COVID-19 Contact Tracing and Privacy: A Longitudinal Study of Public Opinion

LUCY SIMKO, Paul G. Allen School of Computer Science & Engineering, University of Washington
JACK CHANG, Information School, University of Washington
MAGGIE JIANG, Paul G. Allen School of Computer Science & Engineering, University of Washington
RYAN CALO, School of Law, University of Washington
FRANZISKA ROESNER and TADAYOSHI KOHNO, Paul G. Allen School of Computer Science & Engineering, University of Washington

There is growing use of technology-enabled contact tracing, the process of identifying potentially infected COVID-19 patients by notifying all recent contacts of an infected person. Governments, technology companies, and research groups alike have been working towards releasing smartphone apps, using IoT devices, and distributing wearable technology to automatically track "close contacts" and identify prior contacts in the event an individual tests positive. However, there has been significant public discussion about the tensions between effective technology-based contact tracing and the privacy of individuals. To inform this discussion, we present the results of seven months of online surveys focused on contact tracing and privacy, each with 100 participants. Our first surveys were on April 1 and 3, 2020, before the first peak of the virus in the US, and we continued to conduct the surveys weekly for 10 weeks (through June), and then fortnightly through November, adding topical questions to reflect current discussions about contact tracing and COVID-19. Our results present the diversity of public opinion and can inform policy makers, technologists, researchers, and public health experts on whether and how to leverage technology to reduce the spread of COVID-19, while considering potential privacy concerns.

CCS Concepts: • **Security and privacy → Human and societal aspects of security and privacy**; • **Human-centered computing → Collaborative and social computing systems and tools**; **Collaborative and social computing**; • **Applied computing → Life and medical sciences**; • **Social and professional topics → Government technology policy**; **Medical information policy**

Additional Key Words and Phrases: Privacy, security, usable security, contact tracing, longitudinal, COVID-19

ACM Reference format:
Lucy Simko, Jack Chang, Maggie Jiang, Ryan Calo, Franziska Roesner, and Tadayoshi Kohno. 2022. COVID-19 Contact Tracing and Privacy: A Longitudinal Study of Public Opinion. *Digit. Threat.: Res. Pract.* 3, 3, Article 25 (October 2022), 36 pages.
https://doi.org/10.1145/3480464

This research was supported in part by a University of Washington Population Health Initiative's COVID-19 Rapid Response Grant and by the University of Washington Tech Policy Lab, which receives support from: the John D. and Catherine T. MacArthur Foundation, Microsoft, and the Pierre and Pamela Omidyar Fund at the Silicon Valley Community Foundation. This work was also supported by the US National Science Foundation (Awards 1565252 and 1513584).
Authors' addresses: L. Simko, M. Jiang, F. Roesner, and T. Kohno, Paul G. Allen School of Computer Science & Engineering, University of Washington, Seattle, WA, 98195, USA; emails: simkol@cs.washington.edu, mjiang@cs.washington.edu, franzi@cs.washington.edu, yoshi@cs.washington.edu; J. Chang, Information School, University of Washington; R. Calo, School of Law, University of Washington, Seattle, WA, 98195, USA; email: rcalo@uw.edu.

2576-5337/2022/10-ART25 $15.00
https://doi.org/10.1145/3480464

1 INTRODUCTION

Technology companies, university research groups, and governments have been diligently working to deploy COVID-19 contact tracing apps, for which adoption has been slow [9, 18]. Prior work has determined that contact tracing apps are most effective when used by the majority of a population [22, 26, 64]; however, some have raised security and privacy concerns (e.g., References [15, 86]) as well as broader concerns about efficacy (e.g., Reference [85]).

Our research seeks to provide to the scientific, technology, and policy communities an informed understanding of the public's values, concerns, and opinions about the use of automated contact tracing technologies. We argue neither for nor against automated contact tracing in this work, but instead, we offer a summary of public opinion on potential contact tracing scenarios, since many regions have already implemented automated contact tracing programs or are moving towards them. We ask the following research questions:

- **App functionality.** What do potential users want a contact tracing app to do or not do? What data sources do people feel most and least comfortable with being used for contact tracing? Our survey asks about potential app features and multiple data sources, including: location data (e.g., from cell tower data, credit card history, or wearable electronics), proximity data, data from an existing app, and data from a new app by a known entity or company (Sections 5.2 and 5.4).
- **Developer and stakeholder identity.** What kinds of institutions do potential users trust to conduct or implement automated contact tracing? We ask about trust in a number of potential developers, including government agencies and well-known tech companies (Section 5.3). We also solicit individuals' opinions regarding contact tracing data being shared with or used by different entities for the purposes of contact tracing. We consider data sharing with and usage by multiple entities, including: their government, cellular provider, cellphone manufacturer, and various well-known technology companies (Sections 5.3 and 5.4).
- **Changes over time.** How, if at all, has public opinion about the preceding topics changed over time? We discuss longitudinal changes in Sections 5.2–5.4. We also ask (Section 5.5) whether there are any correlations with demographic factors or world events, e.g., the global or regional infection rate.

We capture public opinion using an international paid survey platform (Prolific). Our first survey (April 1, 2020) was repeated weekly through June and fortnightly thereafter, with the latest data collected on November 6, 2020. Each survey collected data from 100 participants, and we collected two surveys in the first week (200 participants total). Our first surveys preceded the initial viral peak infection rate in North America, which was before contact tracing apps were available in many of the regions that now have them, and was early in the public discourse about contact tracing; our later surveys track how public opinion evolves over time.

This article addresses a broad audience—researchers, app developers, public health officials, policy makers, and so on. Our results can inform (1) ongoing technical efforts to design contact tracing apps in a privacy-preserving manner, (2) how the makers of such a contact tracing app or program communicate the privacy properties of their contact tracing program to their potential users, and (3) legal, ethical, and policy discussions about the appropriate use and design of such technologies. At a high level, we find:

- **Privacy preferences are stable over time at a population level.** We find that public opinion about privacy and contact tracing is roughly stable over time, suggesting that our—and others'—results can successfully inform future efforts. We find there is a shrinking population that has yet to use contact tracing apps, and that privacy concerns limit potential users' willingness to download the apps. Therefore, the population that does not yet use a contact tracing app may appear to become more privacy-conscious as the less privacy-conscious leave it and download an app (Section 5.2).
- **An abundance of concerns about data sharing, usage, and developer identity leads to a personal decision about the tradeoffs between privacy and health and leaves no perfect solution.** We observe that potential contact tracing app users care deeply about the identity of the developer, and have strong opinions about with whom data should or should not be shared. However, we note that participants

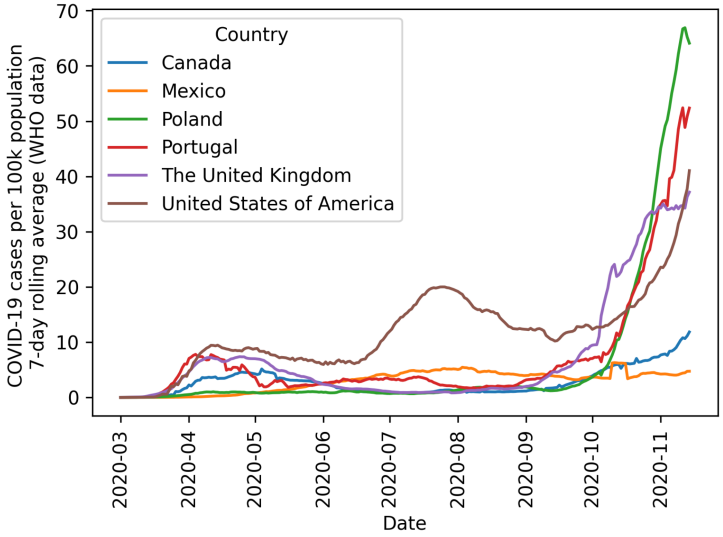


Fig. 1. COVID-19 new infections per 100k as reported to the World Health Organization (WHO) [66] for the six countries from which we had at least 100 participants (together, these countries comprise 74.4% of our participant pool).

disagree about trusted entities. Many participants raised concerns about sharing with their government and data being used for advertising or government surveillance, now or in the future (Section 5.3).

- **Informed consent and transparency about data sharing and usage may mitigate some privacy concerns.** Participants expressed a strong desire for meaningful consent and control over their data. If developers and policy makers (1) better inform the public about the current and future use of their data and (2) give individuals control over how their data are used, then they may be more willing to enroll in automated contact tracing. For example, we find support for judicial oversight of government data usage in some circumstances, potentially making users more confident that their data would not be misused (Section 5.3).
- **Mental models of technical and legal concepts are often incomplete or inaccurate but play a significant role in potential users' willingness to begin contact tracing.** Participants repeatedly reasoned about the *accuracy* of certain technical methods of contact tracing (e.g., GPS vs. Bluetooth), the *competence* of the app developer to implement contact tracing at a technical level, and the *capability* of their government to protect (or exploit) their data. Through this reasoning, we identified multiple inaccurate or incomplete mental models, e.g., some participants thought a proximity tracking app would be less secure than a location tracking app due to constant communication with others' phones via Bluetooth. Other participants overestimated the prevalence of judicial corruption, causing them to discount the protection potentially provided by judicial oversight of government data usage. These mental models invite stakeholders to improve user education so users can make well-informed decisions.

2 THE EVOLUTION OF CONTACT TRACING DURING THE COVID-19 PANDEMIC

To contextualize our results, this section captures the state of the world on April 1, when we first deployed our survey, and how both the infection rates and contact tracing efforts progressed through November, when the last data reported on here was collected.

2.1 COVID-19 Infection Rates and Quarantine Restrictions

Infection rates. On April 1, the course of the COVID-19 pandemic had not yet reached its first peaks outside of Asia. Figure 1 shows the number of infections per 100K people in the six countries from which we had at least

100 participants total: Canada, Mexico, Poland, Portugal, the UK, and the US. After an initial spring peak in many countries in our dataset, the rate of infection declined. The US saw a second peak of infection in August, though rates of infection in many others countries remained low [24]. In November, many countries were experiencing skyrocketing infection rates, as seen in Figure 1.

Regional lockdowns. On April 1, as we began our survey, many European countries (e.g., the UK, Germany, Italy, and Spain) were under varying forms of lockdown, with some combination of schools, restaurants, bars, and non-essential shops closed, public gatherings banned, and citizens urged or mandated to stay inside except for essential outings [13, 46, 54, 79]. Many in the US were under similar restrictions, though some states issued no stay-at-home orders at all during those early months [30, 49, 81, 89].

Due to the lower infection rates over the summer, restrictions largely eased in Europe but had been re-implemented in many countries as of November in the form of nightly curfews, closures of non-essential businesses, travel restrictions, and mask-wearing and social-distancing mandates [6, 50, 58]. In November, restrictions in many US states were not as strict, with limitations but not bans on indoor activities (such as dining and shopping) and masks mandated in some but not all states [89].

2.2 Contact Tracing Technical Efforts and App Adoption

Here, we briefly overview existing contact tracing app efforts and their adoption as well as the conversation around how to contact-trace in a privacy-preserving way. The purpose of this section is to contextualize our findings and recommendations, not to give a comprehensive look at technology-enabled contact tracing efforts.

Why automated contact tracing? Traditionally, contact tracing is done by a team of public health experts and focuses on tracking down those who might have been infected by someone who tested positive for a disease, in combination with widespread testing. A state, region, or other entity might implement *automated* contact tracing (e.g., to augment or complement human-based efforts, for which there has been a shortage [68, 82]) for multiple reasons, although though not all experts agree that automated contact tracing is needed or will be effective. For example, automated contact tracing might be used to keep infection rates low while allowing people to leave their homes or used to enforce quarantine for people identified as COVID-19-positive.

Existing automated contact tracing programs. As of April 1, some governments had already deployed automated contact tracing programs using a variety of devices and data sources [96]. For example, contact tracing apps existed in Bahrain, China, Colombia, the Czech Republic, Ghana, India, Israel, the Republic of North Macedonia, Norway, Singapore, and some US states [5, 12, 16, 31, 35, 42, 44, 60–63, 90, 92]. Some apps were mandatory (e.g., in China), but most were optional (e.g., in Singapore) and struggled with low adoption [9]. Hong Kong deployed electronic wristbands to those infected with COVID-19 to ensure they did not leave their homes [77]. In South Korea, the government sent text messages with details about new COVID-19 cases and made available a central database with anonymized information; however, some entries were specific enough to be traced back to a single person and initiated damaging rumors [14, 51]. Additionally, Taiwan and Israel both began using cell tower data [35, 40].

On April 10, Google and Apple announced "*a joint effort to enable the use of Bluetooth technology to help governments and health agencies reduce the spread of the virus, with user privacy and security central to the design*" [32]. In May, they released the first version of their Exposure Notification API [7, 10, 23]. The API uses proximity tracking through Bluetooth, is opt-in, and can be used only by public health authorities; Apple and Google report that the data will not be monetized [7, 10]. In September, Apple and Google launched "Exposure Notification Express," allowing users to participate in contact tracing without downloading an app [23].

Since the release of Apple and Google's Exposure Notification API, many public health authorities have released apps using the API. According to the *MIT Technology Review* COVID Tracing Tracker [65], in November, 46 non-US countries were using automated contact tracing applications, 13 with Apple and Google's API, and 4 with DP-3T [91]. Additionally, at least 12 US states were using the Apple and Google API in November [74, 97]. Apps have been released steadily over time around the world, yet adoption remains low in most regions: Of the

apps for which the adoption rate is in the *MIT Technology Review*'s database, as of November, Iceland, Ireland, and Singapore had the highest voluntary adoption rates, at just below 40% of the population of each country [65]. Though automated contact tracing is more effective with more users, it can be effective at low rates of adoption as well [64].

Design decisions affecting security and privacy. Design properties at multiple levels affect user security and privacy, some of which are transparent to users (e.g., being potentially identified as infectious in some designs) and some of which are more opaque (e.g., broadcast vs. narrowcast; centralization vs. decentralization). For a more complete and in-depth discussion of these properties, see References [71, 93].

Some groups explicitly focus on privacy-respecting contact tracing. Each group makes design decisions based on its own threat models and on-the-ground situations, including Apple and Google, the **Massachusetts Institute of Technology (MIT)**, the **University of Washington (UW)**, PEPP-PT, Inria, and DP-3T [8, 32, 43, 75, 91]. One high-level distinction that has become extremely popular since our initial surveys in early April is *proximity tracking*, where a user's phone tracks other nearby phones, rather than a more traditional implementation of location-based contact tracing.

Additionally, other, non-smartphone methods are being used to trace contacts, such as credit card purchase history, facial recognition on surveillance camera footage, and wearable devices [41, 83, 84].

