically, the goal of this study is to understand how privacy protections are addressed as controls on COVID-19 related mobile applications, and the level of privacy considerations that users expects from these apps if they were to adopt them. Our research questions were:

- What type of privacy control are made available in the apps?
- What are users' privacy expectations for COVID-19 apps?

We believe that learning about users' expectations on specific privacy-related controls can be an effective way to design human-centered controls and can be helpful to app developers. This is particularly important for designing the COVID-19 mobile apps as the pandemic seems to be a highly politicized matter. In addition, we believe that by bringing technological development whence it is aligned with human perceptions and expectations, it would provide an important step forward towards inclusive privacy in mobile app environments and development life cycle.

2 METHOD

2.1 Study Design

Step1: To conduct our study, we collected 103 $COVID - 19$ apps from the Google Play Store. Based on the apps that had an APK file available for further analysis, we selected 48 apps in our sample which are from different countries. Thus, we analyzed 48 COVID-19 mobile apps for this study. Our investigation was based on **three**

MobileHCI '20 Extended Abstracts, October 5–8, 2020, Oldenburg, Germany
© 2020 Copyright held by the owner/author(s).
ACM ISBN 978-1-4503-8052-2/20/10.
https://doi.org/10.1145/3406324.3410711

[1] Australian Government Department of Health. COVIDSafe App. 2020. Retrieved June 17, 2020 from https://www.health.gov.au/resources/appsand-tools/covidsafe-app

specific criteria which are Data retention; Right to opt-in/opt-out and compliance. The rationale for considering these three privacy protection criteria was based on two aspects. One being that we wanted to focus our study on users having more control over their data and the second was based on previous literature from iapp [2] and NIST $800 - 53$ [2] which recommends specific types of privacy protections that could promote users trust in addition to providing security requirement for information system [2]. More precisely, some of the key recommendations by iapp prioritizes fostering trust in the application in order to uphold transparency, enable users to maintain their privacy and availing users with mechanisms to take informed decision upon proper understanding. Further, NIST also provides models for deploying trustworthiness in the system level. Therefore, in this study we decided to choose data retention as our **first** protection mechanism which includes functionality to make sure that data is securely deleted when it no longer required followed by **second** protection mechanism, Right to opt in/opt out which infers about decision making based on clear instruction and finally **third** protection mechanism, compliance which is to make sure that app is validated by application/region specific regulation. These three anticipated mechanisms can be useful to boost users' confidence during adoption.

Step2: We also analyzed COVID-19 survey responses from a Midwestern region that included 1550 participants. The survey data was collected by Dynata, LLC using Redcap survey platform. The survey was designed to assess individuals' attitudes toward using digital tracing apps and COVID-19 status apps, and factors that might contribute to either positive or negative attitudes towards these technologies. Though our user study is not comprehensive in comparing to our app collection, still we believe, our initial result might be useful to pin down the preferences of a particular nation including diverse population in respect to religion, belief, race, ethnicity, educational and professional background. Our sample includes population from United State where female (49.9%), male (49.2%) and non-binary/self-described gender (1%). It contains population from diverse ethnic background where White/European-American (68.3%), Black/African American (13.3%), Latino (6.7%), Asian (4.7%), Biracial (4.8%), Pacific Islander/Native Hawaiian (0.5%), Native American/Alaskan Native (0.5%), self-described/not answered (0.14%) with a age limit from 18 to 90 years (mean: 44.72 and sd: 16.537).

2.2 Privacy Protections in Apps

We focused our initial analysis on three privacy protection criteria that is related to controls on the apps: data retention, right to opt-in/opt-out, and compliance. For each app, all the three criteria were carefully reviewed, and the data was manually collected and recorded. We also recorded laws/regulations followed explicitly by the app.

Data retention: For the purpose of this study we refer to data retention as storage of any user data on the applications for compliance or other purposes. This also implies the preservation of information as long as it is needed and discarding it in a safely manner.

Right to opt-in/opt-out: The option to opt-in means that customers choose to use the service/ app or sign in and allow the app to use their information (either for processing or sharing with third parties), or receiving notifications from the app. The option to opt-out means that the user has the right/option at any time to direct a particular provider that is handling their data not to sharing data personal information with third parties anymore [3]. In case of app, it does not necessarily to uninstall an app, it also refers to users right to stop sharing their data.

Compliance: In relation to apps privacy, compliance is adhering to an existing privacy protection mechanism. So, compliance in this study means that the app reports conforming to any privacy regulations and policies to ensure that sensitive data like personal information is organized, managed, and shared on the app.

