COVID-19 Apps and Privacy Protections from Users' Perspective

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

Lin Guo
University of Illinois at Urbana-Champaign, USA
linguo4@illinois.edu

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

ABSTRACT
As the spread of the novel coronavirus (COVID-19) continues to be a global challenge, there have been numerous efforts and actions from both government and private organizations towards keeping their community members healthy and safe. One of the approaches is to use mobile apps to trace contacts and update the status of the infected individuals efficiently and conveniently so that the spread of COVID-19 can be minimized and contained. While these apps could offer many advantages, it also raises serious privacy concerns for many users and hence possibly refusing to adopt it. In this study, we aim to understand the users' expectations on the privacy protections and the provisions under which they are willing to use COVID-19 apps. We believe our study results can guide policymakers and app developers on the design, deployment, and acceptability of the COVID-19 apps that can be widely adopted.

KEYWORDS
COVID-19; Mobile Applications; Privacy Concerns, Privacy Protections.

INTRODUCTION
In December 2019, a novel coronavirus was first identified in Wuhan, China, and it quickly became a global challenge with over 10 million cases worldwide being confirmed within six months according to WHO's situation report (2020). The coronavirus disease in 2019 was further named COVID-19 by WHO, and the WHO Director General declared it as a public health emergency of international concern in January 2020 (R&D Blue Print, 2020). The COVID-19 pandemic has had serious negative consequences on individuals around the world, not only by threatening their physical health but also by changing their lifestyles and daily routines. Because of the pandemic lockdown and social distance restrictions, people are forced to start self-quarantine, gatherings are limited, and telecommuting is encouraged instead of meeting in person. Therefore, it has been critical that the governments/health organizations swiftly respond to the pandemic and assist the ones most in need.

As one of the solutions to deal with the COVID-19 pandemic, mobile technologies have been applied by governments and private organizations around the world to control infectious diseases and promote public health. Numerous mobile apps have been developed as an important tool during the outbreak to help with controlling the COVID-19 outbreak. Mainly, there are two types of COVID-19 apps: the status app, which is used to show the user's current disease status, and the contact tracing app, which is used to identify and track the ones that may be in contact with infected individuals. Traditionally, tracing of contacts is done by a public health department, which includes interviewing patients and then calling people who have come into contact with those patients. These recent COVID-19 apps could potentially offer many advantages comparing with the traditional methods. Not only that the tracing cost is much lower since the cases are automatically detected with individuals reporting their information, but it also could identify the infected individuals more efficiently and quickly considering a large number of mobile users (Rowe, 2020). Many governments from different regions have developed their official COVID-19 apps. For example, the COVIDSafe developed by the Australian Government Department of Health is an in-use contact tracing app that helps to keep the community safe during the ongoing pandemic (Cartwright, 2020). By deploying these tracing apps, the governments/organizations devote themselves to minimize the level of exposure to the COVID-19, and limiting the spread of the virus (Abbas & Michael, 2020).

However, even though these apps could help with reducing the community's vulnerability to the COVID-19 by sharing up-to-date information, using these apps may also raise serious privacy concerns for users' data. For example, a previous study found that although many of the current COVID-19 apps did not appropriately protect user's data in an anonymous, encrypted, and secured way, these apps also required or allowed different types of access to user's personal and sensitive information (Sharma & Bashir, 2020). Another case study also found that privacy protections have not been effectively addressed in most of the COVID-19 apps. For example, 60% of the apps selected didn't have explicit data retention controls, and 69% of the apps didn't provide options for users to opt-in/opt-out (Sharma et al., 2020). These privacy breaches from the apps may not only violate users' human rights but

84th Annual Meeting of the Association for Information Science & Technology | Oct. 29 – Nov. 3, 2021 | Salt Lake City, UT.

also makes individuals more concerned and hesitant to use such apps. In addition, results from a prior study indicated that the risks of privacy violations may lead to a lower willingness of individuals to install the apps (Chan & Saqib, 2021).