3 RELATED WORK

Other groups have also investigated public opinion on location tracking during COVID-19, described below.

Themes: Privacy concerns abound, but a majority indicate a willingness to download contact tracing apps. Many groups have assessed a population's willingness to download a contact tracing app, finding rates between 27% and 84% at different points in time, with different privacy and data sharing and usage situations and different populations, including Australia [20, 21, 29], China [55], a number of countries in Western Europe [1, 3, 34, 37, 45, 55, 67, 95, 98], and the US [1, 3, 4, 37, 38, 55, 59, 70, 88, 99]. These w orks identified concerns thematically similar to ours, such as privacy concerns about sharing with the government, and correlations between willingness to download and COVID-19 concern levels or demographic information, e.g., age.

Cross-cultural studies. Some groups have studied participants from multiple countries, including References [1, 3]. For example, Altmann et al. found that people in the US and Germany were less likely than people in France, Italy, and the UK to install a contact tracing app due to security and privacy concerns [3]. Kostka and Habich-Sobiegalla compared public acceptance of contact tracing apps in China, Germany, and the US; in line with Altmann et al., they find that participants in Germany and the US were much less accepting of an app than those in China [55].

Longitudinal studies. Garrett et al. are studying public opinion over time in several countries (including Australia, Germany, and the UK) by periodically surveying participants from those countries in "waves" [21]. In Australia, Garrett et al. have found widespread acceptance for contact tracing apps but lower download rates than were predicted by attitudes about contact tracing apps [29].

Situating our work. In the context of existing work, our work adds a *regular and periodic* survey of public opinion, capturing trends and stability over time. Additionally, the free response answers present in our data provide rich insight into the values and concerns underlying individuals' willingness to download, allowing them to express themselves in their own words in addition to via prescribed quantitative options.

4 METHODOLOGY

To collect rich data and measure public opinion, we designed an approximately 20-minute online survey with both multiple choice and free response questions. Our survey was implemented in Qualtrics. We deployed the survey through Prolific, an online survey platform based in the United Kingdom.

Our institution's IRB determined that our study was exempt from further human subjects review, and we adhered to best practices for ethical human subjects survey research, e.g., we paid at or slightly above minimum

wage, all questions were optional except the initial screening questions about age and smartphone usage, and we did not collect unnecessary personal information.

4.1 Survey Protocol

Because we expected most participants to live in countries where contact tracing apps were not in ubiquitous use, at least for our initial survey, we designed the survey to elicit attitudes about contact tracing in specific *hypothetical* situations. The survey did include branches for those who had already downloaded an app for tracking or mitigating COVID-19, or who had the opportunity to but chose not to, but in this article, *we focus on those who did not have a contact tracing app* at the time of inquiry. To avoid biasing participants towards presenting themselves as more privacy-conscious than they are, the survey did not mention "privacy" until its final two questions (demographics) and asked instead about participants' "comfort" with various situations or their "likelihood" of downloading an app in a certain situation. Each section (except for demographics) concluded with one or more free-response questions, inviting participants to explain their opinions.

When designing this survey in late March—and adding to it in response to the evolving world—we paid close attention to the ways that technology and terminology might change, opting to describe terms that may fall in or out of style (like "contact tracing" or "exposure notification") and prioritized longitudinal consistency by not editing questions after they had appeared once (other than to correct the rare typo). We expand on this experience of future-proofing a longitudinal survey during a rapidly evolving event in Section 6.

The survey had the following main sections (excluding questions for participants who were already using a contact tracing app). See Appendix A for the full protocol.

Demographics. We asked participants three types of demographic questions that focused variables we hypothesized might correlate with their attitude towards COVID-19 and contact tracing programs: (1) standard demographic questions, such as age, gender, geographic location; (2) general political views, news sources, and privacy and technology interest and knowledge; (3) COVID-19-specific questions, such as their general level of concern about the pandemic, whether they live with someone who is in a high-risk group, whether they had had COVID-19 or had ever been tested, and their beliefs about social distancing and mask wearing. We asked many of the demographic questions at the end of the survey to help mitigate stereotype threat.

Cell tower location data. We asked participants how comfortable they were with their cell phone manufacturer or cellular carrier using their location data for the purposes of studying or mitigating the spread of COVID-19. We presented participants with three variations of a situation: their location data being shared with their government; their location data being shared with their government if they tested positive; and their location data being shared publicly if they tested positive.

Existing apps using GPS location data. We asked participants to imagine that "the makers of an existing app on your phone started using your GPS location data to study or mitigate the spread of COVID-19." We chose 3 popular apps from each of 5 categories that we expected would use location data (navigation, social media, messaging, transportation, fitness), for a total of 15 apps. Participants rated their comfort level with each of the 15 apps using their location data for mitigating the spread of COVID-19 on a 5-point Likert scale, with an additional option for "I don't use this app." We then asked two free-response questions about the app that they regularly use that they would *most* trust and the app that they would *least* trust to study or mitigate COVID-19.

New app: perfect privacy. We asked participants to imagine a new app that would track their location for the purposes of mitigating the spread of COVID-19 but that would protect their data perfectly. On 5-point Likert scales, we asked how likely they would be to install the app and how it would change their current behavior.

New app: App makers know location at all times but do not share it. Changing the previous scenario slightly, we asked participants to imagine a new app that would know their location at all times for the purposes of mitigating the spread of COVID-19, but this time the app makers would know their location at all times but would not share this information. We again asked participants how likely they would be to download and use such an app. This time, we asked participants to rate their comfort with each company that made the same

popular 15 apps we showed them previously. We expanded this list to include other companies in week 3 of the survey. We also asked about their comfort level with five generic entities making such an app: a university research group, an activist group, an industry startup, your government, and the United Nations.

New app: App makers know location at all times and share data with your government if you are diagnosed with COVID-19. Again changing the previous scenarios, we asked participants about a situation in which the new app's makers share their location history with the government if they test positive for COVID-19. We asked, again, how likely they would be to download such an app as well as their download likelihood in two variant situations: if the data were shared regardless of whether they tested positive and if the government's use of the data were supervised by a judge.

Non-smartphone location data sources. In response to an evolving conversation about alternate data sources, we asked participants next about their comfort level with having location history derived from surveillance camera footage and credit card purchase history (added in week 3). Beginning in week 16, we also asked participants about their comfort with public area sensors or electronic bracelets.

New app: Proximity tracking. Due to the growing discussions about and technical work on proximity tracking protocols and apps after April 1, in week 3, we added a group of questions about proximity tracking. We asked about proximity tracking by phone manufacturers, phone operating systems, a new app, and apps from several well-known companies or generic entities.

Government use of location or proximity data. In this section, we stepped back from scenarios about specific data sources to ask participants questions about a scenario in which their government acquires their location or proximity data for studying and mitigating COVID-19. We asked about their confidence in their government's deletion of the data post-pandemic, use of data only for COVID-19 tracking, and their general level of concern about their "personal safety or the safety of those in their community."

Desired features in a new COVID-19 mitigation app. We then asked participants about a wide variety of features that a potential new COVID-19 mitigation app might have when notifying people of potential infections or enforcing isolation; features were drawn from existing contract tracing apps or programs. For example, one feature we asked about would "notify you if you came close to someone who later tested positive for COVID-19," while another would "automatically notify the authorities if people were not isolating as mandated."

Location sharing with their government pre-pandemic. Finally, we asked participants to rate their level of comfort with their location data being shared with their government in October 2019, i.e., before COVID-19. Since participants may not accurately recall their own previous beliefs or may have been primed towards privacy-sensitivity by the rest of the survey, any results from this data must be treated with caution.

4.2 Recruitment

We recruited participants through Prolific, an online survey platform, with no demographic restrictions, since Prolific already requires that all participants be 18 or older. The first questions of our survey screened participants as required by our IRB. We asked: (1) are you at least 18 years old? and (2) do you use a smartphone regularly? If participants answered "Yes" to both, then they proceeded to the rest of the survey.

We ran the survey on Prolific on April 1, 3, 8, 10, and every Friday thereafter until June 5, then every *other* Friday, around the same time (3pm PST). We excluded anyone who had taken any previous version of the survey.

4.3 Analysis

In this report, we present analyses of our qualitative and quantitative data. We conducted exploratory and descriptive statistical analysis of our quantitative data rather than testing specific hypotheses, described below.

Longitudinal analysis. To explore longitudinal trends, we present data with time on the x axis and the percent of participants on the y axis. We draw slopes that are statistically significant with $p <= .05$, a standard threshold for significance, but we observe that a statistically significant slope does not necessarily mean that the slope has practical significance. We calculate the statistical mean (μ) for each question.

Demographic analysis. For the questions that displayed longitudinal stability (the majority of the questions), we examined demographic trends by collapsing all weeks of data into one pool. We analyzed each question by: country or region, age bracket, gender, and phone manufacturer, including only demographic groups for which there were at least 100 participants.

Qualitative analysis. To understand participants' values and concerns more deeply, we conducted qualitative analysis of the optional free response questions accompanying many of the survey sections. To analyze these questions, two researchers iteratively created independent qualitative codebooks for each question, first open coding and then creating axial and hierarchical codes for each question. We opted to use separate codebooks for every question except questions that were variants to allow the themes from one question to arise independently from the themes in another. When reporting qualitative data, we report the number of participants for each theme, idea, or concept and attribute quotes to participants using an identifier with both the week and a participant number, e.g., W3P40 for participant 40 from week 3.[1]

4.4 Limitations

As Covid-19 quickly became prevalent outside China in March 2020, we tried to both develop a survey as quickly as possible to collect early data and to develop a survey whose questions and wordings would withstand a year of immense and unknowable change. In doing so, we made choices that contributed to both the strengths and weaknesses of this work. In the interest of consistency, we decided to never edit questions other than to fix typos. This decision allowed us to compare data across the entire year of our data collection, but it also means that we did not correct the survey's imperfections—either places where we accidentally did not adhere to survey best practices or places where the changing world led to potentially outdated terminology or questions.

Because of our commitment to consistency, we chose not to use the term "contact tracing" in the survey even after we perceived it became popular and commonplace, and instead described the relevant qualities of a contact tracing app (e.g., describing it as "*an app that tracks your location for the purposes of mitigating the spread of COVID-19*" for questions 50–52 (Appendix A.5)). This could have introduced confusion if participants thought we were talking about contact tracing but were confused because we did not use the term directly. However, most participants who answered that they have a contact tracing app (Q25) seem to have understood the question, so we estimate that the confusion was minimal (Section 5.2.3).

Another limitation of our work is that we did not randomize question or answer order, which can introduce bias [72]. Additionally, another limitation of a survey such as ours, in which participants are asked about different situations without being able to directly compare them, is that opinions about earlier questions may change given later questions [72].

Additionally, though we intentionally recruited from an international audience, our survey was in English, meaning that those who do not read English are not represented, and some with weaker English skills may have chosen not to complete the free response questions; this could lead to potential biases towards English speakers in the qualitative responses. Although we have an international sample, we did not recruit large numbers of participants from any individual country each week, so our data cannot be used to examine country-level trends *over time*. Additionally, some of our questions, e.g., Q69 and Q42, may be more suited towards a US audience, despite the low rate of US participants in our sample. Thus, answers to those questions should be interpreted with caution.

Prior work on Mechanical Turk participants in the United States, a different survey platform than ours, found, with varied results, that online survey participants may not be representative of the general population [76]. Other studies have examined whether online survey participants' security and privacy knowledge and behavior accurately represent the general public, with varying results [48, 73].

[1]Though each survey had 100 participants, some participant numbers may be greater than 100; we combine results from the two surveys in week 1, so there were 200 participants in week 1. Additionally, some weeks had a few participants who were screened out, causing us to recruit slightly more than 100 participants and causing some participant numbers to be greater than 100.

Finally, online surveys have inherent limitations. Participants may experience survey fatigue and click through long matrix questions, giving inaccurate answers to finish the survey more quickly. From our qualitative analysis, responses to free response questions seem to be on topic and high quality, indicating a low rate of survey fatigue. Survey fatigue, or lack thereof, may also be affected by the fact that participants were paid and therefore incentivized to finish.

5 RESULTS

We now report results from our analysis of both quantitative and qualitative data from weeks 1 (April 1, 2020) through 32 (November 6, 2020) of our survey. On week 1, we conducted two surveys (April 1 and April 3); for weeks 2–10 (through June 5), we surveyed participants once a week; for subsequent weeks, we surveyed every two weeks (hence, there is no data for weeks 11, 13, 15, etc.).

Our survey had two branches, one addressing those who had a contact tracing app and one addressing those who did not. In this article, we focus on the latter cohort, since they may share concerns and values we must understand to make it possible for them to (1) have safe access to automated contact tracing and (2) be able to make an informed decision about participating.

In Section 5.1, we describe our population demographically, finding that while our participants hail from dozens of countries, minority viewpoints may be absent. In Section 5.2, we consider estimates of a population's willingness to download a contact tracing app. We also consider how privacy concerns affect willingness. We find that while adoption of contact tracing applications *is* increasing, a significant minority of the population does not intend to use them and that privacy concerns are indeed a central concern, even among those who might download an app. We also consider functionality users might want from contact tracing apps, finding support for bare-bones tracing features but not for more privacy invasive ones, such as quarantine enforcement.

In Section 5.3, we examine values and concerns potential app users might share about tech companies, governments, or other entities that develop contact tracing apps. We observe that users have substantial concerns about their data being shared or used without their consent and for purposes that might harm them or others. We also find no one-size-fits-all app developer profile: Comfort with an app developer (e.g., Google or the US government) is a complex decision that differs for every user; therefore, policy makers, tech companies, researchers, governments, and public health experts must work together towards protecting users and helping users understand the protections in place so they can make informed decision. Finally, in Section 5.4, we more broadly explore user values and concerns through a discussion of alternative data sources for contact tracing, including cell tower location data, credit card history, public sensors (including surveillance cameras), and wearable electronics. Expanding upon themes from previous sections, we observe that anonymity and technical *accuracy* are of great concern to users, whose mental models may be incomplete or inaccurate.

Two notes on terminology: We use the term "contact tracing" to include "location tracking" and "proximity tracking." When reporting qualitative results, we use the format W1P100 to mean participant 100 from week 1. Further, our notation Q[N], where N is a number, refers to unique identifiers in the Qualtrics survey platform that we used. Question numbers do not appear strictly in order; we analyze questions in groups but encourage readers to refer to the full survey protocol in Appendix A if necessary. Finally, in longitudinal plots, we draw lines when statistically significant ($p \leq .05$) and show the average (μ) in the legend for all questions.

