Enabling User-Centered Privacy Controls For Mobile Applications: COVID-19 Perspective

TANUSREE SHARMA, Informatics, University of Illinois at Urbana Champaign, USA
HUNTER A. DYER, Computer Science, University of Illinois at Urbana Champaign, USA
MASOODA. BASHIR, School of Information Sciences, University of Illinois at Urbana Champaign, USA

Mobile apps have transformed many aspects of clinical practice and are becoming a commonplace in healthcare settings. The recent COVID-19 pandemic has provided the opportunity for such apps to play an important role in reducing the spread of the virus. Several types of COVID-19 apps have enabled health care professionals and governments to communicate with the public regarding the pandemic spread, coronavirus awareness and self-quarantine measures. While these apps provide immense benefits for the containment of the spread, privacy and security of these digital tracing apps are at the center of public debate. To address this gap, we conducted an online survey of a midwestern region in the United State to assess people's attitudes towards such apps and to examine their privacy and security concerns and preferences. Survey results from 1550 participants indicate that privacy/security protections and trust play a vital role in people's adoption of such apps. Furthermore, results reflect users' preferences wanting to have control over their personal information and transparency on how their data is handled. In addition, personal data protection priorities selected by the participants were surprising and yet revealing of the disconnect between technologists and users. In this paper, we present our detailed survey results as well as design guidelines for app developers to develop innovative human-centered technologies that are not only functional but also respectful of social norms and protections of civil liberties. Our study examines users' preferences for COVID-19 apps and integrates important factors of trust, willingness and preferences in the context of app development. Through our research findings, we suggest mechanisms for designing inclusive apps' privacy and security measures that can be put into practice for healthcare related apps so that timely adoption is made possible.

CCS Concepts: • **Security and privacy → Privacy protections**.

Additional Key Words and Phrases: Mobile apps, Privacy & Security, Trust, human-centered, COVID-19

ACM Reference Format:
Tanusree Sharma, Hunter A. Dyer, and Masooda. Bashir. 2020. Enabling User-Centered Privacy Controls For Mobile Applications: COVID-19 Perspective. *ACM Trans. Internet Technol.* 1, 1, Article 1 (January 2020), 26 pages. https://doi.org/10.1145/3434777

1 INTRODUCTION

Advancements in Information and Communication Technologies (ICT) have made our communication capabilities and information exchange easier and more convenient than ever before. For example, in recent years, ICT innovations have dramatically changed and increased remote workforce. The recent COVID-19 pandemic has demonstrated how ICT is

Authors' addresses: Tanusree Sharma, tsharma6@illinois.edu, Informatics, University of Illinois at Urbana Champaign, USA; Hunter A. Dyer, Computer Science, University of Illinois at Urbana Champaign, USA, hadyer2@illinois.edu; Masooda. Bashir, School of Information Sciences, University of Illinois at Urbana Champaign, USA.

allowing people to work and learn remotely like never before. In particular, innovative measures and tools, such as digital contact tracing mobile apps are applied around the globe to contain the spread of the virus.

One critical aspect that is at the heart of the discussion for many researchers, citizens, and technologists all over the world is if privacy and security risks are being considered appropriately for users. For many developed countries (e.g. USA), adopting this contact tracing technology is still controversial. Researchers are attempting to pinpoint security measures and privacy protocols in order to provide a secure technological environment for users [14], [36], [29]. At the same time, recent user studies provide public opinion on contact tracing apps and privacy concerns. However, to the best of our knowledge, none of the reviewed literature [33], [19] formalize their user-based findings as privacy and security controls that users want. Therefore, in this paper we propose the critical mechanisms that consist of public opinions on privacy and security controls that can be applied in contact tracing apps' design.

Therefore, we conducted a survey (N=1550 participants) to better understand users' preferences for this type of an App and what their expectations were for privacy and security protections in such apps. While there were over 200 questions on all aspects of COVID-19 app on this survey, our analyses were focused on privacy-related questions. Subsequently, our human-centered analysis is two folded: 1) conducting descriptive and distributed statistical analysis of different privacy and security related survey questions as well as investigate linearly aligned relationship among different responses in adopting COVID-19 tracking/tracing and status apps and 2) Utilizing topic modeling algorithm to cluster users' perceptions and preferences and categorizing their direct responses (open-ended questions). Our goal was to discover users' concerns, preferences, and expectations if they were to use these COVID-19 apps. We believe this is a timely and critical step forward if we are to deploy contact tracing apps for people around the world, particularly in the United State where users are skeptical of such technologies and its privacy protections measures [1]. Prior research shows that "Privacy by Design" is one of the most recommended approaches that not only provides a comprehensive set of privacy protections, but it also allows users' values and preferences to be integrated in the development of the innovation [12]. Thus, our entire study was designed to answer the following research questions:

Who do people trust to control and provide privacy protections for their data? This question explores people's trust towards different organizations who provide pandemic- related apps. In our survey, we provided several organizations (i.e., private company, federal government, state government, local government, employer, health insurer, medical provider, public research university, private research university, non-profit organization) in order to identify people's trust level for different entities. Our research objective was to determine if human trust in technology changes depending on which entity develops it. We believe this aspect is a crucial facet when developing apps in times of national emergency like a pandemic and if the goal is to have maximum adoption of the technology.

Is data transparency an important factor in adoption decisions? We analyzed survey questions that were focused on how transparency in data handling would affect users' willingness to use COVID-19 apps during this pandemic. Our research objective was to understand if people considered transparent data handling as an important control factor and if so, can this be part of the privacy and security design strategy?

What are users' privacy protection preferences for different data types? From a prior related research project on COVID-19 [32], we found a wide range of permissions and data sharing practices that mobile devices are requiring from COVID-19 apps. In most cases, these permissions and sharing practices do not seem to be needed for specific functionality. Hence, this research question is focused on understanding participant's priority for data protection for a number of different data types and how participants' general privacy and security concerns are related to their privacy

[1]Lomas, N. TechCrunch https://techcrunch.com/2020/03/20/what-are-the-rules-wrapping-privacyduring-covid-19/ (2020).

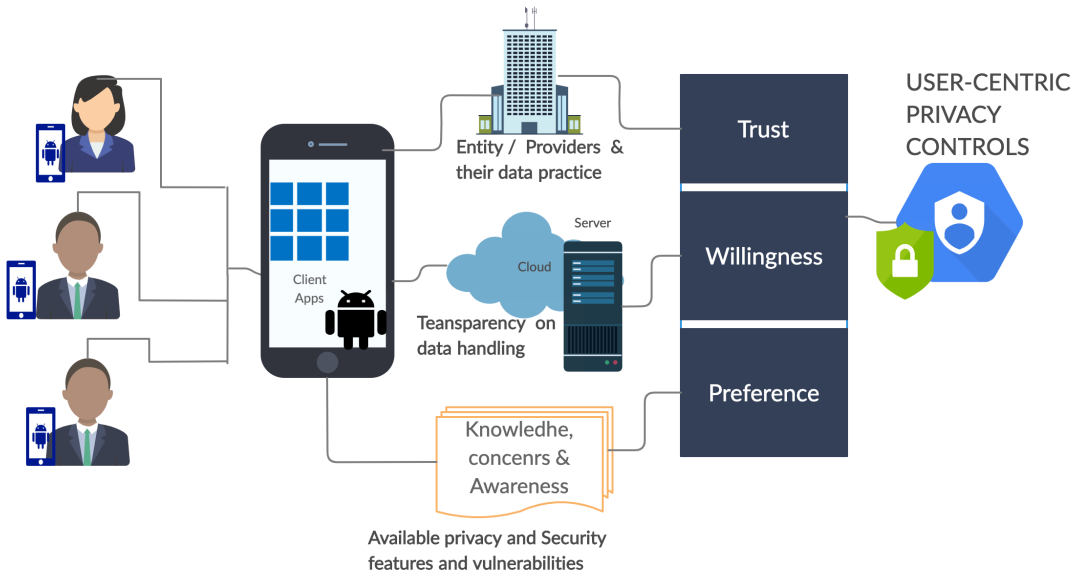


Fig. 1. Framework for Designing user-based privacy controls

protection preferences for a COVID-19 application. Our assumption is that users' priority of data type wise selection will provide us the information for privacy controls to be designed with suitable mechanisms.

Hence, we have conducted a comprehensive analysis that incorporates privacy principles and design specifications principles [9], [12] as well as user-based preferences to formalize our findings. We believe our findings can provide essential guidance for how developers and policy makers can approach privacy and security controls that are human centered for pandemic related mobile applications. Categorically, we concentrated our efforts on privacy and articulated the desired privacy controls for digital contact tracing that participants indicated. It is important to mention that we argue neither for nor against automated contact tracing in this study. Instead we offer our survey results that shows what users' expectations and preferences are when it comes to privacy/security protections in contact tracing technologies. We considered general privacy measures and principles (P_t) that are parameterized by information (I_t) which is being collected, shared, and processed by entities where users' preferences and feedback (U_t) are considered as catalysts that increases or decreases the rate of an adoption of COVID-19 apps.

2 BACKGROUND

This section briefly presents a review of recently proposed frameworks on privacy-ware digital contact tracing for COVID-19 apps as well as studies that focused on risk-associated privacy frameworks.