While privacy considerations for COVID-19 apps have been a global concern, people in the U.S. and western regions are especially demanding the need for privacy protections if they were to use such apps. For instance, according to a study conducted in June 2019, about 79% of Americans in the study said that they were concerned about how the government or the companies used their personal information (Auxier, 2020). Also, a previous research study found that the U.S. public are more willing to accept the contact tracing apps that use decentralized data storage, which preserves a higher degree of privacy, instead of the ones using centralized data storage (Zhang et al., 2020). Given the severity of the pandemic and the cost-effective and timely resolution that the mobile apps can provide in curbing the pandemic it is ever more critical that governments/policymakers, health care providers, and app developers in the U.S. and around the world understand users' need and expectation for privacy protections when it comes to their health data and sensitive information if they are to use COVID-19 apps.

In this study, we aim to understand individuals' perspectives on the privacy considerations for the COVID-19 apps in the United States. While people may be willing to use relevant apps to track new cases or monitor the COVID-19 trends, they may also be cautious about the information they share with the apps considering the amount of personal and sensitive data it involves. On the other hand, a previous survey study found that two-thirds of Americans stated their willingness to install a COVID-19 app to help with controlling the outbreak, even if such an app would collect their location data and health information (Hargittai & Redmiles, 2020). Therefore, the goal of this study is to learn the trade-off when individuals choose to use such an app: what types of privacy protections are people looking for, and what types of information do they agree to provide to the apps. Specifically, the study will identify the privacy considerations that both privacy advocates and privacy opponents expects from three aspects: information collection and sharing, implementation of privacy protections, and trust and surveillance. By studying individuals' needs of privacy protection provided by the app, results from this study could provide privacy design recommendations to policymakers and app developers so that the future development of relevant apps could be more appropriately aligned with users expectations and therefore leading to wider deployment and adoption in the future.

LITERATURE REVIEW

A variety of mobile apps have been developed during the COVID-19 pandemic, and these apps have been very helpful and have become an important part of the strategies to control the outbreak. A prior review study considered the COVID-19 apps as a valuable tool for both individuals and policymakers to overcome the challenges such as reducing the burden on hospitals, providing access to credible information, and tracking the symptoms of individuals (Kondylakis et al., 2020). However, although the new development of COVID-19 apps could potentially help with controlling the outbreak and promoting public health, previous studies also identified various privacy violations by these apps. Especially when the existing privacy law does not exactly prevent companies from developing apps that are not compliant with the data protection regulation (Newlands et al., 2020), a lot of those apps only include initial risk assessment without fully being compliant. For example, a prior research study examined the lack of privacy for a Singaporean government's contact tracing mobile app, which allowed the ministry of health to access the patient's data and track whom they have been near (Cho et al., 2020). Also, it is possible that the COVID-19 apps could be hacked because of security risks (Boutet et al., 2020), and the data collected could be vulnerable to cyberattack and misuse (Open letter, 2020).

While it is evident that users are concerned about privacy protections when it comes to mobile apps, they are particularly concerned when their data is being watched and recorded, or when they lose control over their data, and when collected information is being used for other purposes without notice (Xu et al., 2012). In addition, a recent survey study found that users in the U.S. did have privacy protection expectations when it came to COVID-19 apps even before any such apps were in use. For example, they expressed a preference for having control over their data such as being able to delete their data at any time (Sharma et al., 2020). These privacy expectations tend to be similar from different regions of the world with a research study from the UK reporting that users were worried about increased surveillance by governments, as well as personal data being accessed by third parties (Williams et al., 2020).

Nevertheless, it is also important to consider that there is various conceptualization when it comes to privacy protections and while there are those that are advocates of such protections there are others that oppose it. Thus, we aimed to understand views and expectations for privacy in COVID-19 apps from both advocates of privacy as well as those who are opposed to such protections. We believe this approach provides a balanced assessment on the importance of privacy protections in these types of apps while taking account and considering users' differing baseline views on the role of privacy in society. This additional insight can guide governments, policymakers, and app developing companies the awareness and the critical role that privacy protections plays if wider adoption of

such apps is the goal. Cho et al. (2020) argued that a strong guarantee of privacy is essential to encourage the common use of a COVID-19 contact tracing app. Tang (2020) also recommended that app developers should seek privacy-preserving contact tracing solutions to encourage potential users to install contact-tracing apps. Furthermore, since there seems to be a direct link between the public's decision of using COVID19 apps and their perception of how their health data is being protected, more effort and emphasis need to be in place for these users' expectations. It is shown that such accommodations can be made by some app developers (Ahmed et al. 2020) when they chose to implement decentralized architecture for their COVID-tracing apps over the centralized architecture in order to enhance the privacy protections on users' data. Another example is the COVID-19 app SwissCovid developed by the Swiss Federal Office of Public Health, which requires user's consent to process their data, and only keeps user's ID for 14 days as for data retention (Martin et al., 2020).