5.1 Participant Demographics: European, Male, White, and Young

Over the course of 20 surveys and 32 weeks, we reached **2,337 participants**, **mostly from Europe**. Countries with at least 10% of participants in our dataset are from the United Kingdom (22.4%), Portugal (15.9%), and Poland (14.6%). 9.9% of our participants were from United States. European countries (including the UK, Portugal, Poland, and 21 others) comprised 73% of total survey participants.

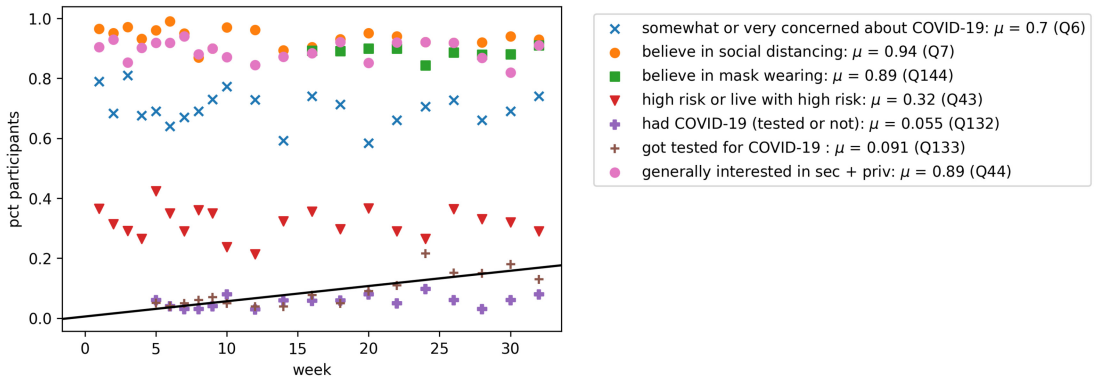


Fig. 2. This plot describes our participants' attitudes toward COVID-19 and preventative measures. Respondents have a generally high degree of belief in preventative measures, such as mask wearing and social distancing. The line at the bottom shows a statistically significant increase in the percent of participants who had been tested for COVID-19.

As is common in online surveys [76], participants were **overwhelmingly young**. Over 70% were under the age of 30; 54.9% between ages 18 and 24 (we screened out anyone younger than 18); 18.9% between 25 and 29; and 11.2% between 30 and 34, with a long tail to a highest age bracket of 70–74.

40.7% of participants who disclosed their gender were female; **58.1% were male**. Approximately 1% of participants disclosed that they were transgender, genderfluid, genderqueer, non-binary, or agender. We manually bucketed participants' gender identities as reported in a free response text field; we believe we have stayed true to participants' gender identities when bucketing, though these identities may change over time and our respondents may have included more trans or gender non-conforming participants than disclosed as such. To avoid stereotype threat, we asked most demographic questions at the end of the survey, asking only high-level questions about demographics (e.g., location) and COVID-19 at the start.

In week 12 (June 19), we began collecting data on race and ethnicity. Because race and ethnicity are complex and have different meanings throughout the world, we provided participants with a number of races or ethnicities commonly asked about in surveys [11, 28] and also offered a free response question if they wished to self-describe in addition to or instead of options we provided, as recommended by the EU [25]. Of these responses, **79.6% identified as white**, 13.5% as Hispanic or Latinx, 6.9% as Asian, 3.2% as Black or African-American, and less than 1% as American Indian, Alaskan Native, Pacific Islander, or Native Hawaiian. Percentages add up to more than 100, because some participants selected multiple identities. Those who chose to self-describe indicated both intersectional identities and European ethnicities, such as Slavic, Irish, and Scandinavian.

Though we have survey participants from a variety of countries, they are overwhelmingly young, white, and European. Thus, our survey is dominated by racial and ethnic majorities in the countries that we surveyed from and, thus, privacy concerns of those who we were unable to reach—**older adults, racial and ethnic minorities—are not well represented in our dataset.**

5.1.1 Participants Who Are Concerned about COVID-19 and Believe in Social Distancing and Mask Wearing. Figure 2 summarizes COVID-19-related demographic information about participants, revealing no statistically significant longitudinal trend other than a slight increase in those who were tested for COVID-19 (Q133, $p < .01$). However, our data reveal that our participants are generally concerned about COVID-19 ($\mu = 70\%$) and believe in social distancing ($\mu = 94\%$) and mask wearing ($\mu = 89\%$) as preventative measures for COVID-19. A sizeable minority are in a high risk category or living with someone who is ($\mu = 32\%$).

A report on public attitudes in the US towards mask wearing and other COVID-19 prevention measures found that mask wearing increased substantially between June and August in many regions of the US [56]. We do not

see such an increase in support for mask wearing in our data but do find support for such measures similar to higher numbers from Reference [56]; the lack of trend in our data may be explained by our smaller and Euro-centric population. A May 2020 CDC report found that those surveyed in Los Angeles and New York City overwhelmingly supported mask wearing and social-distancing measures [17], with numbers similar to our results. However, as revealed in Reference [56], many US regions showed limited support for mask wearing and other measures: These views are not represented in our data, so our findings must be interpreted carefully to consider those who we did not reach.

5.2 Expectations about App Functionality, Data Sharing, and Technical Implementation Suggest Privacy and Accuracy Concerns Influence Users' Willingness to Download Contact Tracing Apps

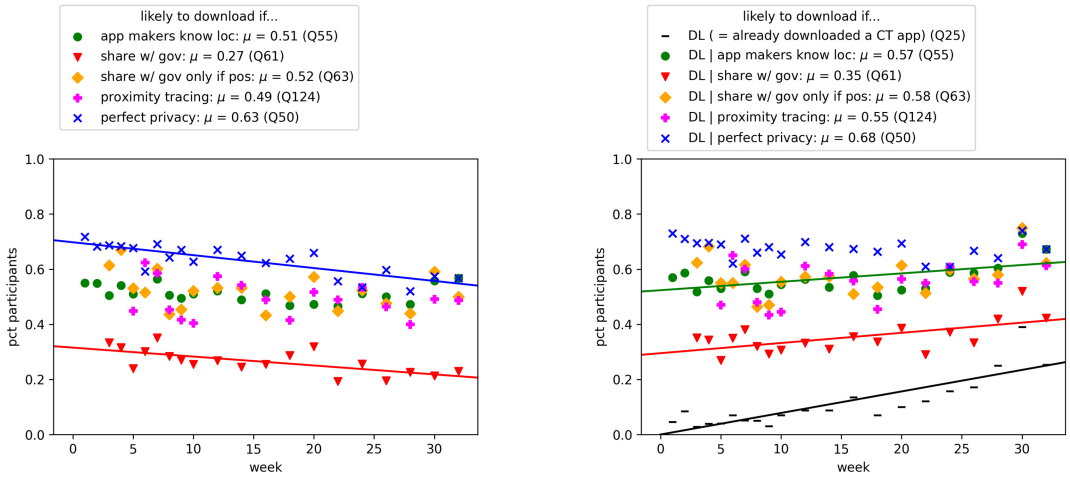
We now ask what proportion of our population might be willing to download a contact tracing application and what concerns or values they might have about what the app does. Estimating the number of people willing to download under *some* circumstances is critical to finding the best-case success of voluntarily downloaded contact tracing applications. Understanding potential users' concerns and values will help app makers and public health experts in ongoing efforts to tailor policy, technology, and public awareness campaigns towards reaching global critical mass usage of automated contact tracing. We find that:

- The upper bound of people willing to download a contact tracing app remains roughly constant over time, but potential **users may be becoming more willing to accept an app that does not have perfect privacy** (i.e., an app that shares data under some circumstances) (Sections 5.2.1 and 5.2.3).
- When comparing contact tracing apps that use location tracking (GPS) and proximity tracking (Bluetooth), participants considered both **expected technical accuracy** and **privacy concerns** (Section 5.2.4).
- Participants value a contact tracing app that **notifies them (or others) if they have been exposed to COVID-19, but not an app that would enforce isolation or quarantine** (e.g., Reference [52]), citing concerns about algorithmic inaccuracy and equity. In qualitative results, participants organically suggested *informational* features, such as regional guidelines or medical advice, perhaps revealing a lack of reliable information about COVID-19 or an unmet desire for a unified or official source (Sections 5.2.5).

5.2.1 Not Everyone Intends to Download a Contact Tracing App; Data Sharing Concerns Reduce Likelihood to Download. Figure 3(a) shows that even if a contract tracing app were to "protect your data perfectly," a significant minority of those who have not yet downloaded an app do not intend to voluntarily do so. Approximately 63% said they would be somewhat or extremely likely to download a contact tracing app with perfect privacy, while many fewer would download an app that shared their location with their government (μ = 27%). Of those who had not yet downloaded an app, participants showed no significant preference between an app for which the app makers have access to location (Q55), an app for which the developers share data for those who test positive with the government (Q63), or proximity tracking (Q124), all around 50%.

5.2.2 Concerns about Sharing Data with the Government Limits Willingness to Download; Users May Be More Likely to Share Data If They Test Positive for COVID-19. Participants were more comfortable with an app that would share location data only from users that tested positive (μ = 52%) than one that would share location data from all users (μ = 27%). This difference in comfort reveals that participants have strong concerns about sharing location data with their government and that those concerns may limit their willingness to download a contact tracing app. This difference in opinion also raises questions about participants' mental models of the mechanics of contact tracing—who do they believe is conducting contact tracing?—as well as their views of government data usage (explored further in Section 5.3).

More broadly, these results suggest that those who test positive for COVID-19 may be more likely to cede some privacy. W1P194 wrote: "*If I were to be tested positive for the virus, I would definitely sacrifice some of my*



(a) This graph addresses the question: what kind of app are those who do not already have a contact tracing app willing to download? One might expect this sector of the population—a shrinking portion—to become proportionally more privacy-conscious over time since those who are less privacy-conscious may download an app voluntarily.

(b) This graph addresses the question: What percent of the population as a whole might have a contact tracing app in the future? (i.e., each colored point is the sum of those who already have a contact tracing app and those who might be willing to download one.)

Fig. 3. The percent of respondents who indicated that they would be somewhat or extremely likely to download an app that tracked their location or proximity to others "for the sake of tracking or mitigating COVID-19. The left plot (a) shows *only the participants who do not have a contact tracing application.* The right plot (b) shows ***all*** *participants: Each colored point is the* ***sum*** *of those who already have a contact tracing app and those who said they would be somewhat or extremely likely to download one.*

privacy to the government if it means protecting others. However I'm conflicted on the thought of sharing this data with the government if I am healthy." W6P58 said: "*I don't want the government to track my location. However, if I tested positive for Covid-19 I understand why it would be necessary so I would reluctantly accept it in that case.*"

5.2.3 Not Everyone Will Voluntarily Download a Contact Tracing App. In Figure 3(b), we add to Figure 3(a)—the participants who have already downloaded a contact tracing app—to ask a subtly different question: What percentage of the entire population might have a contact tracing app in the future? We observe, first, that the percent of our participants who have downloaded a contact tracing application is steadily, and significantly, increasing over time ($p < .01$), from less than 5% in week 1 to almost 25% in week 32[2]). By adding the data from Figure 3(a) on top of the participants who already have a contact tracing app, we find that approximately 68% of our participants have either already downloaded a contact tracing application or would be willing to download one under certain circumstances (including "an app that protects your data perfectly").

Estimates vary on how much of a population needs to participate in contact tracing for it to halt the pandemic, but recent work suggests a rate of around 60% [22, 26] to 70% [39], though Reference [26] shows that automated contact tracing at any rate will slow the pandemic.

[2]Some participants may have misunderstood the question asking whether they had a contact tracing application and answered "Yes" when they did not have an app. In a cursory estimate, we find that about 10%–15% of participants wrote mainstream apps like "Google maps" instead of a contact tracing app; however, here, we count *all* "yes" answers because it is possible that the participants who answered incorrectly *believe* that they have a contact tracing app, given that the incorrect apps are still likely to ask for location or Bluetooth permissions.

Our data show that even in the best possible privacy situation, with "an app that protects your data perfectly" (Q50), many participants have reservations about using an app to study or mitigate COVID-19. Results from other surveys about the same topic have shown a willingness to download ranging from 27% to 84%, depending on the population and exact situations presented. The wide range of willingnesses in related work suggests that further work is necessary to examine the differences between the populations studied and the exact situations presented.

5.2.4 From Participants' Perspectives, Location Tracking Presents Privacy and Security Concerns that Proximity Does Not; Participants Also Reasoned about Equity and Technical Accuracy. Participants did not exhibit a strong preference for proximity tracking over two other forms of location tracking in our quantitative data (Figure 3), potentially due to bias inherent with question ordering, since location tracking situations were presented first. However, qualitative data reveals underlying privacy concerns about location tracking compared to proximity tracking, as well as concerns about privacy and efficacy of proximity tracking itself. We also find that inaccurate mental models of technology and contact tracing drive individuals' concerns, values, and willingness to download.

Participants have technical security concerns with proximity tracking. Proximity tracking evoked security concerns, with participants specifically concerned about anonymity and the security risks of their phone communicating directly with others': "*I don't want the phones to be sharing information between them because it could be easy for a hacker to violate multiple phones privacy*" (W6P74). W16P59 imagined a scenario in which tracing close contacts instead of location might put political dissidents at risk: "*Again, there are MANY people for whom this would simply not be safe if our current government had that information. Identify, say, one person at a protest. Get the info of EVERY phone that came within 6 feet of them on that day, or in that timeframe, and suddenly a LOT of people are at risk that had not been identified, and most often had done nothing wrong.*" Though these scenarios raise questions about the accuracy of participants' mental models of proximity tracking, they reveal that participants' concerns about the technical safety of a contact tracing method drive their willingness to enroll in automated contact tracing initiatives. Additionally, recent work has shown that many contact tracing apps have suboptimal privacy and security properties [80, 87, 94], so even if participant' mental models were inaccurate, their fears were not unfounded.