2.1 Prior Privacy Frameworks

Many of the privacy and security violations that plague today's online world are the result of the deficiency in system design to consider intended users' perspectives. Users' trust, willingness, and preferences to adopt a certain type of application depends on social, cultural and other individual factors [3]. Inspired by the latest Privacy framework offered by NIST [9], we propose privacy engineering controls that reinforce "Privacy by Design" concepts in mobile app development. This is particularly important when developing risk-associated technologies such as COVID-19 apps where people need to be able to trust the entity that is offering the technology, be able to understand the rules of engagement/policies (transparency) that are related to the use of that technology, and be able to obtain some level of control (preferences) of their shared information. These three (trust, transparency, preferences) factors provided us with the necessary configurations needed to structure our survey responses to identify users' perceived privacy concerns and their expected controls. The deployment of any successful technology depends on user engagement [6]. Reluctance to provide functional information due to lack of trust could potentially impede the flourishment of technologies' anticipated goals [4]. Individuals' intention of sharing information and adopting services depends on their trust on a given entity in valuing customers' preferences [16]. For example, health care industries are well-known for providing a trusted computing environment, secure multi-party computing to enable different parties to conduct computation without violating privacy and minimizing the risk of privacy violation [38]. Research on implementing formal security measures for patient's information analysis and keeping trust as a high-level component lead us to our first component (Trust) to be studied from the survey responses. Studies on implementing Privacy Enabling Transparent Systems (PETS) for health care data application [28], [30] and formal privacy design for remote health care's purpose-based transparent data transmission and analysis [13] provided us the motivation for our second component (Transparency) to be studied. Finally, studies focusing on determining the gap between users' preferences and design limitation [31], [5] laid out the motivation for our third component (Preferences) to be studied. Analysis of these three factors can be helpful to identify the privacy features/controls that users wanted to have for COVID-19 apps.

2.2 Recently Proposed Frameworks for COVID-19 Apps

Technology companies, academics, and governments are rapidly working to develop and deploy contact tracing apps to track and mitigate the spread of COVID-19. Prior work has determined that contact tracing apps will be most effective when used by the majority of a population [37]. However, some have raised security and privacy concerns [17] as well as broader concerns about efficacy [32]. Our research seeks to provide insight into people's perspectives on privacy values, concerns, and opinions on the use of proposed contact tracing technologies to combat COVID-19. Our findings can guide the design and development of privacy/security inclusive schemes for contact tracing. Recent studies of COVID-19 apps suggest that minimizing privacy risks based on users' feedback would be an appropriate design component [19]. Meanwhile, in the U.S., there is currently a heated public debate on the benefits of such technology-based contact tracing and the risk to individual privacy, [18] which makes our study timely and vital. Here in our study, we are not arguing against contact tracing technology. Instead, we offer the main mechanisms that our survey results reveal to be the essential privacy/security protections that our participants seek in contact tracing technologies. Developers and policy makers can use these findings to design privacy controls and features in these apps that are human-centered.

Table 1. Evaluating Recent COVID-19 Studies from a Privacy-By-Design Angle

Related Work	Study Type	Contribution	Privacy by Design Concept
Cho et.al [15]	Proposed	Security mechanisms with construction of token in Bluetooth contact tracing using private messaging systems	No
DP-3T [36]	Proposed	Design and implementation of decentralized proximity tracing system	Yes. Discussed
CovidWatch [23]	Implemented as proof of concept	Anonymous, decentralized, local bluetooth signals for exposure notification	No
CoEpi [2]	Implemented	anonymous Bluetooth proximity-based exposure alerting based on voluntary symptom sharing	No
CAUDHT [10]	Proposed	distributed hash table to build a decentral messaging system for infected patients and their contacts; to ensure that messages about infections are authentic and unchanged, they used blind signature	No
Liu et. al. [22]	Implemented in Android	formal security model: zero knowledge proving techniques to ensure the privacy is well-preserved and false positive is removed	No
PACT [14]	Proposed	Focused on privacy, security and re-identification risks	No
Simko et. al. [33]	Analysis	User-based study to understand opinion and preference of COVID-19 apps	No

We conducted this recent literature review in Table 1 of recently proposed privacy aware contact tracing architecture in response to the OVID-19 pandemic. Our purpose is to find out current COVID-19 technology's contribution from a design aspect and if those have considered human-centered approaches in their security and privacy measures. Most of the aforementioned framework proposed security mechanisms for either construction of bluetooth tokens for secure contact tracing or an anonymized and decentralized system for exposure notification and security protocols to minimize different types of attacks. As it can be seen in the above table, there is only one study that addressed privacy by design concept.

2.3 Recently Developed COVID-19 Apps and Design Shortcomings

To respond to the COVID-19 pandemic, there has been a surge of apps for different purposes, including contact tracing and information/health assessment. Since many of these apps are developed in a short time, around the world under emergency situations, several of them lack sufficient privacy and security protections. While this is understandable in the midst of COVID-19 crisis, as security and privacy researchers we must evaluate and address these basic privacy vulnerabilities and the risks they may pose to users' personal information. One recent research study analyzed Singapore's OpenTrace app and its use of Google firebase services to manage user data and deployment of reversible encryption and found that such methods can be vulnerable to secret key disclosure [21]. This type of privacy vulnerability can be avoided by decentralizing data management approach if privacy consideration is made by the design stage. In addition, NIST's Common Vulnerabilities and exposures (CVE) report indicated that COVIDSafe (Australia) app 1.0 and 1.1 for iOS allows a remote attacker to crash the app, and consequently interfere with COVID-19 contact tracing via a Bluetooth advertisement containing manufacturer data that is too short. Research shows that this type of attack can occur when an erroneous OpenTrace manuData.subdata call is made. Apps such as The ABTraceTogether (Alberta), ProteGO (Poland), and TraceTogether (Singapore) were also affected by this type of vulnerability [3]. Again, most of these security violations of users' data can be avoided if developers consider privacy and security protections in their initial design and development process.

3 METHOD

The online survey is conducted by Center for Social and Behavioral Science (CSBS) at University of Illinois at Urbana Champaign to assess attitudes toward using COVID-19 apps and the factors that might contribute to either positive or negative attitudes towards these technologies. The online survey of COVID-19 was conducted between May 7 to May 11, 2020. Participants recruited for this survey were from a midwestern state in the United States and they were all adults above the age of 18. The survey link was distributed through REDcap survey platform and the survey data was collected by Dynata, LLC. It should be noted that REDCap is HIPAA compliant and the survey proposal was approved by the Institutional Review Board (IRB).

There were several sections (total of 211 questions) in this survey, such as COVID-19 related health questions, economic questions such as income and food security as well as app related privacy questions. For this study, we focused our analysis on only 3 sections that were directly related to data privacy which included Trace/Track Apps Section; Passport App Section, Tech Survey Section. While a tracing and tracking app is a COVID Technology that is used to keep track of where app users have been and who they have been close to, Passport app is another COVID-19 Technology that keeps track of diseases status. One last section that we focused on is the Tech survey section which includes users' privacy expectations and concerns within COVID-19 technologies/apps. In this survey, participants were asked to answer questions about different factors that motivates and resist them to use COVID-19 apps which in turn is utilized to assess their trust, willingness and preferences in using COVID-19 apps. The online survey included several different types of questions (listed in Appendix A.1). While selecting survey responses, we eliminated participants that did not complete the survey which resulted in our final sample (N) of approximately 1550. It should be noted that the survey questions that focused on privacy protections were developed by the researchers in the context of COVID-19 pandemic and were mostly exploratory in nature due to the lack of standardized privacy protection questionnaires for such situations. Thus, the questions may lack validity and reliability and further research needs to be conducted

[3] CVE-2020-12717, National Vulnerability Database. https://cve.mitre.org/cgibin/ cvename.cgi?name=CVE-2020-12717

to obtain such outcomes. However, while designing the questionnaire, previous literature on user-centric privacy co-design study on different applications, such as, IoT and smart home devices have been taken into consideration [7], [26].

3.1 Strategy for the current study

Selecting questions for analyses: we selected questions that were related to trust, privacy and security for our analysis. Since our first component was Trust, we chose questions that were related to this topic. For a complete list of questions related to this topic that were used in our analysis, please see Appendix A 1, but to provide an example, please see the question below.

"Q1.1: If such an app (tracing/tracking) were available for use, would it matter to you who offered the app and controlled your data"

Preliminary Analysis:

Step1: Our analysis was two-fold. First, we independently analyzed each selected question to measure frequency of responses for those questions. After these distributed statistics, we analyzed a few responses as predictor variables in respect to some other question as response variable to determine if they have any significant relationship between them.

Step2: In addition, we categorized users' direct responses to open-ended questions using topic modeling algorithms. Specifically, we used latent Dirichlet allocation (LDA) to cluster users' preferences and choice in order to assess the overarching themes within each question's response. Our analyzed open-ended questions are also recorded in Appendix in A.1.

Our preliminary goal was to gain insight from the users-study to (1) identify privacy and security controls that users want/prefer when it comes to COVID-19 apps, and (2) to determine what factors are important in their adoption decision. In the sections below we provide the details of the descriptive analysis for analyzing responses so it can be used as illustration of possible privacy controls, examining users' trust, and identifying their willingness and preferences. We have supplemented necessary details of our data that we had analyzed in our Appendix section.

3.2 Strategy Data Description and Raw Percentage

3.2.1 Sample Demographics. The survey responses included 1550 participants. The participants included 49.9.% female, 49.2% male, 0.3% nonbinary, 0.2% preferred to self- describe, and 0.3% preferred not to answer. Our sample participant's age ranged from 18-90 years old: 18-25 years old (16%), 26-35 years (18.72%), 36-45 years old (18.14%), 46-55 years old (16.8%) and so on. The age groups are quite distributed and reported in table 7 in appendix. The ethnic background for our participants were White/European-American (68.3%) followed by Black/African-American (13.3%), Latino/Latina (6.7%), Asian (4.7%), biracial (4.8%), Pacific Islander/Native Hawaiian (.5%), Native American/Alaskan Native (.5%), self-described (.7%), and participants who preferred not to answer (.7%).