2.3 User Perspectives

To understand users' perspectives, we used responses from a survey questionnaire that assessed people's attitudes and opinions related to privacy protections when using COVID-19 apps. Specifically, we were focusing on the responses for two questions:

Q1: If you could be guaranteed that you could completely delete all of your data from this app at any time, would that make you more likely to use it? (Yes or No)

Q2: COVID-19 Mobile Apps should be regulated for privacy protections. (Strongly disagree, Disagree, Neither agree nor disagree, Agree, Strongly agree)

While the survey included several other questions related to privacy protections as well as assessment of users' concerns and preferences in adopting COVID-19 apps such as tracking users' movement, data sharing mechanism and security functionalities, however, we wanted to focus this study on two questions because these questions/responses were the most associated ones to our apps' (48 selected) analysis which was focused on data retention, opt in/out and compliance. Hence, we analyzed participants' responses for the above two questions (Q1 and Q2) to determine users' perspectives on the privacy protections that they would prefer when using COVID-19 mobile apps.

3 RESULTS

Below are the results on the five overlapping categories from both app controls and user perspectives that mentioned in the Method section: data retention (app), right to opt-in/opt-out (app), compliance (app), users' preference for COVID-19 apps retention practices, and users' attitude towards privacy protections on COVID-19 apps.

3.1 App Analysis Results

Data Retention: From the results, we could see that the data retention feature is not appropriately addressed in most apps we analyzed. Only 18 of the 48 apps clearly and explicitly include the control of data retention in their app. Data retention for 60% (29 out of 48) of the apps is either vague or not mentioned, and thus it is difficult to report exact results.

Right to Opt-in/Opt-out: Similarly, to data retention, the option to opt-in/opt-out is not included for 69% of the apps analyzed (33 out of 48). Nearly one-third of apps (13 out of 48) provide explicit

[2] Mobile and Privacy. $https : //iapp.org/media/pdf/resource_center/$

[3] California Consumer Privacy Act of 2018. http://leginfo.legislature.ca.gov/faces/

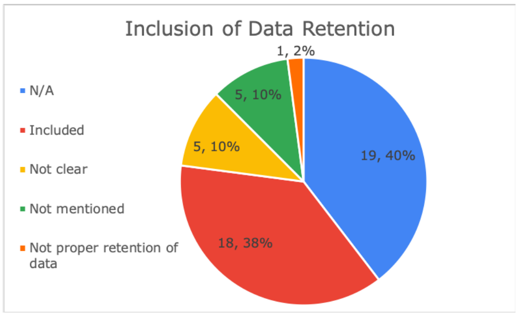

Figure 1: : Number and percentage of apps that included data retention.

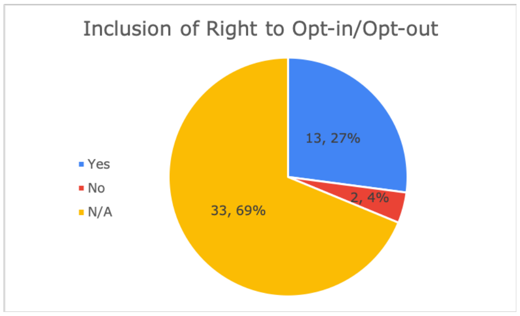

Figure 2: : Number/percentage of apps that includes opt-in/opt-out option.

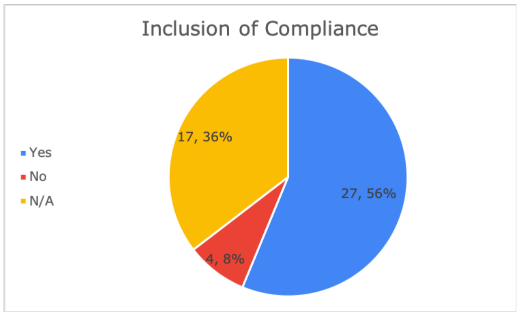

Figure 3: : Number/percentage of apps that indicates compliance.

selection to the users that allow them to choose to opt-in or opt-out when using the app.

Compliance: Comparing with data retention and right to opt-in/opt out, apps analyzed for this purpose are more likely to include compliance control. Over half of the apps (27 out of 48) explicitly included compliance in their app service. In our sample, 17 of the 48 apps don't specify the compliance policy in their app. There are 4 apps that have no compliance mentioned in the app, which are COVID-19 Tam from Mexico, Castor COVID-19 from Holland, StopKorona! from North Macedonia, and an app (non-English name) from Israel.