Qualitative data shows fewer privacy concerns with proximity tracking than with location tracking. Despite their concerns about privacy, 98 participants wrote a response that indicated they preferred proximity tracking, while only 13 preferred location. 18 indicated that it depended on who ran the service. Those who preferred proximity tracking considered it less invasive than location tracking. W9P100 brought up concerns about contact tracing data being shared with both companies and their government, and reasoned that proximity data better preserved their privacy: "*Proximity will probably be easier to swallow than location. There's something fundamentally unsettling about companies/my government having a record of everywhere I've gone, for how long I stayed there, etc. Knowing who I've passed on the street or purchased a burrito from, but not precisely where I passed them or exactly when I bought the burrito would be much less uncomfortable.*"

Participants reasoned about accuracy and effectiveness of both location tracking and proximity tracking. This reasoning revealed inaccurate mental models, e.g., "*I think that proximity tracking is more effective. . .as it would. . .be able to alert others and possibly stop them further spreading it, whereas location tracking would only really give an insight into where the virus is spreading*" (W6P23). Taking the opposite stance, W9P46 wrote: "*This method [proximity] appears to be better in a user data protection sense. But it does not provide the same benefits to the government that location data would. Location data enables lockdown and focus on specific areas with recent outbreaks.*" Other participants were concerned about proximity tracking not capturing surface transmission: "*There is also some evidence about catching from surfaces that others have touched, so location tracking may also be relevant*" (W14P67). Regardless of the accuracy of participants' mental models—both about the mechanics of automated contact tracing and about virus transmission—their concerns about efficacy reveal that they value

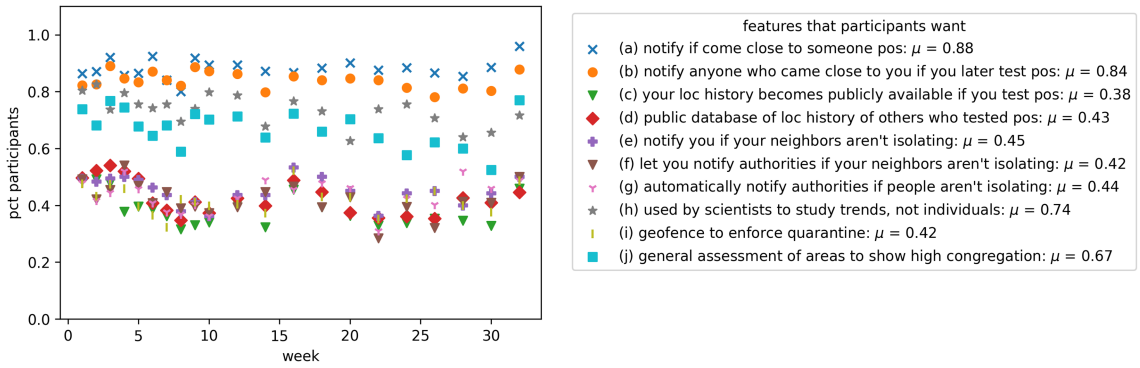


Fig. 4. Features desired by participants in a COVID-19 tracking app (Q72).

a technology that they believe can *accurately* conduct automated contact tracing and that their views of what technology is most likely to produce accurate contact tracing results will play into their decision to download.

5.2.5 Participants Desire Bare-bones Contact Tracing and Informational Features, Not an App that Might Enforce Quarantine or Reveal Personal Information. The features or functionality of an app may also influence how many people are willing to download it. Participants responded positively to 4 of the 10 potential app features,[3] shown in Figure 4: They desire contact tracing notifications (a, b) (μ = 88%, 84%) and general reports on trends (h, j) (μ = 74%, 67%). All other potential features received less than 50% support.

In qualitative responses (Q74), 106 participants indicated support for informational features, with 44 desiring general information such as news and safety guidelines and 62 expressing interest in location-specific resources such as information about nearby hospitals. W6P97 suggested that "*it would be useful to have a hotline or chat where you could be evaluated and diagnosed,*" and W1P54 thought it would be useful for a contact tracing app to "*provide national announcements and guidelines so that people get them in a clear, uniform fashion.*" Thirty-one participants also expanded upon (j), expressing support for an app that shows COVID-19 hotspots, and 39 supported the options to notify (or be notified) if in contact with a positive case (a, b). Participants' desire for an *informative* app raises the question of whether access to reliable information about COVID-19 is an issue.

Concerns about security, privacy, equity, and access also arose. Forty-one participants mentioned anonymity, specifically bringing up stalking, harassment, and other forms of app abuse. Participants also reiterated their desire for health information to be shared with scientists, health professionals, and family, but not with the public. Though 16 participants wanted enforcement of rules to keep themselves or others safe, others were strongly opposed to this idea, citing concerns about fairness: "*I would prefer it to only inform and not gather any data or contact any law enforcers because everyone has their own circumstances and there might be people who cannot be on quarantine because of being not wealthy enough.*" (W6P53). W14P75 noted that developers must be mindful of resource consumption and backwards compatibility lest they risk excluding people, since "*not all of us have the privilege of having the latest models.*"

5.3 App Developer Identity Matters: (Mis)trust in Government and Some Companies

We next more deeply investigate the privacy concerns revealed in Section 5.2 by exploring participants' trust in both government agencies and well-known tech companies. We find that:

- **Participants trust companies they perceive to be competent and resource-rich** (Section 5.3.1). In both qualitative and quantitative responses, participants indicated trust for Google over other companies.

[3] All features were drawn from existing or proposed designs as of April 1, 2020.

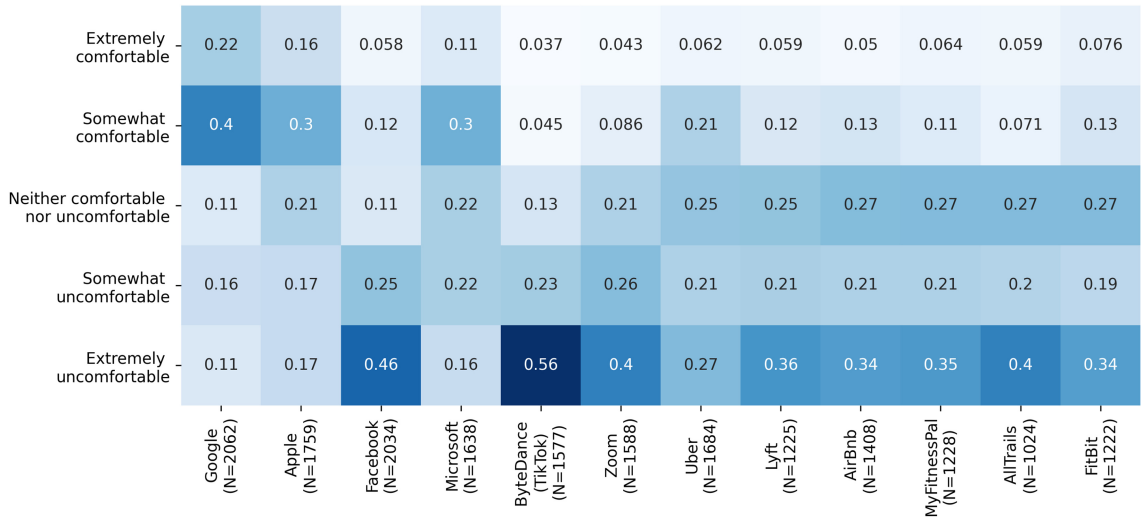


Fig. 5. Participant comfort with a known company creating a *new* app using their location to study or mitigate COVID-19 (Q56). Due to longitudinal stability of the data, we combine all data here to show nuances in opinion. Columns sum to one and represent only participants who responded to the question and did not choose the option "I do not know enough about this company to make a decision."

- When weighing pros and cons of generic entities (e.g., government, university researchers) that might create a contact tracing app, participants go through a **complex decision process**, with no entity preferred by all and both positives and negatives about each of the entities we presented (Section 5.3.2).
- Participants conveyed substantial **mistrust in their government** (as a generic entity) conducting contact tracing, but displayed more trust in government health agencies and, in some circumstances, judicial oversight of government (Section 5.3.3).

5.3.1 Participants Prefer Large, Known, Already-trusted Tech Companies over Other Tech Companies. Our survey asked both about a known company adding contract tracing to an *existing* app vs. creating a *new* app to trace contacts. Though these situations require subtly different threat modeling, the results were similar; here, we present numbers from the question about a *new* app, since that more closely reflects today's reality.

Participants indicated trust in large tech companies that have a good reputation concerning security and privacy and that they perceive to be capable of conducting contact tracing. More participants indicated comfort with Google or Google products than with any other company (μ = 62% comfortable), as shown in Figure 5. Participants also indicated some comfort with Microsoft and Apple (μ = 41% and 46% comfortable, respectively), as shown in Figure 5. Less than 30% of participants indicated comfort with all other companies. Participants displayed the least comfort with ByteDance (TikTok) (μ = 79% uncomfortable) and Facebook (μ = 71% uncomfortable).

Qualitative analysis results reveals themes around user values and concerns regarding what apps they would trust most (Q23) and least (Q24) to use their location data for COVID-19 tracking. In line with the quantitative results reported above, 1,205 users picked Google Maps or another Google app as their most trusted app, and 431 picked Facebook as their least-trusted app in the context of using location data for COVID-19 tracking. Reasons for picking their most-trusted app or for not picking their least-trusted app include the following:

Pre-existing technical capabilities, user base, and resources. Participants value a company that already has a large user base, sufficient monetary resources to add contact tracing to its capabilities, and the technical resources to implement accurate contact tracing (from participants' perspectives). W2P60 wrote: "*I would trust*

Google maps because it shows the most accurate current location real-time. I believe Google maps has the resources and manpower to allocate where I've been and when, I trust a more accurate and informational app. I imagine an app such as Instagram would be inaccurate because anyone can pick a location when they post a picture."

Some participants preferred an app in which location tracking is already central to its purposes (e.g., Google Maps, fitness apps, Uber, Snapchat, Pokemon Go), which they believed was a sign of technical capability to conduct contact tracing via location tracking. W8P77 explained, "*I would trust Google Maps or Apple Maps the most. Mainly because the app is made to track your location. Other apps for things like social media don't necessarily consider location as a huge factor of the app so I would feel more comfortable using an app that already tracks your location to determining spread of COVID-19.*" Others trusted a mapping app additionally because it was *not* social media and therefore maintained a degree of anonymity: *"Google Maps because it does get the location access, but not more of my personal data like instagram or facebook etc, where all my contacts and photos are"* (W2P151).

Already use and trust the app. Participants value an app that they already know and trust either because they feel like they understand the app's data sharing and privacy procedures or because they have already ceded privacy to that app: "*Waze, it uses my data anyway so why not*" (W1P125), and W3P3: "*I am . . . locked in Apple's ecosystem, so they likely have all the data about me anyways.*" W4P17 clarified that it was less about trust and more about risk management: "*not necesarily (sic) trust, but resignation- I know Google and Waze already know my whereabouts and am resigned to them having my data.*"

Positive history and reputation with respect to security and privacy. Participants preferred a company known for protecting user data and making secure and private apps. W14P85 wrote: "*I would probably trust google maps the most since most of the other apps are known to be susceptible to data breaches/leaks in the past.*" W16P93 commented: "*I trust banking applications the most, because storing money is a serious matter,*" while W14P43 wrote that they trusted WhatsApp the most "*as I know it's encrypted and is very hard for mallicious (sic) hackers to break into to find my data.*" However, W1P75 wrote that they would not trust Facebook, because "*Facebook is notorious for selling user data to third parties, and I would be very uncomfortable to know that they are tracking my location with the purpose of researching COVID-19.*" Fourteen participants wrote that they would not trust an app developed in China, e.g., TikTok: "*TikTok because I heard it sends user data to China*" (W2P140).

Participants also considered privacy policies: W5P91 preferred Apple because "*Apple have a reliable privacy policy and therefore I would trust this the most as I don't believe any of my data would become public without my permission.*"

Company-agnostic concerns about privacy and personal harm. Participants also mentioned concerns that extend to any contact tracing program and reflect broader themes throughout this survey: (a) stalking or personal harm due to poorly anonymized data, (b) data leakage or privacy breaches, (c) data being sold by the company, and (d) a "slippery slope," in which this sort of tracking eventually becomes the norm.

5.3.2 Mixed Trust Levels for Non-corporate Generic Entities. Stepping back, we asked for participants' comfort with *other* types of entities developing a contact tracing app. Participants indicated general mistrust for a potential new COVID-19-tracking app created by an industry startup (μ = 21% comfortable) or an activist group (μ = 24% comfortable), as shown in Figure 6, but were largely split on generic trust for a government- or United Nations-developed app. Responses indicate the most would place trust in a university-developed app (72% comfortable), but we note that at the beginning of the survey, participants were shown our university's logo and told that this survey was an academic endeavor, which may have caused response or selection bias [19]. In contrast, Hargattai and Redmiles found that universities would be one of the least trusted entities, at less than 10%, while a survey by the *Washington Post* and the University of Maryland found they were relatively trusted, at 57%. This discrepancy highlights the need for multiple surveys and qualitative data to better understand the nuances of public opinion.

Qualitative data revealed nuanced decisions around trust of a company or entity, echoing themes of general reputation and ability to both technically conduct contact tracing and protect data, while adding in participants'

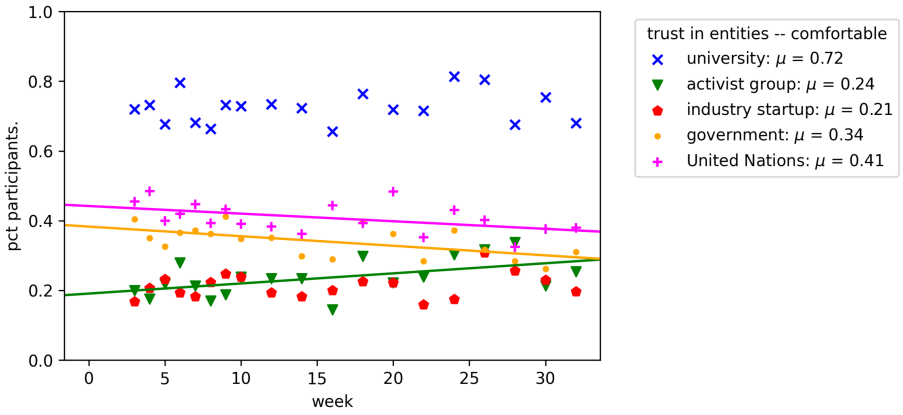


Fig. 6. Participants' trust in generic entities (Q126). The higher reported trust in universities could be due to response or selection bias, as participants were shown the logo of our university before beginning the survey.

beliefs about the *intentions* of a given entity. As such, 86 wrote that they would trust an app developed by scientists, universities, or researchers over any other entity.

Participants argued both for and against the entities in Figure 6, revealing complex and individual decisions. Generally, participants indicated that trust depended on an entity's (a) intent to share or sell data, (b) anonymity or privacy guarantees, (c) reputation with respect to privacy and security, and (d) commitment to transparency and consent. Some expressed a desire for a regulatory body or for open source apps.

Some would support a tech startup, because there is "*less notoriety attached to the brand*" (W9P55) and because they do not already have *other* data about the users; others would trust a big company because of its resources, credibility, and stability. Some participants considered activists unstable, unreliable, not credible, and incapable of actually securing data properly, while others valued activists groups' purer intentions, i.e., they believed that activists groups, unlike tech companies, would not sell the data on principle.