METHOD

To understand individuals' privacy perspectives towards the COVID-19 apps, we designed and sent a survey with questions related to COVID-19 experiences to 10,000 students at a midwestern university in the United States in June, 2020. Participants in this survey have a variety of backgrounds. Since we recruited the participants through university emails, majority of participants are students under 29 years old. For those who indicate their ethnicities, 56% of the participants are white, and there are also other ethnic groups (25% Asian, 9% Hispanic/Latino, and 4% Black). While the survey was designed as a comprehensive questionnaire including questions related to different fields, in this study, we only focused on analyzing participants' attitudes towards the two types of COVID-19 apps: the tracing app and the status app. The scenario of using these two apps were described as follows:

- Tracing app: The app is used to trace the contacts of people who have been diagnosed with COVID-19. The tracing app is expected to document where you've been and whom you've been close to.
- Status app: The app is used to keep track of whether the smartphone's owner has had COVID-19, whether he or she has been tested for COVID-19 and is disease-free, and other indicators of disease status, like current temperature. The status app is expected to show the user's current disease status and could be used to allow people more freedom of movement, such as going back to work and school.

Besides surveying the attitudes towards the COVID-19 apps, we also asked participants to respond on their personal view of privacy protections provided by these apps in three aspects: 1) information collection and sharing, 2) implementation of privacy protections, 3) trust and surveillance. In addition, we assessed participant's baseline views on the role of privacy protections in society and classified users as either Advocates or Opponents in order to better understand privacy expectations from a diverse point of view. After collecting and pre-processing the data, a total of 729 participants who fully completed the survey were selected. We conducted descriptive statistical analysis on the collected data based on participants'' privacy preferences, and also analyzed their inclination on the privacy protections for the two applications. The following section presents our results in two parts: participants' willingness to use the two apps, and their privacy concerns towards the COVID-19 apps.

RESULTS

Willingness to Use the App

Tracing App

As shown in Table 1, 62% of the participants are willing to use the tracing app. For those participants who chose "Maybe", many of them exhibit privacy as the major concern. Also, 79% of the participants care about the provider of the tracing app. From their preferences, the CDC ranks the highest, followed by the university and WHO. In other words, they are more comfortable to use the app if it is provided by health-related authorities or the university.

Selected Survey Question	Participants Response
Would you be willing to use an tracing app?	
• Yes, I would be willing to use the COVID-19 tracing app.	455 (62%)
• No, I would prefer the traditional approach to tracing	153 (21%)
• Maybe.	121 (17%)
If such an app were available for use, would it matter to you who offered the app and controlled your data?	
• Yes, it would matter to me who offered the app and who had access to my data.	574 (79%)
• No, I'd use the tracing app regardless of who offered it.	106 (15%)
• Maybe.	49 (7%)
Which one of the following options would you prefer (to be the provider of the app)?	
• CDC or any health center	379 (52%)
• My university	306 (42%)
• World Health Organization (WHO)	286 (39%)
• Government	69 (9%)
• My employer	49 (7%)
• Private company	33 (5%)
• Other	32 (4%)