3.2.2 Questions/Responses Selected from the Survey for Trust and Transparency. As described above, the survey included several sections that were focused on particular technologies innovations related to COVID-19. For our study, we focused our analysis on questions that were focused on trust, and privacy/security transparency in the section of the survey that covered "Track and Trace App" as well as questions that were in the "Passport App" section of the survey. For a complete list of questions that were analyzed in our study see Appendix A.1. As it can be seen in the appendix, many of the questions in these two sections were identical, but each section directed survey participants to consider a

particular type of app (namely track and trace or Passport) when providing responses. Here is an example of a likert scale question that was included in both sections of the survey.

"Q1.3: If you could be guaranteed that you could completely delete all of your data from this tracking/tracing app at any time, would that make you more likely to use it?"

The question above, and other questions related to this topic, were selected in order to determine users' motivations towards installing those apps based on transparency and data handling as well as which entities they trust to control their data. Our objectives were to pin down likelihood of installing apps based on who controls their data and how data will be retained. All the other section questions are included in Appendix A. 1.

3.2.3 Questions/Responses Selected from the Survey for privacy/security preferences. We selected responses to questions that inquired about users' preferences for privacy/security features when using a COVID-19 mobile app as well as questions that assessed their general privacy and security concerns. Our objective was to understand the frequency of users' concerns for certain types of data and which data they are reluctant to share. Responses to these questions indicate that participants were concerned about their overall privacy when it relates mobile apps usage while they were particularly concerned about their security when it comes to COVID-19 apps. Here are two examples of questions that we asked about general privacy concerns and security concerns for COVID-19 apps.

"Q3.1 In general, how concerned are you regarding your privacy on Mobile Apps these days?

Q3.2: Are you concerned about security vulnerabilities (getting hacked by malicious actors) when using COVID19 mobile apps?"

In addition, we selected questions from the survey that requested participants' data protection preferences for different types of information that COVID-19 apps collect. Here is an example of a question that we asked about participant's choice of data types that they don't want apps to collect.

"Q 3.3: Mobile Apps often collect information for them to function. Please indicate if you do not want a COVID19 App collecting any of the following information (Please check all that apply). (options included =email address, contacts, photos, machine address, browsing history, geographical location, none of these, I don't know)"

As you can see the options provided in the question above included most or common data types that are often accessed by apps. Furthermore, we wanted to examine if participants were already using any kind of COVID-19 related apps and any other insight that we can gain from those apps that are already being adopted. For our participant sample, 14.9% had used Fitness and healthy living apps, 7.5% had used Pandemic Tracking app, 13.2% population from our sample used COVID-19 Information App provided by CDC, WHO, FEMA, 6% used Symptom/health Tracker app, 6.7% used Screening apps, 9.9% used some other types of technologies for COVID-19 pandemic. We have seen that people are already using some kind of pandemic tracking app in the USA and most of the population are using COVID-19 Information app provided by CDC, WHO, FEMA and regular used Fitness and healthy living apps. The possible reason might be trust and privacy concerns that our sample population have in the context of the United States where there is still much debate in adopting contact tracing apps for COVID-19 incident response.

Moreover, for our study we included questions/responses that indicated participants' agreement/ disagreement for COVID-19 mobile apps' privacy protections. Survey Participants were requested to provide their dis/agreement to the following likert scale question:

"Q3.5: Please indicate your agreement/disagreement with the following statements

1. COVID-19 Mobile Apps should be regulated for privacy protections.

2. We should not use mobile Apps to track US citizens because of COVID19.

Table 2. Distribution of responses for Q3.5

Statements	mean	Sd
COVID-19 Mobile Apps should be regulated for privacy protections	4.03	1.149
We should not use mobile Apps to track US citizens because of COVID19	3.15	1.252
I think Mobile Tracking Apps are a great way to end the pandemic.	2.99	1.237

3. I think Mobile Tracking Apps are a great way to end the pandemic. "

In addition, we also analyzed questions/responses that participants provided for the following two questions to better understand people's personal motivations for wanting to adopt these types of an app.

"Q3.6: COVID-19 has impacted everyone in unique ways. What reasons, if any, do you think are the most compelling for why you might personally utilize a track-and-trace app?

Q3.7: I would be okay providing personal information to a COVID19 related App if.."

Finally, we analyzed responses from open-ended questions (recorded in Appendix A.1 Q4.1-Q4.7) to get a deeper understanding of participants' concerns for privacy and security as it relates to COVID-19 tracking/tracing and status apps. Open-ended questions are a great source for getting authentic feedback in users' own voice. It is also an excellent opportunity to empathize with the audience and make the right decisions on suggesting privacy controls in our case.

4 FINDINGS

In this paper, we present descriptive and distributed statistical analysis results for the close ended questions. We also present the significance of the relationship between users' perception, concerns, and trust with COVID-19 technology adoption decision of surveyed participants. From our initial descriptive results, we decided to use linear and logistic regression on particular relationships among variables in our data since our focus was to understand the significance level of those relationships and if they satisfy or void the hypothesis. Furthermore, we have utilized LDA which is a supervised learning method to categorize open ended responses into our hypothesized overarching themes (trust, concerns, transparency, perceptions).While there are many other ML methods and approaches could analyze this data, we believe this particular method is a best-fitted strategy when dealing with such an exploratory and qualitative data analysis. Furthermore, our open-ended question includes a mixture of topics from users' direct feedback within a given question belonging to several topics and so, each question can be represented as a vector of proportions that denote what fraction of the words belong to each topic [8]. This made the determination of topic generation flexible due to LDA's reliance on knowing the number of topics as input and chosen number of topics for each question by testing the values in the range of 2 to 15, inclusive.

4.1 Trusted Parties for Privacy Protections

For tracking and tracing apps, the results for users' trust on a particular entity to control their data was answered with the five-point Likert scale from 1 to 5. We found people have the highest trust (mean 3.32) in medical providers followed by health insurers (mean 3.08), private companies (mean 2.90), public research universities (mean 2.89), private research universities (mean 2.85), employers(2.83), non-profit organizations (mean 2.80), local governments (2.75), state governments (2.71), federal governments (mean 2.61). The visualization for trust distribution in tracking apps are on the left side of Figure 2. Elaboration of x axis are for different entity: p: Private company (e.g., Google, Apple) fg: Federal

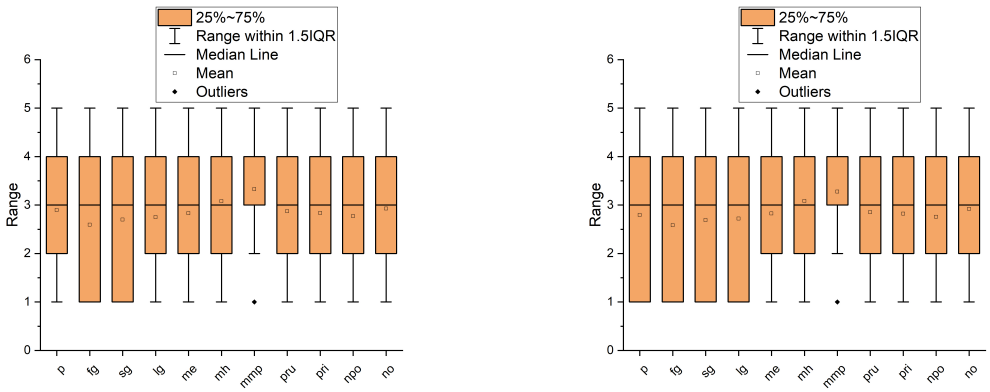


Fig. 2. Who do people trust to protect their privacy?

government sg: State government lg: Local government me: My employer mh: My health insurer mmp: My medical provider pru: A public research university pri: A private research university npo: A non-profit organization (e.g., United Way) no: I would not trust anyone to protect my data privacy.

For Status app, the results for users' trust on a particular entity to control their data was answered with the 5-point Likert scale from 1 to 5. Similar to tracking/tracing apps, our observation was quite consistent. We found that people have higher trust (mean 3.29) in medical providers followed by health insurer (mean 3.09), public research university (mean 2.87), private research university (mean 2.84), employer (2.83), private company (mean 2.80), non-profit organization (mean 2.77), local government (2.73), state government (2.71) and the least trust in Federal Government (mean 2.61).

We also analyzed several questions with linear regression to indicate if they shared significant relationships and dependency. For Status apps, users' trust in particular entities in providing COVID-19 apps (responses for Q1.1 Appendix) is related to general security concerns (responses for Q3.2 in Appendix) with positive trends. Concerns on who offered the app and controlled their data is significantly correlated with collective security concerns of participants where p-value is 2.2e-16 whereas for tracing app, this trend was consistent and indicates similar positive relation where p-value is 3.73e-13. From these results, we inferred that users who have concerns about security vulnerabilities are more likely to have concerns about who offered the app and controlled their data in case of COVID-19 app usage. As stated in the introduction, considering this positive relationship of users' trust with technology adoption and privacy preference, publishers of the apps should consider having validation and approval from the trusted entities, for example, in our analysis they are medical provider, university researchers. Therefore, even if the app is developed by the state government, they can choose to go through an approval process by the trusted entities preferred by users and developers of apps can choose to explicitly use this validation information on apps.