Participants who wrote about the UN mentioned its power and resources, but its international status was a plus for some (due to mistrust of their own government and not believing the UN would sell their data) and a minus for others (who disagreed with past UN work or believed the UN would be unable to produce a solution that worked for every country). W6P74 wrote in favor of the UN: "*If an International Organization such as the United Nations built the app and manages it, I will be more comfortable using the app "because is a superior force" than a government whom can use my data for electoral purposes or a company whom can use my data for profit.*"

Participants also raised several *positives* that they would expect from a government-developed app compared to other entities: Governments cannot profit off the data, can keep companies in check through policy, and have a degree of legitimacy. W8P50 wrote in support of technical and regulatory transparency: "*I would feel most comfortable if the app was open sourced for the public to be able to scrutinize, by a government agency to remove any profit motivation to misuse the data, and would feel most comfortable if the data was stored in aggregate rather than individual tracking (no data as to where I personally am at a certain time, but rather on a population level what % are at home, near other app users, etc.).*"

5.3.3 Trust in Government Health Agencies; Mistrust for "The Government" as a Whole, with Strong Concerns about Proper Data Use and Sharing. We find that participants are more comfortable sharing location or proximity data with governmental health agencies (as opposed to other sectors of government), and that more participants are comfortable with their location or proximity data being shared with their government only if they test positive for COVID-19, echoing trends from Section 5.2 and reemphasizing the need to protect the privacy of those

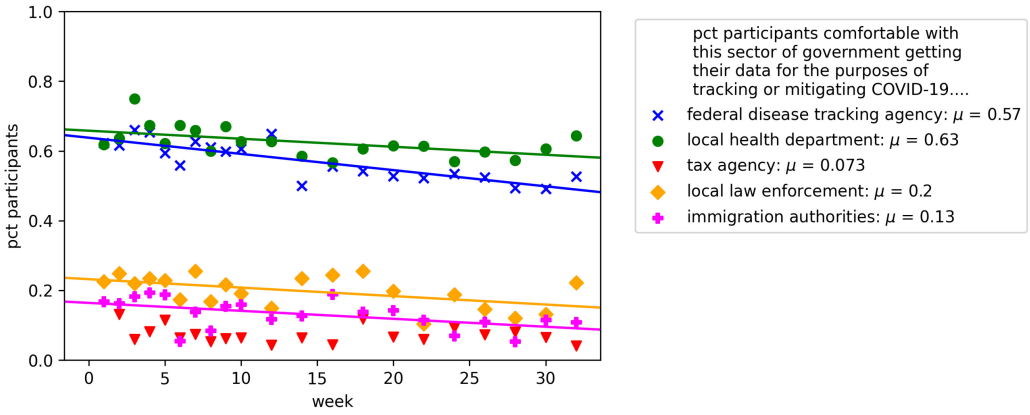


Fig. 7. Participants' comfort with specific government agencies receiving their location or proximity data for the purposes of contact tracing (Q69).

who test positive. We find no strong regional trends concerning trust in government, as noted in Section 5.5, but other surveys have addressed this question more thoroughly, e.g., References [3, 29, 55].

Participants indicated significantly higher comfort with their data being shared with health agencies for contact tracing (in line with Reference [73]), as shown in Figure 7 than with other government agencies. More participants were comfortable with both federal and local health departments (μ = 57% federal; μ = 63% local). Many fewer participants were comfortable with other agencies, i.e., local law enforcement (μ = 20%), immigration authorities (μ = 14%), and a tax agency (μ = 7.3%).

Concerns about data overuse and data sharing. Participants indicated substantial concerns about their government's use of data and about non-consensual data sharing with or within their government. Sixty-five participants believed that the benefits of sharing location or proximity data with their government, especially with local or national health departments, would outweigh any negatives. Of those, 39 imagined restrictions on governmental data use and retention, such as that their government should delete the data after the pandemic. Thirty-six wrote that sharing should be voluntary, and 27 said the US government should not share the data with **Immigration and Customs Enforcement (ICE)**. However, quantitative data indicates a lack of trust that their government would use its citizens' location data conservatively: 72% responded that it was unlikely that their government would delete the data (Q66), and 69% said it was unlikely that their government would use it only for COVID-19 tracking (Q67).

Participants also indicated concern that such data sharing or collection would be harmful to their safety or the safety of those in their community (Q68), with 65% responding that they were extremely or somewhat concerned. W6P58 wrote: "*There is no chance they're going to only use it for Covid, especially in the states, and it could be very dangerous for many people, especially marginalized groups.*"

Mixed trust for judicial oversight of data sharing and use. We observe a clear preference for judicial supervision if data is shared from users regardless of health status, and no preference if data is shared only from COVID-19 positive users, as shown in Figure 8. We also observe that participants' perceptions of judicial oversight is grounded in their mental model of their judicial system and government; thus, overestimations of the level of corruption or self-interest in the judiciary could skew trust and affect decision making.

Despite this preference for judicial supervision and the increase in willingness to share if positive, 220 participants were overwhelmingly negative about judicial supervision in qualitative data, citing general concerns about not trusting their government, concerns about data sharing or usage for another purpose (142), as well as concerns about judicial impartiality (17) and tech literacy of judges (7). W30P50 (UK) wrote: "*No, judges can often*

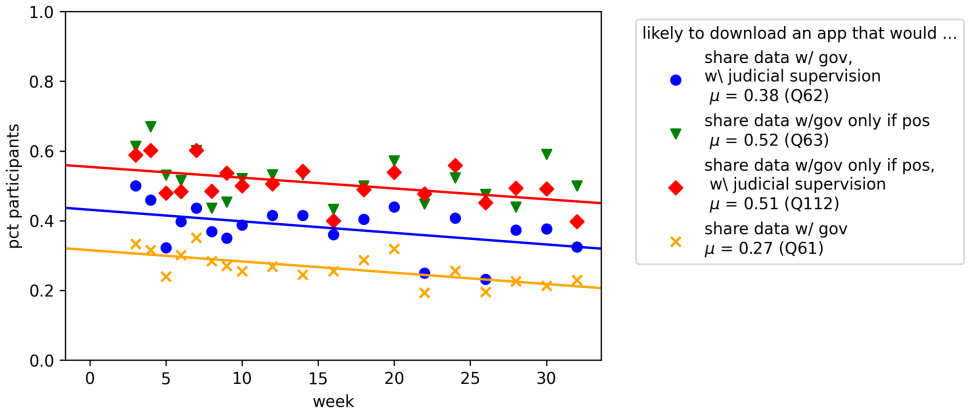


Fig. 8. Participants' self-reported likelihood to download an app that shares their location data with their government under various conditions—sharing only when positive and with judicial supervision of the government's use of data. This plot shows only those who have *not* already downloaded a contact tracing app (unlike Figure 3).

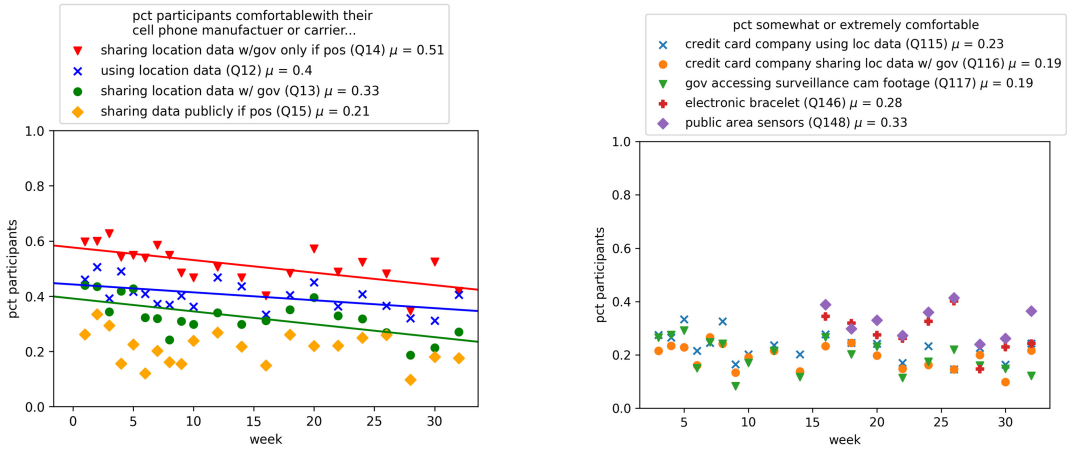
be influenced by and working in a corrupt way with the government," and W28P76 (Poland) brought up bias and harm that could be introduced or exacerbated: "*I'm a member of a minority that our government doesn't like at this moment. I am extremely wary.*" Other participants felt negatively because they did not believe the judges would make the right decisions: "*The judges here in Canada suck, and can't be trusted to deal out justice properly. We have a revolving door justice system for criminals—what makes you think they'd do any better when things aren't as clear cut as criminal cases?*" (W22P88).

Participants commented on judges' digital literacy, citing that "*government officials, globally, seem to have a high rate of technology illiteracy*" (W14P83, Ireland). Instead, one participant suggested that there be "*data watchdogs and possibly even a human rights person*" (W18P98, Slovenia).

Some participants who were concerned about judicial impartiality actually desired oversight, but thought it would not be possible in their country due to corrupt or politically motivated judges: "*Would be more influenced if observed by an independent party not affiliated with the government or partners*" (W24P89, UK). W22P55 (US) wrote: "*Judicial oversight is a good starting point. But with the current administration, I feel like trust in the judicial system has been slowly getting eroded.*" Alluding to different levels of trust, understanding, and different political systems, W26P89 (Chile) wrote that "*Judges in my country are not really that much better than politicians....*"

Despite many concerns about corruption, politicization, and bias, some participants did present positive values, including already trusting the judicial system and/or their government (115) or judicial oversight being better than none (24). W28P11 (UK) felt that judicial oversight would prevent corruption, instead of enabling it; they wrote that judicial oversight "*should prevent abuse of power.*" W26P71 (Portugal) wrote: "*I think judicial oversight of apps should be more common.*" Additionally, themes of consent arose (27) along with the idea that such oversight is already occurring (21). Echoing themes from Section 5.2, 32 participants reiterated that their government should have access to their location data only if they actually tested positive for COVID-19.

This combination of qualitative and quantitative data tells a complex story about participants' trust in their governments, including trust in the legal system, as well as their understanding of how both judicial oversight and contact tracing operate. It also reflects the seemingly directly competing values of privacy and altruism that push people towards not sharing data and pull them towards sharing it for the common good. Again, participants' mental models of the mechanism in question here, the judicial system, may be inaccurate or incomplete, but still drive their willingness to participate in automated contact tracing. Additionally, political and judicial systems differ across the globe, and judicial oversight may be appropriate in some countries and not others.



(a) Attitudes towards cell tower location data being used for COVID-19 tracking: participants who said they were somewhat or extremely comfortable with their cell phone manufacturer or carrier using their location data for the purposes of COVID-19 tracking.

(b) Attitudes towards other data sources: participants who said they were somewhat or extremely comfortable with electronic wearables, public sensors, surveillance cameras, or credit card data being used for contact tracing.

Fig. 9. Participants' attitudes about cell tower data and other data sources.

5.4 Mixed Attitudes about Alternate Data Sources

We now review participants' opinions about data sources *other than* smartphone apps: cell tower location data, credit card history data, public sensors (including surveillance cameras), and electronic wearables. We find that:

- There is **more support for contact tracing using cell tower location data than for the other non-app data sources** we asked about.
- Many of the concerns and values about smartphone contact tracing are magnified with non-smartphone automated contact tracing. Specifically, we observe that **consent for data collection, use, and sharing is extremely important to participants**, and particularly relevant to these non-smartphone data sources, which can largely occur without the user's informed consent. We call on the stakeholders in power to critically examine the need for consent beyond a terms of service agreement.

5.4.1 Support for Cell Tower Data over Other Data Sources. Regarding comfort with cell tower data being used for contact tracing, participants were most comfortable with their government being given the data if they tested positive, and many fewer were comfortable with the data being released publicly, as shown in Figure 9(a). This preference resembles the increase comfort with data sharing *if positive* (Figures 3 and 8, Sections 5.2 and 5.3).

We observe statistically significant but slight downward slopes for three of the questions, and we note that the order of participants' comfort is largely consistent across weeks: The most participants were comfortable with their cell phone manufacturer or carrier sharing data with their government if they are positive (μ = 51%), and the fewest were comfortable with their location history being shared publicly if they tested positive (μ = 21%). This sentiment of being uncomfortable with public disclosure more generally underscores the importance of contact tracing data being properly protected when and if collected to avoid data exposure were a breach to occur.

As shown in Figure 9, participants were much less comfortable with their credit card history being used for contact tracing: μ = 23% comfortable with contact tracing done by the credit card company, and μ = 19% comfortable with that data going to their government. Participants were generally uncomfortable with their government

using footage from surveillance cameras or other public area sensors for contact tracing (μ = 19% comfortable with surveillance cameras and μ = 33% comfortable with public area sensors) as well as with electronic bracelets (μ = 28%). We find no significant longitudinal trends.

5.4.2 Qualitative Data Reveals Privacy Concerns and the Need for Informed Consent. Through the qualitative data, we find similar thematic concerns as from Section 5.3 about privacy, data sharing, surveillance, equity, accuracy. Participants also reiterate the need for meaningful consent and transparency. We emphasize, again, that there is no perfect data source, and that users will likely have privacy concerns about any potential source. As such, the technology and policy communities must assume responsibility for protecting and informing users about personal data acquisition and use.

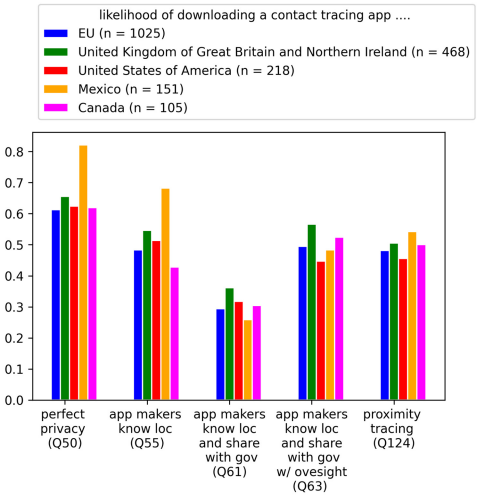
Concerns about privacy, anonymity, and data sharing regarding alternate data sources. Privacy and anonymity were of paramount concern, especially with regard to public sensors and cell tower data, with many mentioning a "surveillance state." Eighty-eight participants wrote that the use of cell tower data for contact tracing could be a "slippery slope" towards more permanent privacy invasion or other misuse of data. Thirty-one specifically referenced George Orwell's *1984* in reference to contact tracing data from surveillance cameras. W3P122 wrote: "*I'm very against expanding the surveillance state, even for a good reason, because it's never going to get rolled back.*" Sixty-seven participants were also uncomfortable with the idea of wearable electronics, with 22 specifically associating it with feeling like a "criminal," "prisoner," or "animal."