Table 1. Willingness to use a tracing app

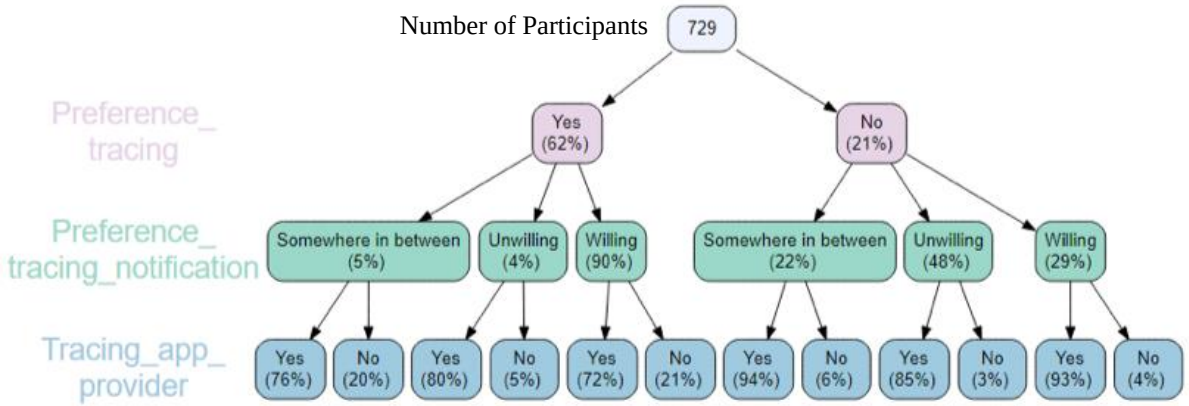

Figure 1. Tree plot (Top: Willingness to use the tracing app; Middle: Willingness to be noticed their contact with COVID-19 cases; Bottom: If who offers the tracing app matters)

From the tree plot in Figure 1, we find that 90% of those who express willingness to use the app, are also willing to receive notifications about contact with COVID-19 cases. In addition, the app provider generally matters more for those who chose unwilling to use the app, implying that these participants are more concerned about their private information and tend to choose the app more carefully based on the provider.

Status App

Similar to the tracing app, as shown in Table 2, 69% of the participants would like to use the status app. Also, for those who chose the answer "Maybe", many of them express their concerns on data safety and privacy. 77% of the participants believed that who offers the app matters. Similar to the tracing app, the medical provider and the university are more trustworthy as the app providers.

Selected Survey Question	Participants Response
Would you be willing to use a status app?	
• Yes, I would be willing to use the COVID-19 status app.	464 (64%)
• No.	101 (14%)
• Maybe.	164 (22%)
If such an app were available for use, would it matter to you who offered the app and controlled your data?	
• Yes, it would matter to me who offered the app and who had access to my data.	566 (78%)
• No, I'd use the status app regardless of who offered it.	118 (16%)
• Maybe.	45 (6%)

Table 2. Willingness to use a status app

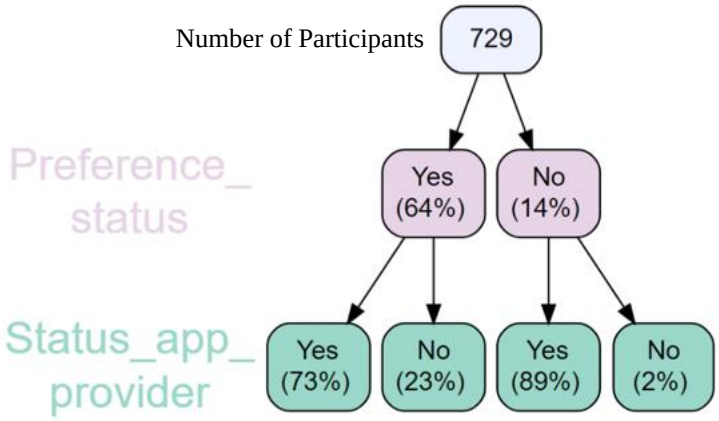

Figure 2. Tree plot (Top: Willingness to use Status APP; Bottom: If who offers Status APP matter)

Also similar to the tracing app, the tree plot shown in Figure 2 could tell that the provider of the status app generally matters more for those who chose unwilling to use the app.

Privacy Concerns

In general, when participants being asked which is more important for the app, 61% of them (444 participants) chose both Privacy and Safety as the important factors of the app. Comparing the two factors, the Safety of the app (21%) got more attention than the Privacy of the app (17%). Further analysis revealed that those who felt like both safety and privacy are important also showed their concerns on the provider of the status app (as shown in Figure 3). The results also found that if the participant cares about the provider of one of the apps, they are likely to care about provider of the other one as well.