4.2 Importance of Data Transparency

For track and tracing apps, participant responses to question Q1.3, revealed that the majority (65%) of the participants would prefer to have some level of control over their data and transparency for the apps data practices. It is likely that control over their data and a retention policy will lead users to adoption of these apps. However, 34.7% of our

participants indicated that control over their data would not change their likelihood to adopt an app. What we found interesting is the difference in participants' preferences when it comes to different kinds of apps. In our case, participants were more likely to want control in tracing apps as compared to status apps. For Status app, responses to Q2.3 were very similar to tracing/tack app results above. Most participants (62.9%) preferred to have disclosure on data handling and a deletion policy while 36.5% of the participants reported that having control would not change anything on their likelihood to adopt the apps.

Security related question: To assess participants preferences for sharing personal information via COVID-19 apps, we asked them to complete a sentence for Q3.7 that provided a list of plausible reasons.

"I would be okay providing personal information to a COVID19 related App if..."

As shown in Figure 3, the number one preference (51%) for participants to be ok in sharing personal information is if they knew what information was being collected and for what purpose. This order of preferences indicates that users want to have clarification and transparency about their data protection and usage limitation of their data when it comes to COVID 19 pandemic apps. In addition, participants wanted transparency in how their data was going to be used and shared as well as assurance of data use and collection in a secure aggregated manner.

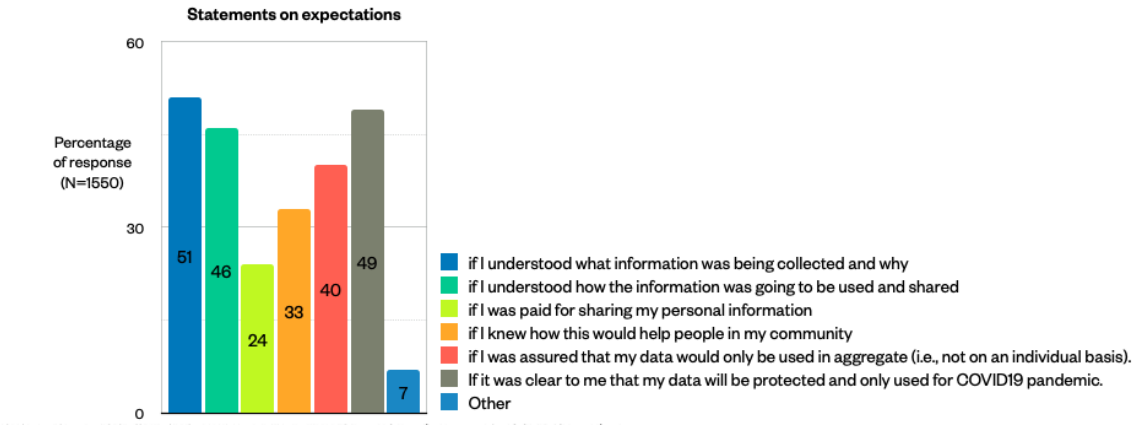


Fig. 3. In which condition users would be okay providing personal information to a COVID19 related App?

We also investigated participants' general privacy and security awareness and concerns. In addition to performing independent analysis of responses for particular privacy/security questions (Q3.2) and users' expectations of transparent data handling (Q1.3, Q2.3), we also performed linear regression analysis to examine whether the responses of these two questions were correlated. For example, we utilized a given question as an independent variable: Are you concerned about security vulnerabilities (getting hacked by malicious actors) when using COVID19 mobile apps? and another question as a dependent variable: 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 tracing apps? to conduct this analysis. This helped us map if users' motivation to use tracing apps after being guaranteed confirmation to delete data anytime depended on general security concerns. As we can see in Table 3, We found a significant positive relationship (p-value 0.0000024) which indicates higher concern of users wanting to have guarantee over their data if they want to use COVID-19 apps. Moreover, we found a similar positive relationship in case of status app (Q2.3) use with privacy/security concerns where p -value was 0.00192 and indicates a positive relationship.

Table 3. Relationship between security concerns in using COVID-19 app and using it upon guaranteed deletion of data from apps

Response Variable	Predictor Variable	P-Value	RSE
security concerns	Q1.3: If you could be guaranteed that you could completely delete all of your data from this tracking/tracing app at any time, would that make you more likely to use it?	.0000024	.433
security concerns	Q2.3: If you could be guaranteed that you could completely delete all of your data from this status app at any time, would that make you more likely to use it?	0.00192	0.4344

4.3 Privacy Protection Preferences

For understanding participant's preferences of privacy protections for particular data types, we asked participants to indicate if they did not want certain data types to be collected by COVID-19 apps, given that mobile apps often collect personal information that may not be relevant to its functioning. These data types included email, username, photos, contacts, browsing history, machine address, geographical locations, operating system, and screen size. Based on the responses from participants, we found that the greatest concern was for photos (60%), followed by browsing history (59%), contact list (57%), and email (48%), username is 40%, machine address is 38.5%, Geographical location is 33%, operating system is 32%, screen size is 23%, None was 11% and 7.8% replied they don't know. Interestingly, our results show that a comparatively small percentage of our participants are concerned about sharing their geographical location than we had anticipated A recent study have reported that several COVID-19 apps, in particular contact tracing apps have been using different permissions requests to access photos and media, Bluetooth, contact information, internal and external storage, and network state in the installation stage [24]. As it can be seen above, this survey results show that users do not want to share their photos, browsing history, and contacts.

The above results present an interesting dilemma. Many of the recent literature on privacy preserving contact tracing focuses on privacy protections for location data by providing protocols that can either make the user's exact location confidential or utilizing bluetooth token exchange in certain distances to avoid using GPS location. For example, some researchers proposed different types of construction of those bluetooth tokens and some raised concerns in utilizing those tokens in a privacy preserving manner. However, we encountered a disparity in users' priority in protecting their geographical data (only 33%) which is comparably lower than some other data types namely username, emails. Our results did not support a prior study which had reported that people did not consider their username and email address as sensitive data [2]. However, this might not be a potential contradiction. Perhaps these priorities are related to users' level of knowledge and awareness about the privacy violations that can occur with their geographical data if shared within the wrong hands [20]. It might be also related to the shortfalls of self-management when it comes to privacy protections [34]. Perhaps the existence of structural problems for an individual to manage their privacy separately while different entities are collecting their data is an impossible task. For example, it may not be feasible for an individual to weigh privacy cost and benefit based on sensitivity without an understanding of potential downstream uses. From a psychological aspect, it can also be described as an inconsistency in planned behavior where an individual's intention is to engage in a behavior at a specific time and place. The theory is intended to explain all behaviors over which people have the ability to exert self-control [1]. We haven't probed into details on these psychological aspects. Instead, we

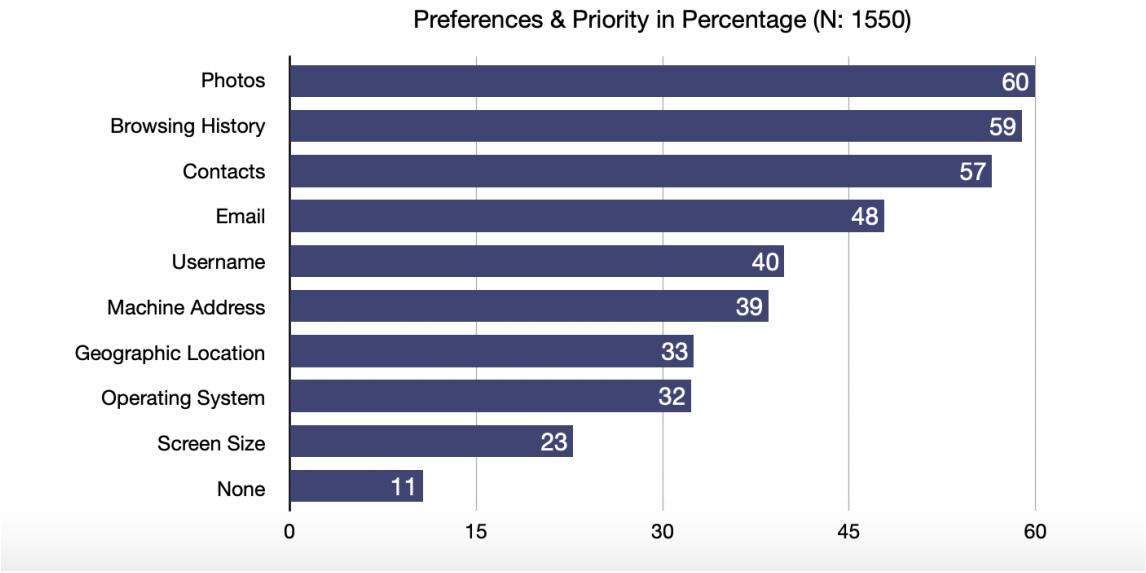


Fig. 4. Percentage of users' reluctance in collection of different Data types by COVID-19 apps.

have addressed human limitations on self-management for their privacy and how a better design can nudge them to measure and make informed decisions while using technologies, like, COVID-19 apps which can lead a user into potential exploitation if privacy protection are not implemented properly.

Besides these three main mechanisms of trust, transparency and preferences, we also investigated other factors that users provided as their personal reasons for why they would utilize a track/trace app in this case of COVID-19 (Q3.6). As shown in table 4, intention of helping the community and concerns for the economy were the top two personal reasons that our participants reported as their motivation for adopting COVID-19 apps. Their responses showed a mean score of 3.337 (N: 1550; in 5 likert scale where 1: not compelling at all and 5: extremely compelling) which made many people unemployed. The economic impact of COVID-19 is substantial. There are two dominant factors which are collective health concerns for the community (mean 3.174) and sense of responsibility (mean 3.177).