One-hundred and thirty-two participants had concerns about the privacy of cell tower data, focused on the data being publicized or shared with their government (see Figure 9(a)); 68 of those specifically mentioned anonymity as a value. In responses about using credit card data, 53 specifically considered the sensitive nature of financial data. Some participants considered credit card data less private because it "*gives only a handful of specific locations, and not a complete timeline of every location like a phone would*" (W16P59), while others mentioned a mistrust of financial institutions ("*Credit card companies are not customer friendly and are always behind monetary benefits therefore I would not like them to have my data and trust them*" W3P20). These responses also suggest that participants' mental models of the privacy of their credit card history is that location tracking would involve revealing their purchase history, which may be inaccurate.

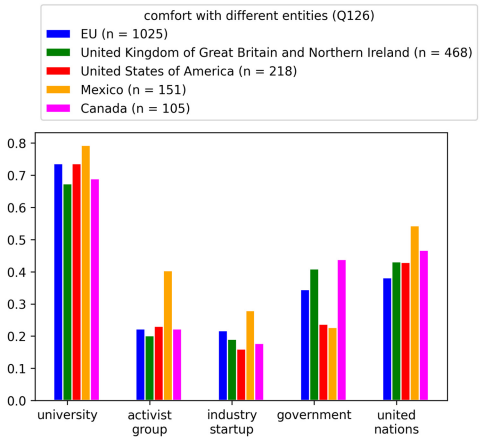
Concerns about equity, discrimination, and personal harm regarding alternate data sources. Participants raised concerns about the potential for discrimination, harm, and equity, echoing concerns from privacy experts [85] and emphasizing the need for technologists and policy makers to take extraordinary and thorough measures to protect potentially vulnerable populations. Seventeen participants feared harassment, prosecution, or discrimination with the use of cell tower data: "*if the location of people that has tested positive for COVID-19 is publicly shared, they might get targeted and hurt (or worse). This last idea comes from the fact that this was a situation given in my country, where it was publicly shared that a group of immigrants was tested positive, and this lead to them being persecuted*" (W16P98, Chile). Another participant mentioned the concern "*that people would would draw conclusions from (for example) two people being at the same hotel at the same time*" (W20P89). This situation is reminiscent of South Korea's initial handling of location tracking: location data and biographical details were posted publicly and were not sufficiently anonymized; groups discovered the identities of those who had tested positive and rumors started about extramarital affairs and plastic surgery trips [53]. South Korea has since started anonymizing the publicly released data more thoroughly [84].

Speaking to a theme of equity, some participants wrote that contact tracing using credit card data would be ineffective because "*credit cards are only for the elite*" (W3P33, South Africa). W3P63 extrapolated further, raising concerns about the potential societal implications of health information being linked to financial status: "*I fear this will lead to access to credit and my credit score being linked to my health or my compliance with social distancing. I am social distancing, but I worry about the future implications for this.*"

Participants also described the potential for harm caused through racial bias, specifically in reference to public sensors and surveillance cameras, recalling numerous issues with existing facial recognition systems. Others



(a) Likelihood of downloading a contact tracing app versus location (for the countries from which we had at least 100 participants total). (See Section 5.2.)



(b) Comfort with generic entities creating a contact tracing app (for the countries for which we had at least 100 participants). (See Section 5.3.2.)

Fig. 10. These figures show two sets of questions broken down by regional responses.

were concerned about the potential for future misuse: "*Police have already been caught illegally using face ID software, I certainly wouldn't trust them [using surveillance camera data for contact tracing]*" (W7P30).

Concerns about accuracy regarding alternate data sources. Echoing themes from Sections 5.2 and 5.3, participants reasoned about the accuracy of alternate data sources, concerned that cell tower data, credit card data, public sensors, and electronic wearables could not provide sufficient data for accurate contact tracing. Ninety-four participants raised concerns about the lack of accuracy of credit card data: W9P60 noted that credit card data would be an inappropriate source of contact tracing data, because it is "*not good enough to track movement. Park/beach and many more places where I would not use card but be around people.*" Participants also reflected on the potential for facial identification from surveillance cameras to fail (e.g., if wearing masks or sunglasses) or to be impractical due to cost or lack of population density. Reflecting on practicality, W16P71 wrote: "*A tracking bracelet may get lost or people may forget to wear it when they leave the house. It wouldn't provide the most accurate data.*"

Participants value consent and transparency regarding alternate data sources. Throughout all questions, participants raised concerns about consent and transparency, which are particularly important with data that could be collected without their knowledge or with minimal consent (e.g., through a terms of service agreement), for example, via public sensors or data that already exists, such as credit card data or cell phone tower data. W1P190 wrote that an end-date for cell tower data collection and use would make them feel more comfortable: "*If I were informed in advance of the initiative and there was a sunset date for the initiative, I'd be somewhat likely to allow it for the purpose of scientific research. Absent my explicit consent and for only a short period of time, however, I'd be extremely uncomfortable with it.*" Even W12P86, who was largely comfortable with the use of credit card data for contact tracing, gave the caveat that "explicit consent" was necessary: "*I feel more comfortable with my location being acquired (with my knowledge and consent) via this method as it makes me more relieved that I am not actively being tracked (or my location is not being tracked and traced to beach movement). The usage of my credit card history allows me windows of privacy which I would not want anyone interfering with.*" Thus, policy makers and technologists must both work to protect and inform users.

Some support for non-smartphone data sources for contact tracing. Though a majority of participants raised concerns, some supported the alternative data sources we asked about. Of those who supported (or did not oppose) the idea of cell tower data being used for contact tracing, 123 mentioned altruism and the greater good of contact tracing, suggesting that many users, under the right circumstances, may decide that the greater good of their communities outweighs some personal privacy concerns. Twenty-four said they would accept such data sharing if it were for research, while 20 would accept only if they tested positive for COVID-19; these opinions raise questions about these participants' mental models of contact tracing or whether they would consider such data sharing as a way to reduce their need to quarantine if positive.

5.5 Demographic Trends

Given the lack of strong longitudinal trends in many of the questions, we examined demographic trends by combining data from *all* weeks. We find no trends for age, gender, or time spent outside home. We also observe no correlation with infection rate (see Figure 1). The following section presents trends that are largely present throughout all questions; we show the questions related to willingness to use a COVID-19 contact tracing app.

Few regional trends appear in our dataset, but related work investigates more thoroughly. When examining regional trends, we include only regions (e.g., the EU) or countries from which we had more than 100 participants: EU, UK, USA, Mexico, and Canada. We do not find regional trends between the EU, UK, USA and Canada. However, we find that participants from Mexico are less willing to share data with their government, but perhaps more willing to give up privacy if their government is not involved, as shown in Figure 10 (as compared to participants from the EU, UK, US, and Canada). Others have studied regional differences in attitudes towards contact tracing applications [1, 3, 55], and there is a growing body work about cultural or regional differences in privacy attitudes and definitions more generally (e.g., References [36, 78]).

Concern (or lack of concern) about COVID-19 correlated to willingness to download a contact tracing app or give up privacy. Perhaps unsurprisingly, as shown in Figure 11, we find that extreme concern about COVID-19 is correlated with greater willingness to download a contact tracing app or surrender some personal privacy for the sake of contact tracing. However, we also find that extreme *unconcern* is correlated with the same willingness to download a contact tracing app or give up some privacy. One possible explanation is that those who are unconcerned are more accepting of risk in general and thus may be more willing to take actions that others view as potential violations of privacy.

6 DISCUSSION

Drawing from our findings, we surface lessons for both researchers and stakeholders (including app makers, public health experts, policy makers, and others).

User education is needed to correct inaccurate mental models and therefore enable adoption. Users are concerned with the accuracy of the technology involved in contact tracing as well as companies' abilities to actually conduct contact tracing but may be ill-equipped to accurately reason about these factors due to an understandable lack of technical training. Adding to recommendations by groups with similar findings [98, 99], we recommend that technology companies and governments conduct user education campaigns to teach users—at an appropriate technical level—to reason about the extent to which the contact tracing app available to them is appropriate for their personal situation.

Users value transparency and consent and may be less concerned about privacy if they feel in control. Our data revealed substantial fears about data overuse and oversharing, echoing privacy concerns found by numerous others (see Section 3). Participants feared non-consensual data sharing with both their own government and foreign governments as well as data being used for purposes other than contact tracing (e.g., advertising, national security). We recommend that policy makers continue to both create restrictive policies to make users comfortable and educate users about those policies.

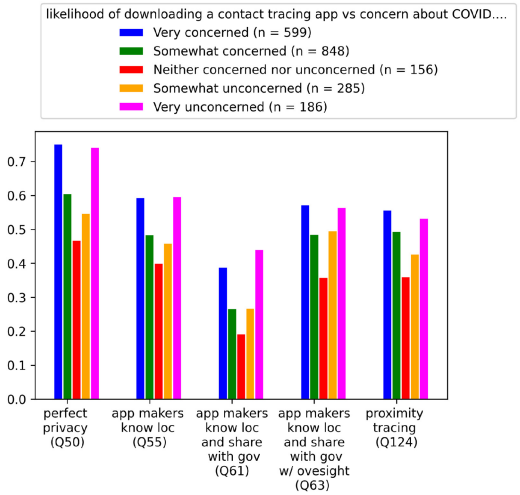


Fig. 11. Willingness to download as compared to concern about COVID-19.

An individual's willingness to download a contact tracing app depends on security and privacy *and other factors.* Beyond the privacy and security concerns and opinions that our work surfaces, there are many other broader issues that must be addressed with the release of a contact tracing application, some of which arose in our qualitative data: Participants brought up concerns of accuracy, equity, and access to smartphones, as well as concerns about the harms of data overusage or sharing disproportionately affecting certain parts of the population. Building on those themes, we encourage stakeholders to consider *accessibility and usability by all*, including those who do not speak the majority language, those who cannot read or write, those who have one or more disabilities (e.g., vision impairment). Additionally, *not all people have smartphones*, and some high risk groups, such as seniors, may be less likely to regularly use a smartphone. A smartphone app excludes those sets of users. If a certain demographic group is left without access, or without usable access, they will benefit less from contact tracing, potentially resulting in different rates of infection. Thus, we urge stakeholders to explore acceptance for automated contact tracing in a broader context than strictly security and privacy and refer readers to References [2, 33, 57, 69, 71, 85] for a fuller discussion of equity and efficacy concerns.

There are substantial challenges with future-proofing longitudinal work during a rapidly evolving global event due to changing terminology and technology. Terminology and technology have evolved *rapidly* during the COVID-19 pandemic, and we thus implore other researchers doing longitudinal work to carefully consider the phrasing of their survey. In designing our survey in late March, we knew we were trying to design questions that would remain relevant for months, throughout a rapidly changing world event. We designed our survey with a goal of being resilient to such world changes. We include our full survey in the Appendix and explicitly note when new questions were added, as the world and the global discussion around contact tracing evolved. Our key recommendations, to any future designers of surveys focused on rapidly evolving issues, are to: (1) design the initial survey with an eye toward future-resiliency, (2) strive to make sure that any additions or modifications to the survey do not invalidate longitudinal analyses, and (3) clearly document any such changes, so the scientific community can fully evaluate the work and the results.

Researchers should continue to study acceptance for automated contact tracing within *specific* populations. Our survey focused on a longitudinal view of young, white, European, and North American views towards automated contact tracing, but we were unable to study any one particular population in depth. Other work has studied populations at a single-country level, e.g., the Netherlands, Germany, Australia, but to our knowledge, few have focused yet on specific and potentially vulnerable subpopulations or minorities, who might

have heightened or different privacy preferences and who also might have greater vulnerability to the virus (one exception is Filer et al., who studied adoption and attitudes among health care workers in England's national health care system, the NHS [27]). We specifically call for further research on minority populations that may be harder hit by the virus (e.g., communities of color in the US [47]), communities that may have a more strained relationship with government or authorities (e.g., Black communities in the US, undocumented immigrants, political dissidents), or communities that may remember a past epidemic (e.g., gay men who lived through the AIDS epidemic). Despite certain communities being particularly vulnerable, we are not aware of existing studies about contact tracing and privacy for such populations, and we believe it is crucial for future work to study and address the specific contexts of these groups.

7 CONCLUSION

Here, we have presented results from a longitudinal survey about public opinion surrounding location privacy and contact tracing during the COVID-19 pandemic, finding that public opinion is largely stable over time and that they have significant and diverse privacy concerns about contact tracing.

The report adds to other concurrent work about public opinion on potential contact tracing technologies and privacy concerns, and we strongly encourage contact tracing developers, policy makers, and others to consider the user values and concerns presented here, as user cooperation is crucial.

APPENDIX

A SURVEY PROTOCOL

The latest version of the survey protocol is below, with footnotes marking questions that were not present in some earlier versions. We give section headings and descriptors for the reader's reference here; participants did not see headers. Unless otherwise specified, all questions were answered on a 5-point Likert scale.

The logo of our institution (with the institution name prominent) appear as a header to each survey page. Our lab and department name did not.

Throughout the course of this research, we have become aware of some inconsistencies or ambiguities in the questions. We chose not to revise the protocol to address these issues to preserve the ability to do longitudinal comparisons. We present the protocol here as it was presented to participants so the reader can understand what participants experienced.

A.1 Consent and Screening

This is a survey about **location tracking and Coronavirus (COVID-19)** by researchers at the University of Washington, in Seattle. University of Washington's Human Subjects Division reviewed our study, and determined that it was exempt from federal human subjects regulation. We do not expect that this survey will put you at any risk for harm, and you don't have to answer any question that makes you uncomfortable. In order to participate, you must be at least 18 years old, regularly use a smartphone, and able to complete the survey in English. We expect this survey will take about 15–20 minutes to complete.

If you have any questions about this survey, you may email us at <study-specific-email>.

Thanks for taking our survey! To start, please answer the two questions below...

Are you at least 18 years old? [yes, no]

Do you use a smartphone regularly? [yes, no]

A.2 Demographics I

This survey involves questions about **COVID-19**, the disease caused by SARS-CoV-2 (commonly known as **coronavirus**).

Q6: How concerned are you about COVID-19?