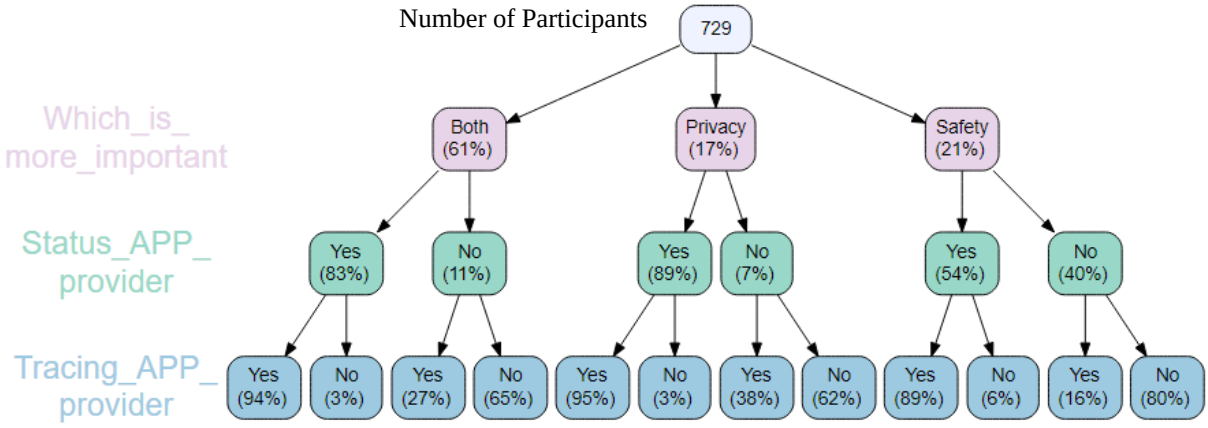

Figure 3. Tree plot (Top: Which is more important for the APP; Middle: If who offers Status APP matter; Bottom: If who offers Tracing APP matter)

To understand if individuals' view of privacy relate to their privacy concerns towards the COVID-19 apps, we divided the participants into two groups based on their answers on the view of privacy: privacy advocate (people who view privacy as a human right, civil liberty, constitutional right, or people's right to make themselves inaccessible to others) and privacy opponent (people who view privacy as negative freedom within society, a mechanism that allows people to keep unfavorable information secretly, or believe privacy invasion on individuals is necessary to ensure national security). After collecting the answers, there are 603 participants in the privacy advocate group and 112 participants in the privacy opponent group.

Information Collection and Sharing

Table 3 shows the types of information that participants are comfortable or uncomfortable to share with the COVID-19 apps. We found that the location (60%), personal information such as name (54%), health information (52%), and phone number (42%) are the types of information that participants felt most comfortable to share with the apps. Meanwhile, we also recorded the types of information that participants are uncomfortable to reveal. For example, about 83% of the participants are not willing to share their browsing history, and 80% of them do not want to give the app access to their photos.

For the two different groups, we found that participants in the privacy advocate group are more reserved on sharing sensitive data with the COVID-19 apps, and they may feel more uncomfortable sharing personal information such as browsing history, photos, phone information, and location, comparing with the privacy opponent group.

Selected Survey Question	**Overall Responses**	**Privacy Advocate**	**Privacy Opponent**
What type of information are you **comfortable** to share?			
• Your location	434 (60%)	339 (56.2%)	88 (78.6%)
• Personal information such as name	395 (54%)	320 (53.1%)	67 (59.8%)
• Health information	376 (52%)	308 (51.1%)	62 (55.4%)
• Phone number	303 (42%)	234 (38.8%)	61 (54.5%)
• Your contacts	119 (16%)	82 (13.6%)	35 (31.3%)
• Bluetooth	94 (13%)	73 (12.1%)	21 (18.8%)
What type of information are you **uncomfortable** to share?			
• Browsing history	604 (83%)	512 (84.9%)	83 (74.1%)
• Photos	586 (80%)	495 (82.1%)	81 (72.3%)
• Contacts	468 (64%)	406 (67.3%)	57 (50.9%)
• Machine address	373 (51%)	327 (54.2%)	41 (36.6%)
• Device's operating system	309 (42%)	268 (44.4%)	37 (33.0%)
• Screen size	268 (37%)	232 (38.5%)	34 (30.4%)
• Geographical location	232 (32%)	210 (34.8%)	19 (17.0%)
• Email address	208 (29%)	183 (30.3%)	24 (31.4%)
• Username	158 (22%)	139 (23.1%)	18 (16.1%)

Table 3. Attitude on types of information shared with the app

Implementation of Privacy Protections

Table 4 presents participants' preferences on the implementation of privacy protections by the app. As the results showed, over half of the participants (62%) believe that all the privacy protections listed in the survey is necessary for the COVID-19 apps. Among all the choices, participants value the protection of sensitive information more over the others. In addition, participants in the privacy advocate group demand more privacy protections than the privacy opponent group (more of them choose all the protections as their preference instead of a single answer).