3.2 COVID-19 user survey results

User Preferences for COVID-19 Apps:: Out of the 1510 response, 65.3% of participants responded "Yes" to Q1. Other 34.5% respond "No" which mean they would not use mobile apps even if they could completely delete all of their data at any time. There could be other reasons behind this response which are trust on app providers; willingness to use those app based on their individual security concerns. From our survey, 74.8% participants are concerned about their security while using those apps. However, analysis of these factors is beyond this study focus where we only concentrated on privacy controls they would like to have. On the contrary our preliminary manual analyses reveal that only 18.38% of the apps include a data retention policy. Similarly, when examining opt in/ opt out features, only 13.27% out of total apps had this option available to users. From the results of Q1 in our user survey, we learned that users prefer to have control over their data and perhaps this feature may encourage people to use COVID-19 apps.

COVID-19 user survey results While our survey participants had a mean of 4.03 out of 5 for Q2, only 27.56% of the apps had indicated that they were compliant with particular laws/regulation.

4 DISCUSSION

Our initial results show that there seems to be a clear disconnect between what users' preferences are for privacy protections in COVID19 apps and what the apps offer. While over half of the apps we studied openly include information about their compliance with a privacy law/regulation the other half did not. The data retention and the option to opt-in/opt-out is even more detached from users wishes. As reported above, a small percentage of the apps have the inclusion of data retention or the opt-in/opt-out option.

From our survey results, it is evident that users do have privacy protection expectations when using COVID-19 apps. For example, they wanted assurance that they can delete their data any time they want which implies the kind of control they wish to have over their data. Hence, including such potential controls in designing COVID-19 apps to increase users' adoption of this technology might be a positive step forward. We know from previous studies that imposing the appropriate privacy compliance on an any apps are a difficult task because often these apps are developed by different entities, for example, government, industries or even an individual [7]. Therefore, there is an urgent need for a comprehensive or universal set of privacy regulations that app developers can use no matter where the app is developed or what type of inter/national crisis may be motivating the app development. In addition, it is equally important to assess and comply with user preferences when designing such apps with transparent data practices that are easy to understand. The design of such features would provide not only user-centered approach but would also satisfy users' needs for privacy protections when the app is collecting and processing sensitive personal data. We believe that our study provides the preliminary steps towards the development of apps that gives regard to users' preferences and expectations on privacy protection in case of using COVID-19 apps. Our initial findings can provide app developers and designers user's perspective that can be taken into consideration if we aim to increase adoption of such apps.

5 LIMITATIONS

It is important to note that our user survey was conducted in the united states while our comprehensive set of app collection were from around the world. Thus, the user's views and preferences reported in this study may not be representative of all countries and people around the world. In the United states, people are more mindful of privacy and civil liberties while people from the EU countries like Germany, Italy, Poland and China may view privacy differently and thus we may have different results in respect to users' preferences [3].

REFERENCES

[1] Hyunghoon Cho, Daphne Ippolito, and Yun William Yu. 2020. Contact tracing mobile apps for COVID-19: Privacy considerations and related trade-offs. *arXiv preprint arXiv:2003.11511* (2020).

[2] Joint Task Force and Transformation Initiative. 2013. Security and privacy controls for federal information systems and organizations. *NIST Special Publication* 800, 53 (2013), 8–13.

[3] Christopher Kuner. 2010. Regulation of transborder data flows under data protection and privacy law: past, present, and future. *TILT Law & Technology Working Paper* 016 (2010).

[4] Alireza Sahami Shirazi, Niels Henze, Tilman Dingler, Martin Pielot, Dominik Weber, and Albrecht Schmidt. 2014. Large-scale assessment of mobile notifications. In *Proceedings of the SIGCHI conference on Human factors in computing systems*. 3055–3064.

[5] Tanusree Sharma, John C Bambenek, and Masooda Bashir. 2020. Preserving Privacy in Cyber-physical-social Systems: An Anonymity and Access Control Approach. (2020). https://www.ideals.illinois.edu/handle/2142/106049

[6] Tanusree Sharma and Masooda Bashir. 2020. Use of apps in the COVID-19 response and the loss of privacy protection. *Nature Medicine* (2020), 1–2.

[7] Murugiah Souppaya and Karen Scarfone. 2013. Guidelines for managing the security of mobile devices in the enterprise. *NIST special publication* 800 (2013), 124.