Q7: Do you believe that social distancing is an important tool for slowing the spread of COVID-19? [yes, no, not sure]

Q8: Averaged over the past week, approximately how many hours much time per day did you spend out of your home, within 6 feet (2 meters) of other people? (e.g., getting groceries, working at an essential job like in a hospital, in a grocery store, etc.). ["I did not leave my home," 0–1 hours per day, 2–3 hours per day, . . . , 7–8 hours per day, 8+ hours per day]

Q144: Do you believe that wearing a mask is an important tool for slowing COVID-19? [yes, no, not sure]

Q145: Over the past week, how often did you wear a mask when you were out of your home? [All of the time, most of the time, some of the time, rarely, never]

Q9: In which country do you currently reside? [drop-down country list]

Q10: For respondents in the USA: in which state do you currently reside? [drop-down US state list]

A.3 Cell Phone Manufacturer and Provider Location Data

Cell phone manufacturers and cellular providers have access to your physical-world location.

Q12: How comfortable are you with your cell phone manufacturer or your cellular carrier using your location data for the purposes of studying or mitigating the spread of COVID-19?

Q13: How comfortable are you with your cell phone manufacturer or your cellular carrier sharing your location data for the past two weeks **with your government** for the purposes of studying or mitigating the spread of COVID-19? (**Regardless of whether you test positive for COVID-19.**)

Q14: **If you tested positive for COVID-19**, how comfortable would you be with your cell phone manufacturer or your cellular carrier sharing your location data for the past two weeks **with your government** for the purposes of studying or mitigating the spread of COVID-19?

Q15: **If you tested positive for COVID-19**, how comfortable would you be with your cell phone manufacturer or your cellular carrier sharing your location data for the past two weeks **publicly**?

Q16: Optionally, do you have any other thoughts about your cell phone manufacturer or your cellular carrier sharing your location data for the purposes of studying or mitigating the spread of COVID-19? [free response]

A.4 Existing App Location Data

Some phone applications have access to your physical-world location, either when the application is in use or all the time. ***Suppose the makers of an existing app on your phone started using your GPS location data to study or mitigate the spread of COVID-19.*** *For example, this could include disclosing past locations of known positive COVID-19 cases to the public or to the government, or alerting people who have crossed paths with the positive case.*

Q18: Below we've listed 15 commonly-used apps. For the apps that you use regularly: how comfortable are you with the following apps using your location data for the purposes of studying or mitigating the spread of COVID-19? ["I don't use this app" + 5-point Likert scale for each of the following apps]

- Google Maps
- Apple Maps
- Waze
- Facebook
- Instagram
- TikTok
- WhatsApp
- Facebook Messenger
- Zoom
- Uber

- Lyft
- Airbnb
- Calorie Counter (MyFitnessPal)
- FitBit
- AllTrails

Suppose that one of the apps that you regularly use—not necessarily one of the ones above—started using your location data to study or mitigate the spread of COVID-19.

Q20: How comfortable are you with this app using your location data for the purposes of studying or mitigating the spread of COVID-19?

Q22: **If you tested positive for COVID-19**, how comfortable would you be with this app sharing your location data for the past two weeks **publicly**?

Q23: Consider all the apps you regularly use on your phone (not just the apps listed earlier). Which app would you **most** trust to use your location data for the purposes of studying and mitigating COVID-19? Why? [free response]

Q24: Which app that you currently use would you **least** trust to use your location data for the purposes of studying and mitigating COVID-19? Why? [free response]

A.5 Current Use of COVID-19 App

Q25: Have you used any apps that help track the spread of COVID-19? (i.e., Singapore's "TraceTogether") [yes, no]

If yes, participants branch to "already have app."

If no, participants continue.

A.6 New App, Perfect Privacy

*Imagine there is a **new** app that would track your location at all times for the purposes of mitigating the spread of COVID-19.*

Suppose that this app protects your data perfectly.

Q50: How likely would you be to install and use this app?

Q51: Would this app change your current behavior?

Q52: Optionally, please use this space tell us any initial thoughts you have about such an app. [free response]

A.7 New App, App Makers Know Location

Imagine there is a new app that would track your location at all times for the purposes of studying or mitigating the spread of COVID-19.

Suppose now that the makers of the application would know your location at all times, but would not share your location with any other entity.

Q55: How likely would you be to install and use this app?

Q56: Now, suppose that the app is made by one of the following companies, all of which already have created popular apps. Please rate how comfortable you would be if each company were responsible for this new app. ["I don't know enough about this company to make a decision" + 5-pt Likert scale for each of the following]

- Google (Google Maps, Waze, etc.)
- Apple (Apple Maps)
- Facebook (Facebook, Facebook Messenger, Instagram, WhatsApp)
- Microsoft (Skype, OneDrive, etc.)[4]

[4]Added April 17 (week 3).

- ByteDance (TikTok)
- Zoom Video Communication
- Uber
- Lyft
- AirBnb
- MyFitnessPal
- AllTrails
- FitBit

Q57: Suppose that the app is made by one of the following general entities. Please rate how comfortable you would be if one of the following were responsible for this new app, which would use the location data they collect from your smartphone to track the spread of COVID-19. [5-pt Likert scale for each of the following]

- A university research group
- An activist group
- An industry startup
- Your government
- The United Nations

Q58: Optionally, please use the space below to elaborate on your thoughts about one or more companies using your location data for the purposes of tracking COVID-19. [free response]

A.8 New App, App Makers Share Data with Government

Again, imagine there is a new app that would track your location at all times for the purposes of studying or mitigating the spread of COVID-19.

Suppose now that the makers of the application would know your location at all times, and would also share that data with your government if you were diagnosed with COVID-19.

Q61: How likely would you be to install and use this app?

Q62: If the government's use of the data were **supervised by a judge**, how likely would you be to install and use this app?[5]

Now suppose that the makers of the application would share your location data with your government ***only if you tested positive for COVID-19.***

Q63: How likely would you be to install and use this app?

Q112: If the government's use of the data were **supervised by a judge**, how likely would you be to install and use this app?

Q64: Optionally, do you have any other thoughts about a company that is doing COVID-19 tracking sharing your location with your government? [free response]

Q115: Optionally, do you have any other thoughts about judicial oversight of the government's usage of location data? [free response]

A.9 Other Location Data Sources: Credit Card History and Surveillance Camera Footage

There[6] *are other ways to track someone's location. One is the use of video cameras in public places. Another is the use of credit card purchasing histories.*

Q115: How comfortable would you be with your **credit card company** deriving your location history for the past two weeks for the purposes of studying and mitigating the spread of COVID-19?

[5]This question, and the rest of this section, was added on April 17 (week 3) as a previous version was ambiguous.
[6]Added April 17 (week 3).

Q116: How comfortable would you be with your **credit card company** deriving your location history for the past two weeks **and sharing it with your government** for the purposes of studying and mitigating the spread of COVID-19?

Q117: Optionally, do you have any other thoughts about your location history being derived from your **credit card** purchase history?

A.10 Other Data Location Sources II: Wearable Electronics and Public Area Sensors

Suppose[7] there were an electronic bracelet that would track your location for the purposes of studying or mitigating the spread of COVID-19.

Q146: How likely would you be to use this bracelet?

Q147: Optionally, do you have any other thoughts about wearable electronics being used for the purposes of studying or mitigating the spread of COVID-19?

Suppose your region added sensors (such as cameras, phone tagging stations, etc.) in public areas (such as subway stations, bus stops, storefronts, public parks, etc.).

Q148: How comfortable would you be with the use of public-area sensors to study or mitigate the spread of COVID-19?

Q149: Optionally, do you have any other thoughts about such sensors being used for the purposes of studying or mitigating COVID-19?

A.11 Proximity Tracing

One alternative[8] *to location tracking for the purposes of studying or mitigating COVID-19 is* ***proximity tracing****, in which your phone would automatically exchange information with every phone within 6 feet (2 meters) of your phone,* ***keeping track of your close physical encounters, but not tracking your actual location****. This data could then be used to reconstruct your close encounters if you contracted COVID-19, or could alert you if someone you had been in close physical proximity to tested positive for COVID-19.*

Q121: Imagine that your **cell phone manufacturer or phone operating system** would conduct proximity tracing for the purposes of studying or mitigating COVID-19 (and, vice versa, other phones will record that they have been in the proximity of your phone). How comfortable would you be with this?

Q122: Suppose that your **cell phone manufacturer or phone operating system** would share this proximity data **with your government** if you tested positive for COVID-19. How comfortable would you be with this?

Q123: Optionally, do you have any other thoughts about your cell phone manufacturer or phone operating system tracking other phones nearby? [free response]

Imagine instead there is a new ***app*** *that would conduct proximity tracing for the purposes of studying or mitigating COVID-19: that is, it would not track your location, but would instead keep track of other phones that you are nearby (and, vice versa, other phones with this app will record that they have been in the proximity of your phone).*

Q124: How likely would you be to download this app?

Q125: Now, suppose that the proximity tracing app is made by one of the following companies. Please rate how comfortable you would be if each company were responsible for this new app. ["I don't know enough about this company to make a decision" + 5-pt Likert scale for each of the following]

- Google (Google Maps, Waze, etc.)
- Apple (Apple Maps)
- Facebook (Facebook, Facebook Messenger, Instagram, WhatsApp)
- Microsoft (Skype, etc.)
- ByteDance (TikTok)

[7] Added July 17 (week 16).
[8] Added April 17 (week 3).

- Zoom Video Communication
- Uber
- Lyft
- AirBnb
- MyFitnessPal
- AllTrails
- FitBit

Q126: Now, suppose that the proximity tracing app is made by one of the following general entities. Please rate how comfortable you would be if each entity were responsible for this new app.

- A university research group
- An activist group
- An industry startup
- Your government
- The United Nations

Q127: Optionally, do you have any other thoughts about an app that tracks other phones nearby?

Q128: Optionally, do you have any other thoughts about proximity tracking versus location tracking for the purposes of studying or mitigating COVID-19?

A.12 Government Use of Data

If the government acquired your location data or proximity data[9] *(i.e., from an app on your phone, from your cell phone carrier, etc.)* ***for the purposes for studying and mitigating COVID-19****....*

Q66: How likely do you think it is that your government would **delete** the data after the pandemic ends?

Q67: How likely do you think it is that your government would **only** use the data for the purposes of tracking COVID-19?

Q68: How concerned would you be about your government's use of your location data harming **your personal safety** or the safety of those in your community?

Q69: Suppose your location was shared with only a specific sector of the government. For each of the following sectors of government, please rate how comfortable you would be with them having access to your location data.

- Federal Disease Tracking Agency (US: CDC)
- Your state or City Health Department
- Tax Agency (US: IRS)
- Local law enforcement (state, country, city, etc.)
- Immigration authorities (US: CBP or ICE)

Q70: Optionally, please use the space below to elaborate on your thoughts about the government having access to your location data for the purposes of COVID-19 tracking. [free response]

A.13 App Features

In some countries, such as South Korea, China, and Singapore, there do exist apps to monitor the spread of COVID-19 through location tracking. These apps can have multiple purposes, including:

— Alerting the user if they have come into contact with someone who later tests positive with COVID-19;

— Helping the community or law enforcement enforce isolation and quarantine edicts;

[9]"or proximity data" added April 17.

— *Tracing viral strains through the community.*

Q72: If a new app were deployed in your country to mitigate the spread of COVID-19, which of the following features would you want it to have? (5-point Likert-scale for each of the following:)

- Notify you if you came close to someone who later tested positive for COVID-19
- Notify anyone you came close to in the past two weeks if you tested positive for COVID-19
- Make your location history for the past two weeks publicly available if you tested positive for COVID-19
- Make public a database of the location histories of anyone who tested positive for COVID-19
- Notify you if your neighbors were not isolating themselves as recommended or mandated
- Let you notify the authorities if you saw people you suspected or knew to be breaking the isolation recommended or mandated
- Automatically notify the authorities if people were not isolating as mandated
- Used by scientists to study tends, not individuals
- Geofence to enforce mandatory or voluntary quarantine
- General assessment of social distancing in an area to display areas of high congregation

Q73: Optionally, do you have any other thoughts about what you would want such an app to do? [free response]

Q74: Optionally, do you have any other thoughts about what you would want such an app to NOT do? [free response]

Q75: Is such an app available in your country? [Yes/No/I'm not sure]
If yes, participants branch to "App available"

A.14 Section 5.0: Prior Privacy Preferences

We're now going to ask you about your thoughts about location sharing with your government BEFORE COVID-19.

Q80: In Oct 2019 (before the first known cases of COVID-19), how comfortable would you have been with your location data being shared with the government in general?

Q81: In Oct 2019 (before the first known cases of COVID-19), how comfortable were you with your location data being shared with the following sectors of government? [5-point Likert scale for each of the following:]

- Federal Disease Tracking Agency (US: CDC)
- Your state or City Health Department
- Tax Agency (US: IRS)
- Local law enforcement (state, country, city, etc.)
- Immigration authorities (US: CBP or ICE)

Q82: Optionally, please use the space below to elaborate on your thoughts about one or more companies sharing your location data with some part of the government (before COVID-19). [free response]

A.15 Demographics II

Almost done!

Q39: What is your age? (you may answer approximately if you do not know, or wish not to say exactly) [free response]

Q40: What is your gender identity? [free response]

Q141: Please select any races or ethnicities that you feel accurately reflect who you are. Please select as many as apply to you. We also realize that because race and ethnicity cannot be put into categories, you may prefer to self-describe your race and ethnicity in the following question. You may also select from the options below and submit

a free-response. The following races and ethnicities are presented in alphabetical order. [American Indian or Alaskan Native, Asian, Black or African American, Hispanic, Native Hawaiian or Other Pacific Islander, White][10]

Q142: If you prefer to self-describe your race and ethnicity instead of or in addition to using the checkboxes above, please do so here. [free response][11]

Q41: What political party do your views typically align with? [free response]

Q42: What are your top three news sources? (i.e., Twitter, Facebook, Fox News, CNN, NPR, New York Times, etc.) [free response]

Q132: Have you ever had COVID-19? [Yes, definitely; Yes, I think so; I am unsure; No, I don't think so; No, definitely not][12]

Q133: Have you ever been medically tested for COVID-19? [Yes, I have had a test; No, I have not been tested][13]

Q43: Regarding COVID-19, are you in high risk group or live with someone with high risk? [yes/no]

Q44: Are you generally interested in or concerned about privacy and technology? [yes/no]

Q45: Do you know how to change location permissions for apps on your phone? [yes/no]

Q129: What is your phone manufacturer? (e.g., Apple, Samsung, Huawei, Nokia, OnePlus, XiaoMi, OPPO, etc.) [free response][14]

A.16 Branch: App Is Available

Q76: Have you downloaded the app in your country to mitigate or study the spread of COVID-19? [yes, no]

Q77: If you have not downloaded the app: why not? what changes, or assurances by the manufacturer or government (if any) would you want to see to the app before downloading? [free response]

Q78: What are your thoughts about the privacy properties of this app? [free response]

A.17 Branch: Already Have App

You indicated that there is an app (or apps) available in your country to track, study, or mitigate COVID-19. This section will ask about that app.