We further investigated the relationship between general privacy/security concerns and users' three potential personal reasons (with highest mean mentioned above) to utilize track/trace COVID-19 apps. As reported in Table 2, we did not find any significant relationship among these variables. Concerns for security vulnerabilities and concerns for collective health had p-value of 0.518 with residual standard error of 0.4358. Respectively, Concerns for security vulnerabilities and sense of responsibility showed p value of 0.8473 and residual error of 0.4353 whereas economic concerns with security vulnerability showed p-value of 0.378 and residual standard error of 0.4362. From these results it seems that participants' concern related to privacy and security of apps is not related to their personal reasons for adaptation. However, we can see from table 5 that the predictor variable is independent of whether they are concerned about security of COVID-19 apps. Perhaps this is influenced by their own and societal concern about the coronavirus.

Table 4. Three compelling Personal reason for utilizing COVID-19 Tracing/tracking apps

What reasons, if any, do you think are the most compelling for why you might personally utilize a track/trace app?	mean	Sd
The economic impact of COVID-19 is substantial; many people have lost wages, jobs, or aren't able to pay their housing, food, and other basic needs.	3.337	1.312
With COVID-19, our collective health is intertwined; protecting others is the best way to protect myself.	3.19	1.319
Many others are doing their part to help combat the spread of COVID-19; we're all in this together, and I should do my part as well.	3.19	1.287

Table 5. Linear relationship between general security concerns and users' three potential personal reasons of using COVID-19 apps in this pandemic

Response Variable	Predictor Variable	P-Value	Residual Standard Error	Multiple R2	Adjusted R2	F-Stat
security concerns	economic concerns	0.378	0.4362	0.0004908	-0.0001402	0.7778
security concerns	concerns for collective health	0.5184	0.4358	0.0002645	-0.0003695	0.4172
security concerns	sense of responsibility	0.8473	0.4353	2.353e-05	-0.000611	0.03709

4.4 Consideration of Preference, Trust, and Transparency

In this section, we experimented with chosen open-ended questions (recorded in Appendix A.1) from user surveys. Topics within the open-ended questions were modeled with Latent Dirichlet Allocation (LDA) in order to assess the overarching themes within each question's response. Responses were cleaned with lemmatization and filtered with Python's NLTK stop word list. From the remaining tokens, only those that were tagged as nouns, adjectives, verbs, or adverbs (as determined by Python's Spacy '$en_{core\,web}'_{sm}$ model) were used in the determination of topic generation. Due to $LDA's$ reliance on knowing the number of topics as input, the chosen number of topics for each question was determined by testing values in the range of 2 to 15, inclusive. Configurations were compared with the topic coherence $UMass$ score and the number of topics that resulted in the highest score for each question were used. Topics were later condensed by inference based on the top ten keywords presented for each individual topic along with the context of the question asked in order to qualify general response trends. After the topics within the replies were modeled, the topic weights from LDA were used within a $t-distributed$ stochastic neighbor embedding ($t-SNE$), which allowed the higher dimensional data to be visualized in two dimensions. This allows an intuition of the structure of the data to be gained and understand the magnitude at which the topics were classified [27], [11].

Of the topics found within the responses represented in Figure 5, the topics that directly addressed app using for the sake of family members, economy, avoiding contact with potentially infected individuals, or if the user themselves

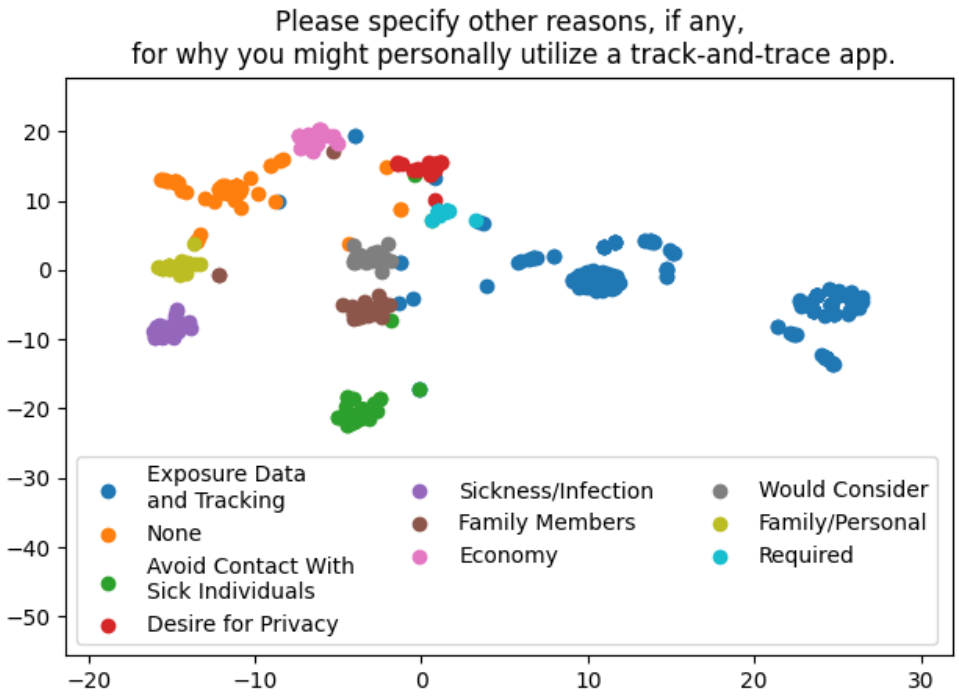


Fig. 5. Topic Modeling for open-ended question Q4.1 (appendix A 1). Please specify other reasons, if any, for why you might personally utilize a track-and-trace app.

were infected. Other topics found seemed to be indicated individuals had concerns about such apps before they would consider using it. These concerns included the tracking aspect of the app and desires for privacy. There was also indication that some participants would consider using an app, possibly dependent on other conditions, or would only do so if it were required.

For Q4.2 in Figure 6, the groups that participants said they would trust fell into 3 main categories: entities within the health industry such as insurance companies or healthcare professionals, government entities, or family. Some participants were unsure of if there were other entities that may trust or left a response that indicated that there were none. With some of the responses only being the word 'none', perhaps this topic is selected either because participants do not trust any entity at all or because they could not think of any other entities at the time. Some responses indicated topics, like, Hackers and police but this only accounted for 2 of the overall responses that were difficult to interpret, and each only appeared in one response.

From topic modeling of Q4.3 in figure 7, our hypothesis driven results were confirmed. As it can be seen in Figure 7, expectations around trust, transparent data collection and secure management of information in case of using COVID-19 apps are frequent topics that are specified. In brief, our results indicate that most participants would be okay sharing their personal data via COVID-19 apps if privacy protections were provided for the information that is being collected and security measures were put in place for the information storage. The other insight from our topic modeling is that users would never provide personal information or would only do so if there was a mandate. Some users replied

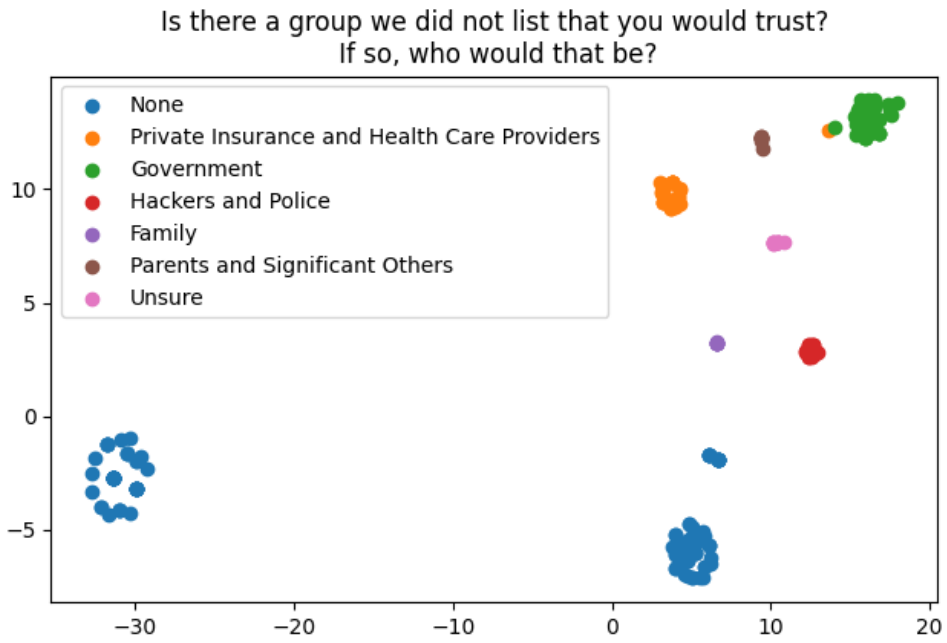


Fig. 6. Topic Modeling for open-ended question Q4.2 (appendix A.1). Is there a group we did not list that you would trust? If so, who would that be?

with the word 'none', which may signify they did not wish to respond to this particular question or they would not be comfortable providing information in any scenario. The topics that covered negative feelings towards this particular scenario were populated by statements that had negative sentiment towards tracking apps and COVID19 itself.

Figure 8 represents responses regarding the conditional use of a tracing app or status app both raised concerns about the data generated by the respective apps. In this regard, the conditional use of a tracing app hinged more on the reputability of the entity that handles the data, while the status app had more of a focus on the privacy of the data. In both scenarios, concerns over accuracy were raised, which may indicate that users are not sure of the functionality of the apps and therefore do not want to indicate under which conditions they would use it.