Selected Survey Question	Overall Responses	Privacy Advocate	Privacy Opponent
What's your preference on the privacy protections provided by the app?			
• All of them	453 (62%)	398 (66%)	46 (41.1%)
• Protect sensitive information	138 (19%)	98 (16.3%)	38 (33.9%)
• Preventing unauthorized functionality	78 (11%)	58 (9.6%)	18 (16.1%)
• Limit permissions	36 (5%)	30 (5%)	6 (5.4%)
• Regulate mobile app data collection	24 (3%)	19 (3.2%)	4 (3.6%)

Table 4. Preferences on privacy protections

Trust and Surveillance

Table 5 shows the different app providers that participants trust to protect their privacy. The top two ranked providers are participants' medical providers (29%) and the university (28%). It is noticeable that the federal government and the state government are only trusted by 6% and 5% of the participants accordingly. From the results, we also found that the privacy opponent group is more likely to build trust with any of the app providers (only 4.5% of them choose not to trust anyone to protect their data privacy, comparing to the 10.9% for the privacy advocate group).

Selected Survey Question	Overall Responses	Privacy Advocate	Privacy Opponent
If such a COVID-19 app were offered, who would you trust most to protect your privacy?			
• My medical provider	210 (29%)	187 (31%)	20 (17.9%)
• My university	204 (28%)	165 (27.4%)	36 (32.1%)
• I would not trust anyone to protect my data privacy	73 (10%)	66 (10.9%)	5 (4.5%)
• A non-profit organization	67 (9%)	58 (9.6%)	8 (7.1%)
• Privacy company (e.g. Google, Apple)	46 (6%)	31 (5.1%)	15 (13.4%)
• Federal government	41 (6%)	32 (5.3%)	9 (8%)
• State government	38 (5%)	26 (4.3%)	9 (8%)
• My health insurer	34 (5%)	24 (4%)	8 (7.1%)
• My employer	16 (2%)	14 (2.3%)	2 (1.8%)

Table 5. Trust on app providers

The participants' attitudes towards tracking of their information are shown in Table 6. While a lot of the participants (63%) felt acceptable if the government is tracking the location of COVID-19 cases, a larger number of them are not comfortable if everyone using the app is under the surveillance of the app providers. Similar to the previous results, people who view privacy as an important right (privacy advocate group) are more against the tracking on location of COVID-19 cases or individuals, while people who view privacy negatively (privacy opponent group) are more supportive on tracking from the government.

Selected Survey Question	Overall Responses	Privacy Advocate	Privacy Opponent
Is government tracking on location of COVID-19 cases acceptable?			
• Very acceptable	203 (28%)	142 (23.5%)	56 (50%)
• Somewhat acceptable	253 (35%)	214 (35.5%)	36 (32.1%)
• Not sure	97 (13%)	84 (13.9%)	11 (9.8%)
• Somewhat unacceptable	76 (10%)	69 (11.4%)	4 (3.6%)
• Very unacceptable	100 (14%)	94 (15.6%)	5 (4.5%)
Is government tracking for everyone acceptable?			
• Very acceptable	31 (4%)	21 (3.5%)	9 (8%)
• Somewhat acceptable	82 (11%)	56 (9.3%)	26 (23.2%)
• Not sure	110 (15%)	83 (13.8%)	24 (21.4%)
• Somewhat unacceptable	167 (23%)	133 (22.1%)	32 (28.6%)
• Very unacceptable	339 (47%)	310 (51.4%)	21 (18.8%)

Table 6. Attitudes on information tracking by the apps

DISCUSSION

In this research study, we found that most users are willing to use COVID19 status and tracing apps if certain privacy and security protections are designed and implemented. For example, over half of the participants view both safety and privacy as an important factor of the COVID-19 apps while knowing that they need to provide their personal and sensitive information to the apps while using it. In addition, users are more willing to use tracing and status apps to help with contact tracing if the apps had privacy protections. About 78% of participants who viewed safety and privacy as important factors agreed to use both the status app and tracing app. Based on the results from this study, policymakers and app developers need to take privacy protections more seriously and make those features more explicit if their goal is to encourage more users to adopt the COVID-19 apps.