Within the conditional use of the tracing app, users mentioning the government appeared in both positive and negative connotations (in reference to the tracing app itself). Of the 3 responses (out of 122) that directly mentioned the word 'government', there was 1 indication that the participant would only use the tracing app if government was not involved, 1 indication that they would use the app only if the government were involved or endorsed the app, and 1 that did not clearly indicate either way. Responses regarding the conditional use of a status app elaborated more on their conditional use, possibly due to the increased number of responses (259). The reasons that users would use the status app can be summarized with topics of occupational need, health related issues, medical information, and family. Other topics discussed within the responses again touched on concerns about privacy and security of the information collected as well as concerns about how intrusive such an app might be. The topic of discrimination was also brought up in 3 other responses.

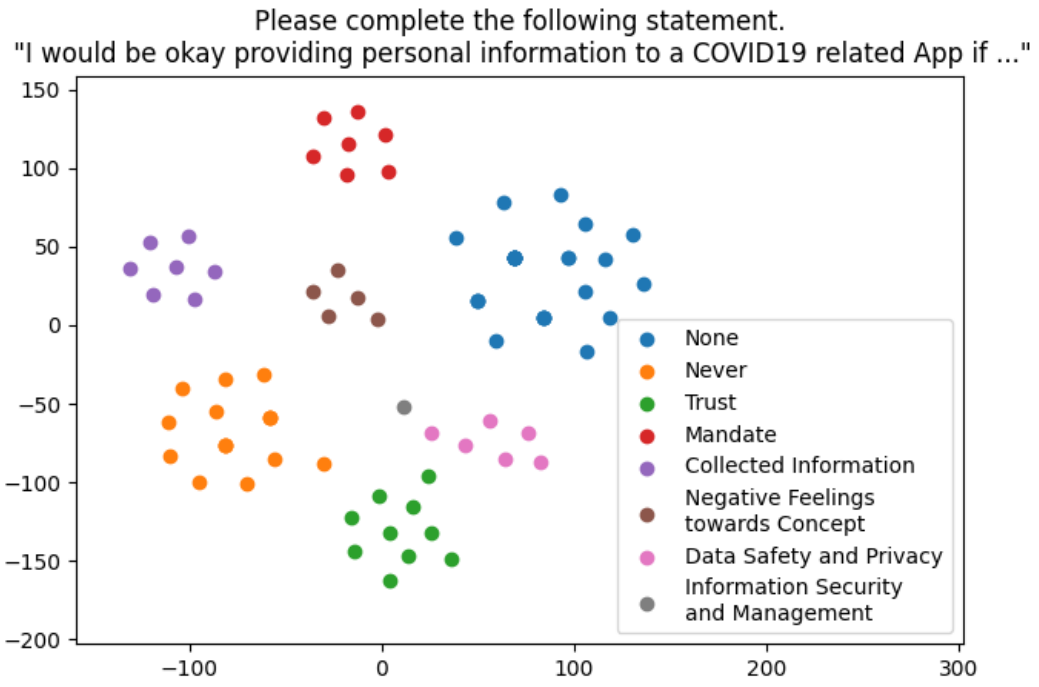
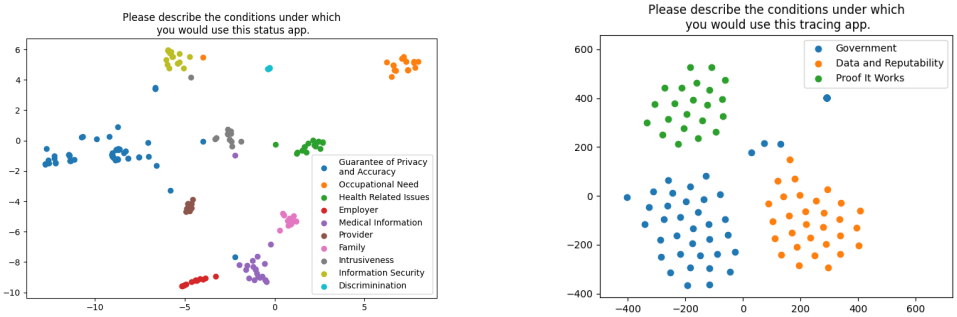


Fig. 7. Topic Modeling for open-ended question Q4.3 (appendix A.1). Please complete the following statement. I would be okay providing personal information to a COVID19 related App if...



(a) (b)

Fig. 8. Topic Modeling for open-ended questions Q4.4, Q4.5 (appendix A.1). Please describe the conditions under which you would use this tracing app. & Please describe the conditions under which you would use this status app

Within most questions and scenarios presented for the participants, the topic of information security or privacy was discussed to some degree. There were also concerns about abuse of this information, such as discrimination, that may need to be addressed with such apps. There is also a variety of factors that are disincentivizing users from using

apps like these. The topics above seem to indicate that one of those main concerns is about how information is used and where it ends up. Perhaps this is due to the users' unfamiliarity with how this technology functions. In order to circumvent this unfamiliarity, an app's design may need both privacy-driven design and user-driven design in which the user feels satisfied with the level of control they have over their data and their working knowledge of how the app works. Mechanisms that allow users to control over their own data may include systems in which data is sent to others only when specified and is not an automatic process. Such a system would also need to be accompanied by a system that informs the user of what information is actually being released, along with which entities are receiving what information and why that is needed for the app to function. Allowing users to view this data use and flow would be a good design strategy may alleviate some of these reported concerns.

5 DISCUSSION

As people around the world are dealing with the recent COVID-19, many different strategies are being used and proposed for how we can combat this pandemic. One of the main solutions that technologists have offered is the use of contact tracing. While some countries have been successful in using these apps to tackle the pandemic, the use of such apps in the US and some regions of the world remains unclear and there is much public debate about not only the efficacy of such apps but also the protection of individual privacy rights. To provide some insight into this national debate, we conducted an online study for a midwestern region in the US to learn more about people's attitudes towards such innovative technologies, their privacy/security concerns, and to explore the conditions under which they will adopt such an app. To the best of our knowledge, there aren't any standardized assessment questionnaires or framework developed for measuring users' perspectives on privacy for mobile apps. While the National Institute of Science and Technology (NIST) and International Association of Privacy Professionals (iapp) does have a framework for assessing mobile apps security by vetting approach [35], [25] it does not address or include privacy explicitly. Therefore, we followed the closest framework relevant to our work which is NIST's privacy framework that includes aspects such as accountability, trust and transparency both from a stakeholder and user's point of view [9].

As presented above, our results indicate that most of our survey participants regard privacy/security protections as one of the main features they seek in these types of apps. We assessed participant's trust in using COVID-19 apps and our results reveal that when it comes to tracing and status apps, most participants would put their trust in medical providers while they trust at least the federal government. More in-depth analysis of the open-ended question shows a similar pattern where participants would trust private insurance and health care providers the most for developing such apps. These results were further confirmed when we analyzed participants' current use of COVID-19 apps which demonstrates participants preference for using COVID-19 health/fitness and Information apps that are mainly provided by CDC and WHO. Furthermore, through statistical analysis, we found that participants' adoption decision for such apps is based on how much they trust a given entity with the privacy protections of such apps.

Our survey results also provide empirical evidence for the kinds of data protections that users are seeking when it comes to COVID-19 contact tracing and status apps. For example, participants would prefer control over their data and like to know the data practices of COVID-19 apps. Therefore, transparency of data practices such as when their data will be deleted or having control over such matters are important considerations. Additionally, our findings suggest that most participants would be okay with providing personal information if they knew the purpose for the data collection and the type of data that are being collected. For example, many of the participants expressed concern over the protection of their data and if the use of such data will be limited to COVID-19 pandemic. Participants also conveyed

a preference for knowing how their information was going to be shared and used as well as requiring even trusted entities to provide assurance for the security of their shared data.

In our survey, we also inquired about the privacy protections that participants were seeking, as well as their expectations from such contact tracing and status apps. We know from previous studies that people might have more sensitivity for one type of information over another. An analysis of our survey questions dedicated to users' feature preferences and their expectation and priority of privacy show that most of our participants want COVID-19 apps to be regulated and have data protections mechanisms in place. Interestingly, our study participants prioritize their privacy protections for personal data in the following order with the highest protection offered to photo libraries, browsing history followed by contacts, email, username, machine address, geographical location, and so on. This is a surprising and yet illuminating discovery because it is often expected that users would consider their geographical location data as one of the most sensitive data and therefore would prioritize it for privacy protections [2]. This data type is one of the main data components that is needed for the functionality of contact tracing and status apps and yet most of our participants did not rate this as a top privacy vulnerability. What is even more disconcerting is that most of the recent literature related to COVID-19 apps privacy and security focuses on location information within these apps. For example, as it can be seen in Table 1 that most of the published research emphasizes the design and security protocol to protect fine grained location information by proximity tracing and Bluetooth technology usage. So, there is evidently a disconnect between what people consider to be private and personal information versus what technology developers are considering to be private information. Perhaps some of this disconnect may be attributed to participants' lack of knowledge about location data and the privacy vulnerabilities that it may introduce. Nevertheless, while we acknowledge the limitations of our study and acknowledge that our findings do not generalized to all populations in the US or abroad, we do believe this phenomena warrants further research and attention if we want to align public and technologists attention and efforts and design human-centered technologies that respects social norms and incorporates privacy by design. The survey participants also provided additional insight on their views of the COVID-19 apps. Though privacy and security protections are the top preferences when using COVID-19 apps, some of the participants reported that they would use such apps regardless of privacy/security protections due to economic, personal, and social concerns for the wellbeing of loved ones and to avoid contracting the virus.

These findings undoubtably indicate that one of the main challenges in deploying contact tracing and status apps in the United State and many other countries is related to privacy/security protections. It is also worth considering that perhaps, these findings are influenced by the emergencies and risk-based factors that are present in the minds of our participants in the midst of a pandemic. Furthermore, factors such as political ideology and level of education and many other factors may have influenced our findings. However, our focus in this paper has been related to direct questions related to privacy protections. Therefore, further analysis of these confounding variables will be performed at a later time. We believe the results of this study are not only timely, but also crucial for the development of COVID-19 apps in the U.S. and other regions. Our findings can guide app designers and developers, as well as health policy makers who may want to use technological approaches in combating COVID-19 and future pandemics. For example, providing users more control over data in times of crisis might alleviate some of the general uncertainty that comes with the contact tracing apps. This will also provide users a more tangible and active form of involvement with their own information which may lead to more adaptation of these apps. It is also important to note that currently there is a lack of comprehensive privacy protection criteria for mobile apps and thus having some set of user-centered protections that can be operationalized as possible privacy controls in COVID-19 app design can serve as a potential strategy forward.

In conclusion, our research findings suggest that in order to design and develop a privacy inclusive COVID-19 app, technologists must plan for the appropriate data protection mechanisms that considers three important factors related to its users namely trust, transparency, and their preferences. Especially if we are aiming to increase timely adaptation and our lives and well-being may depend on it. Based on our study findings we recommend the following 3 design components:

1. **Trust:** Our results showed that there is a strong positive relationship between trust and COVID-19 app adoption. Participants are more likely to use apps if those are provided by medical providers and university researchers. It should also be noted that users in the US trust the Government the least. While governments are typically the entity that would develop or publish such apps in times of medical emergencies and thus it is important to consider other approaches that can address this predicament. For example, perhaps the apps that are developed by the government can be validated or approved by a trusted third party that users trust.

2. **Transparency**: Transparency has been shown to be an important factor in many "Privacy by design" frameworks. In the app context it refers to users' expectations for wanting to have a clear indication of how their data will be handled [9]. In our study, transparency is clearly noted as an important factor by the users and therefore we recommend that app developers take this aspect into consideration if their goal is to increase adoption.

3. **Preferences**: This is a critical factor in any app design since the success of any app depends on its users, and the particular features they seek in a given app. When developing COVID-19 apps, we recommend that developers also consider cultural and regional differences in their design. Based on our survey results from a midwestern US state it is clear that users have a strong preference for privacy and security protections if they were to use such an app.

6 LIMITATION

As stated above, this survey was conducted in the midwestern region of the United States and therefore the results may not be applicable to other parts or people of the world. Further research studies that include different populations and regions of the world need to be conducted to determine if these results apply to a global context. In addition, factors such as social desirability may have influenced our results because participants may have been primed to value privacy protections based on the questions. Furthermore, our survey was online, hence, we only reached participants who are familiar with using technologies. Therefore, their response on privacy/security concerns involving COVID-19 technologies can be biased in some ways.

Considering above limitations, further studies need to be conducted to replicate and confirm our results with diverse sets of samples. We plan to conduct more in-depth analysis to implement the three user-based mechanisms in formal engineering methods with a focus of technological aspects.

7 CONCLUSION

Privacy protections are important considerations for societies where civil liberties and democracy are mainstream. To assure these protections, technical measures in the system level are important elements to assure privacy. While legal protections may lag behind technological innovations it is essential to consider users preferences when designing effective technologies. If our aim is to design human centered computer applications that is also privacy preserving. We need to design accessible features that allows users to have controls over how and what the technology does with their data. This is especially critical when it comes to apps that are to be used in emergency situations where lives can be saved. With COVID-19 apps, if the goal is to increase user engagement/adoption, then app designers must consider not only how users' privacy can be protected but also consider how the app may pose unexpected privacy risks. Since

currently there are no privacy protection standards for mobile apps, we suggest that developers at least consider the three main mechanisms (trust, transparency, and preferences) from users' perspective when designing COVID-19 apps. We believe these design recommendations can be applied for any future apps that may be associated with privacy risks.

REFERENCES

[1] Icek Ajzen. 2011. The theory of planned behaviour: Reactions and reflections.

[2] Faiz Anuar and Ulrike Gretzel. 2011. Privacy concerns in the context of location-based services for tourism. In *ENTER 2011 Conference*.

[3] Kakoli Bandyopadhyay and Katherine A Fraccastoro. 2007. The effect of culture on user acceptance of information technology. *Communications of the Association for Information Systems* 19, 1 (2007), 23.

[4] Gaurav Bansal, David Gefen, et al. 2010. The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision support systems* 49, 2 (2010), 138–150.

[5] Mahmoud Barhamgi, Charith Perera, Chirine Ghedira, and Djamal Benslimane. 2018. User-centric privacy engineering for the internet of things. *IEEE Cloud Computing* 5, 5 (2018), 47–57.

[6] Mahmoud Barhamgi, Mu Yang, Chia-Mu Yu, Yijun Yu, Arosha K Bandara, Djamal Benslimane, and Bashar Nuseibeh. 2017. Enabling end-users to protect their privacy. In *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*. 905–907.

[7] Erlend Bergen, Dag F Solberg, Torjus H Sæthre, and Monica Divitini. 2018. Supporting the co-design of games for privacy awareness. In *International Conference on Interactive Collaborative Learning*. Springer, 888–899.

[8] David M Blei. 2012. Probabilistic topic models. *Commun. ACM* 55, 4 (2012), 77–84.

[9] Kaitlin R Boeckl and Naomi B Lefkovitz. 2020. NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0. (2020).

[10] Samuel Brack, Leonie Reichert, and Björn Scheuermann. 2020. Decentralized Contact Tracing Using a DHT and Blind Signatures. *IACR Cryptol. ePrint Arch.* 2020 (2020), 398.

[11] Diego Buenaño-Fernandez, Mario González, David Gil, and Sergio Luján-Mora. 2020. Text Mining of Open-Ended Questions in Self-Assessment of University Teachers: An LDA Topic Modeling Approach. *IEEE Access* 8 (2020), 35318–35330.

[12] Ann Cavoukian et al. 2009. Privacy by design: The 7 foundational principles. *Information and privacy commissioner of Ontario, Canada* 5 (2009).

[13] Ann Cavoukian, Angus Fisher, Scott Killen, and David A Hoffman. 2010. Remote home health care technologies: How to ensure privacy? Build it in: Privacy by design. *Identity in the Information Society* 3, 2 (2010), 363–378.

[14] Justin Chan, Shyam Gollakota, Eric Horvitz, Joseph Jaeger, Sham Kakade, Tadayoshi Kohno, John Langford, Jonathan Larson, Sudheesh Singanamalla, Jacob Sunshine, et al. 2020. Pact: Privacy sensitive protocols and mechanisms for mobile contact tracing. *arXiv preprint arXiv:2004.03544* (2020).

[15] 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).

[16] Kevin Anthony Hoff and Masooda Bashir. 2015. Trust in automation: Integrating empirical evidence on factors that influence trust. *Human factors* 57, 3 (2015), 407–434.

[17] Marcello Ienca and Effy Vayena. 2020. On the responsible use of digital data to tackle the COVID-19 pandemic. *Nature medicine* 26, 4 (2020), 463–464.

[18] Nirmal Kandel, Stella Chungong, Abbas Omaar, and Jun Xing. 2020. Health security capacities in the context of COVID-19 outbreak: an analysis of International Health Regulations annual report data from 182 countries. *The Lancet* (2020).

[19] Gabriel Kaptchuk, Eszter Hargittai, and Elissa M Redmiles. 2020. How good is good enough for COVID19 apps? The influence of benefits, accuracy, and privacy on willingness to adopt. *arXiv preprint arXiv:2005.04343* (2020).

[20] Bandana Kar, Rick C Crowsey, and Joslyn J Zale. 2013. The myth of location privacy in the United States: Surveyed attitude versus current practices. *The Professional Geographer* 65, 1 (2013), 47–64.

[21] Douglas J Leith and Stephen Farrell. 2020. Coronavirus contact tracing app privacy: What data is shared by the singapore opentrace app. *Retreived from https://www. scss. tcd. ie/Doug. Leith/pubs/opentrace_privacy. pdf* (2020).

[22] Joseph K Liu, Man Ho Au, Tsz Hon Yuen, Cong Zuo, Jiawei Wang, Amin Sakzad, Xiapu Luo, and Li Li. 2020. Privacy-Preserving COVID-19 Contact Tracing App: A Zero-Knowledge Proof Approach. *IACR Cryptol. ePrint Arch.* 2020 (2020), 528.

[23] Anna U Morgan, Mohan Balachandran, David Do, Doreen Lam, Andrew Parambath, Krisda H Chaiyachati, Nancy M Bonalumi, Susan C Day, Kathleen C Lee, and David A Asch. 2020. Remote Monitoring of Patients with Covid-19: Design, implementation, and outcomes of the first 3,000 patients in COVID Watch. *NEJM Catalyst Innovations in Care Delivery* 1, 4 (2020).

[24] N Nair. 2001. Childhood tuberculosis: public health and contact tracing. *Paediatric Respiratory Reviews* 2, 2 (2001), 97–102.

[25] Steve Quirolgico, Jeffrey Voas, Tom Karygiannis, Christoph Michael, and Karen Scarfone. 2015. *Vetting the security of mobile applications.* US Department of Commerce, National Institute of Standards and Technology.

[26] Julie M Robillard, Aaron W Li, Shilpa Jacob, Dan Wang, Xin Zou, and Jesse Hoey. 2017. Co-Creating Emotionally Aligned Smart Homes Using Social Psychological Modeling. In *Proceedings of the 4th international Workshop on Sensor-based Activity Recognition and Interaction*. 1–6.