If we are to address users' privacy concerns and place appropriate protections in order to satisfy users' needs, it is important to understand users' expectations for privacy protections and provide the protections in the COVID-19 apps to increase the usage. According to many survey results, most participants are reserved on providing their sensitive information to the COVID-19 apps, while only a small percentage are open to give their health and personal data to the app. For example, only 16% of our study participants feel comfortable in share their contacts. In addition, participants worry about the level of surveillance and lack trust in certain entities that may provide the COVID-19 app. In our survey, 70% of participants reported that it was unacceptable if the government is tracking everyone, instead, they are more comfortable if the app only tracks users' locations (73% rated acceptable). Also, participants tend to have more trust towards some entities that they are more familiar with instead of the governments. Since the survey was sent to college students, about one-third of our participants chose the University as the one entity that they would trust the most to protect their privacy. These results imply that policymakers still need to consider trust with individuals as an important factor when asking them to use relevant apps.

The study also found that most participants prefer and expects privacy protections for COVID-19 apps regardless of whether they are Advocates or Opponents of privacy protections in general. While privacy advocate participants are more reserved to share their personal and sensitive information with the COVID-19 apps, they still demand more comprehensive privacy protections from the apps and are less likely to trust the app providers to protect their information. In contrast, privacy opponent participants who view privacy as negative freedom or believe privacy invasion is necessary report being more acceptable of a government tracking location or personal information during the COVID-19 pandemic. Nonetheless, the results of this study shows that while there are differing views on the role of privacy protections in society when it comes to COVID-19 apps privacy protections are critical to users adoption of such apps and therefore app providers and designers are encouraged to implement comprehensive privacy protections and make it explicit in order to satisfy users' needs.

Furthermore, the above findings regarding users' privacy protection expectations even when accounting for their baseline views regarding privacy in general reveals another vital aspect that needs further examination. This aspect is considering privacy expectations from an underrepresented population. Previous research shows that under-represented minority individuals distrust such collection of information and worry about how that information may be used to discriminate or exclude them in some way (Ringelheim, 2008). For example, a previous report revealed that ethnic minority groups are at higher risk of oversurveillance after protests (Privacy International, 2020). Because of the possible risks of privacy violations and discriminations, minority groups might seek more privacy protections and be more careful about sharing their information. As shown by our study results, participants from minority groups such as the Hispanic/Latino participants are more concerned about providing their personal information with COVID-19 apps comparing with White participants, especially when it comes to sharing their health information (61% for Hispanic/Latino, 48.8% for White) and phone number (47.5% for Hispanic/Latino, 40.5% for White). Therefore, it is critical to consider all of these individual differences when designing relevant apps in order to minimize the risk of discrimination and mistrust.

LIMITATIONS

While our study only recruited participants from a public midwestern university, it is necessary to involve people in different age groups and with different backgrounds to have a more comprehensive understanding of individuals' privacy concerns in future studies. Also, since the survey was conducted and sent out during the early stage of the COVID-19 outbreak (July 2020), the results are mostly a reflection of participants' expectations of the COVID-19 apps in the first six months of the pandemic and their perspectives may have changed after they have used the apps.

CONCLUSION

In conclusion, our study results show that while many people are willing to use COVID-19 status and tracing apps, they also have concerns about the information that is being collected and expect appropriate privacy protections for the use of their personal and health data. We believe these findings are essential when designing, developing, and deploying pandemic-related apps. If users' expectations are met, then adoption of technology often increases and

since the ultimate goal is to have more users adopt such apps in times of a health crisis, we cannot afford to ignore such expectations.

REFERENCES

Abbas, R., & Michael, K. (2020). COVID-19 contact trace app deployments: Learnings from Australia and Singapore. *IEEE Consumer Electronics Magazine*, 9(5), 65-70.

Ahmed, N., Michelin, R. A., Xue, W., Ruj, S., Malaney, R., Kanhere, S. S., Seneviratne, A., Hu, W., Janicke, H., & Jha, S. K. (2020). A survey of covid-19 contact tracing apps. *IEEE Access*, *8*, 134577-134601.

Auxier, B. (2020). How Americans see digital privacy issues amid the COVID-19 outbreak. In Pew Research Center. Retrieved from (https://www.pewresearch.org/fact-tank/2020/05/04/how-americans-see-digital-privacy-issues-amid-the-covid-19-outbreak/).

Boutet, A., Bielova, N., Castelluccia, C., Cunche, M., Lauradoux, C., Le Métayer, D., & Roca, V. (2020). *Proximity tracing approaches-comparative impact analysis* (Doctoral dissertation, INRIA Grenoble-Rhone-Alpes).

Cartwright, J. (2020). The Government's COVID-19 tracking app is called CovidSafe and is launching today. In techAU. Retrieved from (https://techau.com.au/the-governments-covid-19-tracking-app-is-called-covidsafe-and-is-launching-today/).

Chan, E. Y., & Saqib, N. U. (2021). Privacy concerns can explain unwillingness to download and use contact tracing apps when COVID-19 concerns are high. *Computers in Human Behavior, 119*, 106718.

Cho, H., Ippolito, D., & Yu, Y. W. (2020). Contact tracing mobile apps for COVID-19: Privacy considerations and related trade-offs. *arXiv preprint arXiv:2003.11511*.

Fife, E., & Orjuela, J. (2012). The privacy calculus: Mobile apps and user perceptions of privacy and security. *International Journal of Engineering Business Management*, *4*(Godište 2012), 4-11.

Hargittai, E., & Redmiles, E. (2020). Will Americans Be Willing to Install COVID-19 Tracking Apps? In Scientific American. Retrieved from (https://blogs.scientificamerican.com/observations/will-americans-be-willing-to-install-covid-19-tracking-apps/).

Martin, T., Karopoulos, G., Hernández-Ramos, J. L., Kambourakis, G., & Nai Fovino, I. (2020). Demystifying COVID-19 digital contact tracing: A survey on frameworks and mobile apps. *Wireless Communications and Mobile Computing*, *2020*.

Newlands, G., Lutz, C., Tamò-Larrieux, A., Villaronga, E. F., Harasgama, R., & Scheitlin, G. (2020). Innovation under pressure: Implications for data privacy during the Covid-19 pandemic. *Big Data & Society*, *7*(2), 2053951720976680.

Open letter. (2020). Joint statement on contact tracing. Retrieved from (https://drive.google.com/file/d/1OQg2dxPu-x-RZzETlpV3lFa259Nrpk1J/view).

Privacy International. (2020). Ethnic minorities at greater risk of oversurveillance after protests. Retrieved from (https://privacyinternational.org/news-analysis/3926/ethnic-minorities-greater-risk-oversurveillance-after-protests).

R&D Blue Print. (2020). COVID-19 Public Health Emergency of International Concern (PHEIC) Global research and innovation forum: Towards a research roadmap. In World Health Organization. Retrieved from (https://www.who.int/publications/m/item/covid-19-public-health-emergency-of-international-concern-(pheic)-global-research-and-innovation-forum).

Ringelheim, J. (2008). Minority protection, data collection and the right to privacy. *European Yearbook of Minority Issues Online*, *6*(1), 51-77.

Rowe, F. (2020). Contact tracing apps and values dilemmas: A privacy paradox in a neo-liberal world. *International Journal of Information Management*, *55*, 102178.

Sharma, T., & Bashir, M. (2020). Use of apps in the COVID-19 response and the loss of privacy protection. *Nature Medicine*, 26(8), 1165-1167.

Sharma, T., Wang, T., & Bashir, M. (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).* Association for Computing Machinery, New York, NY, USA, Article 22, 1–4.

Situation Report – 162. (2020). In World Health Organization. Retrieved from (https://www.who.int/docs/default-source/coronaviruse/20200630-covid-19-sitrep-162.pdf?sfvrsn=e00a5466_2).

Tang, Q. (2020). Privacy-preserving contact tracing: current solutions and open questions. *arXiv preprint arXiv:2004.06818*.

Williams, S. N., Armitage, C. J., Tampe, T., & Dienes, K. (2020). Public attitudes towards COVID-19 contact tracing apps: A UK-based focus group study. Health Expectations.

Xu, H., Gupta, S., Rosson, M. B., & Carroll, J. M. (2012). Measuring mobile users' concerns for information privacy.

Zhang, B., Kreps, S., McMurry, N., & McCain, R. M. (2020). Americans' perceptions of privacy and surveillance in the COVID-19 pandemic. *Plos one*, *15*(12), e0242652.