[27] Tushar Kanti Saha Santa Maria Shithil and Tanusree Sharma. [n.d.]. A Dynamic Data Placement Policy for Heterogeneous Hadoop Cluster. ([n. d.]).

[28] Oshani Seneviratne and Lalana Kagal. 2014. Enabling privacy through transparency. In *2014 Twelfth Annual International Conference on Privacy, Security and Trust*. IEEE, 121–128.
[29] Tanusree Sharma, John C Bambenek, and Masooda Bashir. 2020. Preserving Privacy in Cyber-physical-social Systems: An Anonymity and Access Control Approach. (2020).
[30] Tanusree Sharma and Masooda Bashir. 2020. Are PETs (Privacy Enhancing Technologies) Giving Protection for Smartphones?–A Case Study. *arXiv preprint arXiv:2007.04444* (2020).
[31] Tanusree Sharma and Masooda Bashir. 2020. Privacy apps for smartphones: An assessment of users' preferences and limitations. In *International Conference on Human-Computer Interaction*. Springer, 533–546.
[32] 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.
[33] Lucy Simko, Ryan Calo, Franziska Roesner, and Tadayoshi Kohno. 2020. COVID-19 Contact Tracing and Privacy: Studying Opinion and Preferences. *arXiv preprint arXiv:2005.06056* (2020).
[34] Daniel J Solove. 2012. Introduction: Privacy self-management and the consent dilemma. *Harv. L. Rev.* 126 (2012), 1880.
[35] Murugiah Souppaya and Karen Scarfone. 2013. Guidelines for managing the security of mobile devices in the enterprise. *NIST special publication* 800 (2013), 124.
[36] Carmela Troncoso, Mathias Payer, Jean-Pierre Hubaux, Marcel Salathé, James Larus, Edouard Bugnion, Wouter Lueks, Theresa Stadler, Apostolos Pyrgelis, Daniele Antonioli, et al. 2020. Decentralized privacy-preserving proximity tracing. *arXiv preprint arXiv:2005.12273* (2020).
[37] Tyler M Yasaka, Brandon M Lehrich, and Ronald Sahyouni. 2020. Peer-to-Peer contact tracing: development of a privacy-preserving smartphone app. *JMIR mHealth and uHealth* 8, 4 (2020), e18936.
[38] Xiao Yue, Huiju Wang, Dawei Jin, Mingqiang Li, and Wei Jiang. 2016. Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. *Journal of medical systems* 40, 10 (2016), 218.

A APPENDIX

In the appendix section, we recorded our selected survey questions that have been analyzed in this study. In addition, there are some additional graphics and tables included here.

A.1 Analyzed Survey questions

This Appendix includes selected survey questions from three sections from the online survey response. Sections are: Track and Trace app section which contains questions on tracing apps' privacy/security; Passport App Section contains questions on health status apps' privacy/ security and Tech survey Section includes questions about users' preferences on security/privacy while using those apps. Traditionally, tracing contacts is done by the Public Health Department by interviewing patients and calling the people who have come in contact with those patients. The passport app keeps track of whether they have had COVID-19, whether they have been tested for COVID-19 and are disease free, and other indicators of their disease status, like their current temperature. This COVID-19 status app would show their current disease status and could be used to allow people more freedom of movement and do things like go back to work and school.

A.2 Additional Analyzed Open-ended questions from survey

Figure 9 represents participant's thoughts on usage of contact tracing apps when someone is diagnosed with COVID-19 which represents a majority of responses as invasive tracking by using data. Whereas it also represents users' thoughts on status apps documenting COVID-19 categorized as "information". It might be a possible inference on information gathering during COVID-19 status documenting.

Table 6. Survey Question List

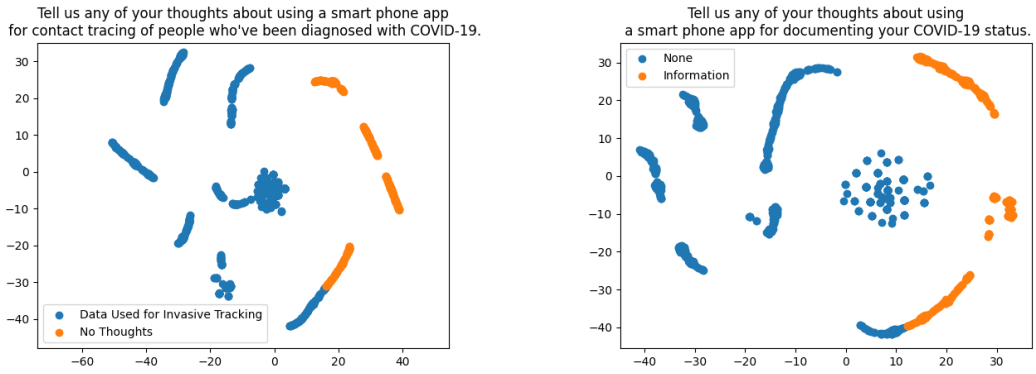
Question Number	Survey Questions	Types
Q1.1	If such an app (tracing/tracking) were available for use, would it matter to you who offered the app and controlled your data?	Multiple Choice
Q1.2	If such a COVID-19 app were offered, who would you trust to control the data? (e.g., private company, federal government, state government, local government, independent institution such as my health system, my employer, or a university)	Likert scale
Q1.3	If you could be guaranteed that you could completely delete all of your data from this tracking/tracing app at any time, would that make you more likely to use it?	Yes/No
Q2.1	If such an app (passport app section) were available for use, would it matter to you who offered the app and controlled your data?	Multiple Choice
Q2.2	If such a COVID-19 app were offered, who would you trust to control the data? (e.g. private company, federal government, state government, local government, independent institution such as my health system, my employer, or a university)	Likert scale
Q2.3	If you could be guaranteed that you could completely delete all of your data from this status app at any time would that make you more likely to use it?	Yes/No
Q3.1	In general, how concerned you are regarding your privacy on Mobile Apps these days?	Likert Scale
Q3.2	Are you concerned about security vulnerabilites (getting hacked by malicious actors) when using COVID-19 mobile apps?	Yes/No
Q3.3	Mobile Apps often collect information for them to function. Please indicate if you do not want a COVID-19 App collecting any of the following information (Please check all that apply). (choice = email address, contacts, photos, machine address, browsing history, geographical location, none of these, I don't know)	Multiple Choice
Q3.4	Have you recently downloaded any of the following COVID-19 related Apps (Please check all that apply)? (choice = Fitness and healthy living apps, Pandemic Tracking app, COVID-19 Information App, Symptom/health Tracker app, Screening apps, Other)	Multiple Choice
Q3.5	Please indicate your agreement/disagreement with the following statements COVID-19 Mobile Apps should be regulated for privacy protections. We should not use mobile Apps to track US citizens because of COVID19. I think Mobile Tracking Apps are a great way to end the pandemic.	Multiple Choice
Q3.6	COVID-19 has impacted everyone in unique ways. What reasons, if any, do you think are the most compelling for why you might personally utilize a track-and-trace app?	Multiple Choice
Q3.7	I would be okay providing personal information to a COVID19 related App if...	Multiple Choice
Q4.1	Please specify other reasons, if any, for why you might personally utilize a track-and-trace app.	Open ended
Q4.2	Is there a group we did not list that you would trust? If so, who would that be?	Open ended
Q4.3	Please complete the following statement. I would be okay providing personal information to a COVID19 related App if ...	Open ended
Q4.4	Please describe the conditions under which you would use this tracing app.	Open ended
Q4.5	Please describe the conditions under which you would use this status app.	Open ended
Q4.6	Tell us any of your thoughts about using a smartphone app for contact tracing of people who've been diagnosed with COVID-19.	Open ended
Q4.7	Tell us any of your thoughts about using a smartphone app for documenting your COVID-19 status	Open ended

Table 7. Demographics of our surveyed participants

Data item	Types	Percentage
Demographics	Midwest USA	
Gender	Female	49.9%
	Male	49.2%
	preferred to self-describe	0.5%
	Nonbinary	0.5%
Ethnicity	White/European-American	68.3%
	Black/African-American	13.3%
	Latino/Latina	6.7%
	Asian	4.7%
	Biracial	4.8%
	Pacific Islander/Native Hawaiian	.5%
	Native American/Alaskan Native	.5%
	self-described/prefer not to answer	.14%
Age	18-90	Total 1378
	18-25	16%
	26-35	18.72%
	36-45	18.14%
	46-55	16.8%
	56-65	17.05%
	66-75	11.17%
	76-90	1.74%

Table 8. Clustered topics of 5 open-ended questions that are analyzed in section 4.4

Data item		Category by Topic Modeling			
Please specify other reasons, if any, for why you might personally utilize a track-and-trace app.	Exposure Data and Tracking	None	Desire for Privacy	Avoid Contact	Sickness / Infection
	Family Members	Economy	Would Consider	Family / Personal	Required
Is there a group we did not list that you would trust? If so, who would that be?	None	Family	Government	Unsure	Hackers / Police
	Insurance and Health Professionals	Parents / Significant Others			
Please complete the following statement. "I would be okay providing personal information to a COVID19 related app if...	Negative Feelings Towards Concept	Data Safety and Privacy	Information Security and Management	None	Never
	Trust	Mandate			
Please describe the conditions under which you would use this tracing app.	Government	Data and Reputability	Proof It Works		
Please describe the conditions under which you would use this status app	Guarantee of Privacy and Accuracy	Health Related Issues	Medical Information	Employer	Occupational Need
	Provider	Family	Intrusiveness	Information Security	Discrimination



(a) (b)

Fig. 9. Topic Modeling for open-ended question Q4.6 and Q4.7