Q27: What is the name of the app, or apps?

Q28: Why did you install and use it?

Q29: Do you know anyone who did not download the app? [yes, no]

Q30: If so, why did they not install it?

Q31: What concerns, if any, do you have about the app?

Q32: If you had or have concerns, what outweighed the concerns and lead you to the decision to download the app?

Q33: What concerns, if any, do you have about your government having access to your location data?

Q34: What concerns, if any, do you have about the app makers having access to your location data?

Q35: Do you expect the app makers to stop storing your location data after the pandemic is over?

Q36: Do you plan to delete the app after the pandemic?

Q37: Anything else you'd like to say about the app and/or your concerns?

ACKNOWLEDGMENTS

We are very thankful to Karl Weintraub for general discussions, sanity, and his Pandas knowledge. We are also thankful to Gennie Gebhart for early discussions about this work. We thank Christine Chen, Ivan Evtimov, Joseph Jaeger, Shrirang Mare, Alison Simko, Robert Simko, and Eric Zeng for their valuable feedback on pilot versions of

[10] Added week 12.
[11] Added week 12.
[12] Added week 5.
[13] Added week 5.
[14] Added week 5.

our survey. Additionally, we are thankful to Gennie Gebhart, Joseph Jaeger, and Elissa Redmiles for their valuable feedback on a draft of this article.

We are also very thankful to Prolific for supporting our research by waiving their fees for one month as part of their COVID-19 fee waiver program.

REFERENCES

[1] Johannes Abeler, Sam Altmann, Luke Milsom, Séverine Toussaert, and Hannah Zillessen. 2020. Support in the UK for app-based contact tracing of COVID-19. Retrieved from osf.io.

[2] Ali Alkhatib. 2020. We need to talk about digital contact tracing. Retrieved from https://ali-alkhatib.com/blog/digital-contact-tracing.

[3] Samuel Altmann, Luke Milsom, Hannah Zillessen, Raffaele Blasone, Frederic Gerdon, Ruben Bach, Frauke Kreuter, Daniele Nosenzo, Severine Toussaert, and Johannes Abeler. 2020. Acceptability of app-based contact tracing for COVID-19: Cross-country survey evidence. Retrieved from *SSRN 3590505*.

[4] Monica Anderson and Brooke Auxier. 2020. Most Americans don't think cellphone tracking will help limit COVID-19, are divided on whether it's acceptable. *Pew Research Center* (16 Apr. 2020). Retrieved from https://www.pewresearch.org/fact-tank/2020/04/16/most-americans-dont-think-cellphone-tracking-will-help-limit-covid-19-are-divided-on-whether-its-acceptable/.

[5] Bahrain. Retrieved from https://play.google.com/store/apps/details?id=bh.bahrain.corona.tracker&hl=en_US.

[6] BBC. 2020. Coronavirus: Austria locks down as new wave grips Europe. Retrieved from https://www.bbc.com/news/world-europe-54945400.

[7] Dave Burke. An update on Exposure Notifications. Retrieved from https://blog.google/inside-google/company-announcements/update-exposure-notifications/.

[8] Justin Chan, Dean Foster, Shyam Gollakota, Eric Horvitz, Joseph Jaeger, Sham Kakade, Tadayoshi Kohno, John Langford, Jonathan Larson, Sudheesh Singanamalla, Jacob Sunshine, and Stefano Tessaro. 2020. PACT: Privacy-sensitive protocols and mechanisms for mobile contact tracing. (2020). arXiv:arXiv:2004.03544.

[9] Clara Chong. 2020. About 1 million people have downloaded TraceTogether app, but more need to do so for it to be effective: Lawrence Wong. *The Straits Times* (1 Apr. 2020). Retrieved from https://www.straitstimes.com/singapore/about-one-million-people-have-downloaded-the-tracetogether-app-but-more-need-to-do-so-for.

[10] Juli Clover. 2020. Apple's Exposure Notification system: Everything you need to know. Retrieved from https://www.macrumors.com/guide/exposure-notification/.

[11] D'vera Cohn. 2015. Census considers new approach to asking about race—by not using the term at all. Retrieved from https://www.pewresearch.org/fact-tank/2015/06/18/census-considers-new-approach-to-asking-about-race-by-not-using-the-term-at-all.

[12] Colombia. Retrieved from https://play.google.com/store/apps/details?id=co.gov.ins.guardianes&hl=en_US.

[13] European Commission. 2020. COVID-19 media surveillance - 31 Mar. 2020. Retrieved from https://ec.europa.eu/jrc/en/science-update/covid-19-media-surveillance-20200331.

[14] Coronamap. Retrieved from https://coronamap.site/.

[15] Andrew Crocker, Kurt Opsahl, and Bennett Cyphers. 2020. The challenge of proximity apps For COVID-19 contact tracing. Retrieved from https://www.eff.org/deeplinks/2020/04/challenge-proximity-apps-covid-19-contact-tracing.

[16] Czech. Retrieved from https://play.google.com/store/apps/details?id=cz.covid19cz.erouska&hl=en_US.

[17] Mark É. Czeisler, Michael A. Tynan, Mark E. Howard, Sally Honeycutt, Erika B. Fulmer, Daniel P. Kidder, Rebecca Robbins, Laura K. Barger, Elise R. Facer-Childs, Grant Baldwin et al. 2020. Public attitudes, behaviors, and beliefs related to COVID-19, stay-at-home orders, nonessential business closures, and public health guidance–United States, New York City, and Los Angeles, May 5–12, 2020. *Morbid. Mortal. Weekly Rep.* 69, 24 (2020), 751.

[18] Alejandro de la Garza. (n.d.).S Contact tracing apps were big tech's best idea for fighting COVID-19. Why haven't they helped? Retrieved from https://time.com/5905772/covid-19-contact-tracing-apps/.

[19] Nicola Dell, Vidya Vaidyanathan, Indrani Medhi, Edward Cutrell, and William Thies. 2012. "Yours is better!" Participant response bias in HCI. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 1321–1330.

[20] Simon Dennis, Paul Garrett, Joshua White, Daniel Little, Amy Perfors, Yoshihisa Kashima, and Stephan Lewandowsky. 2020. A representative sample of australian participant's attitudes towards government tracking during the COVID-19 pandemic. Retrieved from https://paulgarrettphd.github.io/Site/Wave2Final.html.

[21] Simon Dennis, Stephan Lewandowsky, Philipp Lorenz-Spreen, Klaus Oberauer, Yasmina Okan, Rob Goldstone, Yang Cheng-Ta, Yoshihisa Kashima, Amy Perfors, Josh White, Paul Garrett, Nic Geard, Daniel Little, Lewis Mitchell, Martin Tomko, Anastasia Kozyreva, Stefan Herzog, Ralph Hertwig, Thorsten Pachur, Muhsin Yesilada, and Marcus Butavicius. Social Licensing of Privacy-Encroaching Policies to Address the COVID-19 Pandemic. Retrieved from https://stephanlewandowsky.github.io/UKsocialLicence/index.html.

[22] Zak Doffman. 2020. Forget Apple and Google–Here's the real challenge for COVID-19 contact-tracing. Retrieved from https://www.forbes.com/sites/zakdoffman/2020/04/12/forget-apple-and-google-heres-the-real-challenge-for-covid-19-contact-tracing/#4f9426092709.

[23] Darrell Etherington. 2020. Apple launches COVID-19 "Exposure Notification Express" with iOS 13.7—Android to follow later this month. Retrieved from https://techcrunch.com/2020/09/01/apple-launches-system-level-covid-19-exposure-notification-express-with-ios-13-7-google-to-follow-later-this-month/.
[24] Evaluate research. Retrieved from https://www.evaluate.com/covid-19-daily-update.
[25] Lilla Farkas. 2017. Data collection in the field of ethnicity: Analysis and comparative review of equality data collection practices in the European Union. *European Commission* (2017).
[26] Luca Ferretti, Chris Wymant, Michelle Kendall, Lele Zhao, Anel Nurtay, Lucie Abeler-Dörner, Michael Parker, David Bonsall, and Christophe Fraser. 2020. Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing. *Science* (2020).
[27] Joshua Filer and Daniel Gheorghiu. 2020. Test, track, and trace: How is the NHSX Covid app performing in a hospital setting? *Cold Spring Harbor Laboratory Press* (2020).
[28] US Food and Drug Administration. 2016. Collection of race and ethnicity data in clinical trials: Guidance for industry and food and drug administration staff. *Rockville, MD: US Food and Drug Administration* (2016).
[29] Paul Garrett, Joshua Paul White, Stephan Lewandowsky, Yoshihisa Kashima, Andrew Perfors, Daniel R. Little, Nic Geard, Lewis Mitchell, Martin Tomko, and Simon Dennis. 2020. The acceptability and uptake of smartphone tracking for COVID-19 in Australia. *PsyArXiv* (2020).
[30] Jacob Gershman. 2020. A guide to state coronavirus lockdowns. *The Wall Street Journal* (31 Mar. 2020). Retrieved from https://www.wsj.com/articles/a-state-by-state-guide-to-coronavirus-lockdowns-11584749351/.
[31] Ghana. Retrieved from http://ghcovid19.com/.
[32] Google. 2020. Apple and Google partner on COVID-19 contact tracing technology. Retrieved from https://www.blog.google/inside-google/company-announcements/apple-and-google-partner-covid-19-contact-tracing-technology/.
[33] Matthew Guariglia and Adam Schwartz. 2020. Protecting civil liberties during a public health crisis. Retrieved from https://www.eff.org/deeplinks/2020/03/protecting-civil-liberties-during-public-health-crisis.
[34] M. Guillon and P. Kergall. 2020. Attitudes and opinions on quarantine and support for a contact-tracing application in France during the COVID-19 outbreak. *Pub. Health* 188 (2020), 21–31.
[35] David M. Halbfinger, Isabel Kershner, and Ronen Bergman. 2020. To track coronavirus, Israel moves to tap secret trove of cellphone data. *The New York Times* (16 Mar. 2020). Retrieved from https://www.nytimes.com/2020/03/16/world/middleeast/israel-coronavirus-cellphone-tracking.html.
[36] Marian Harbach, Alexander De Luca, Nathan Malkin, and Serge Egelman. 2016. Keep on lockin' in the free world: A multi-national comparison of smartphone locking. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*. 4823–4827.
[37] Eszter Hargittai and Elissa Redmiles. Covid-19 study on digital media and the coronavirus pandemic. Retrieved from http://webuse.org/covid/.
[38] Eszter Hargittai and Elissa Redmiles. 2020. Will Americans be willing to install COVID-19 tracking apps? *Scientific American* (28 Apr. 2020). Retrieved from https://blogs.scientificamerican.com/observations/will-americans-be-willing-to-install-covid-19-tracking-apps/.
[39] Joel Hellewell, Sam Abbott, Amy Gimma, Nikos I. Bosse, Christopher I. Jarvis, Timothy W. Russell, James D. Munday, Adam J. Kucharski, W. John Edmunds, Fiona Sun, et al. 2020. Feasibility of controlling COVID-19 outbreaks by isolation of cases and contacts. *The Lancet Global Health* (2020).
[40] Mary Hui. 2020. How Taiwan is tracking 55,000 people under home quarantine in real time. *Quartz* (31 Mar. 2020). Retrieved from https://qz.com/1825997/taiwan-phone-tracking-system-monitors-55000-under-coronavirus-quarantine/.
[41] Mary Ilyushina. 2020. How Russia is using authoritarian tech to curb coronavirus. *CNN* (29 Mar. 2020). Retrieved from https://www.cnn.com/2020/03/29/europe/russia-coronavirus-authoritarian-tech-intl/index.html.
[42] India. Retrieved from https://play.google.com/store/apps/details?id=nic.goi.aarogyasetu&hl=en_US.
[43] Inria. Retrieved from https://github.com/ROBERT-proximity-tracing/documents.
[44] Israel. Retrieved from https://play.google.com/store/apps/details?id=com.hamagen&hl=en_US.
[45] Stephanie Maria Jansen-Kosterink, Marian Hurmuz, Marjolein den Ouden, and Lex van Velsen. 2020. Predictors to use mobile apps for monitoring COVID-19 symptoms and contact tracing: A survey among Dutch citizens. *Cold Spring Harbor Lab. Press* (2020).
[46] Jessica Jones. 2020. Spain toughens restrictions as coronavirus death toll surges. *Reuters* (29 Mar. 2020). Retrieved from https://www.reuters.com/article/us-health-coronavirus-spain/spains-coronavirus-death-toll-rises-by-838-overnight-to-6528-idUSKBN21G0C0.
[47] Rafi Kabarriti, N. Patrik Brodin, Maxim I. Maron, Chandan Guha, Shalom Kalnicki, Madhur K. Garg, and Andrew D. Racine. 2020. Association of race and ethnicity with comorbidities and survival among patients with COVID-19 at an urban medical center in New York. *JAMA Netw. Open* 3, 9 (2020), e2019795–e2019795.
[48] Ruogu Kang, Stephanie Brown, Laura Dabbish, and Sara Kiesler. 2014. Privacy attitudes of Mechanical Turk workers and the US public. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*.
[49] Jennifer Kates, Josh Michaud, and Jennifer Tolbert. 2020. Stay-at-home orders to fight COVID-19 in the United States: The risks of a scattershot approach. *KFF* (5 Apr. 2020). Retrieved from https://www.kff.org/coronavirus-policy-watch/stay-at-home-orders-to-fight-covid19/.

[50] Jamey Keaten and Frank Jordans. 2020. More masks, less play: Europe tightens rules as virus surges. (13 Oct. 2020). Retrieved from https://apnews.com/article/virus-outbreak-pandemics-geneva-france-europe-40521fb6080e35bc4aae4144bf3652bc.
[51] Min Joo Kim and Simon Denyer. 2020. A "travel log" of the times in South Korea: Mapping the movements of coronavirus carriers. *The Washington Post* (13 Mar. 2020). Retrieved from https://www.washingtonpost.com/world/asia_pacific/coronavirus-south-korea-tracking-apps/2020/03/13/2bed568e-5fac-11ea-ac50-18701e14e06d_story.html.
[52] Max S. Kim. 2020. South Korea is watching quarantined citizens with a smartphone app. Retrieved from https://www.technologyreview.com/2020/03/06/905459/coronavirus-south-korea-smartphone-app-quarantine/.
[53] Nemo Kim. 2020. "More scary than coronavirus": South Korea's health alerts expose private lives. *The Guardian* (5 Mar. 2020). Retrieved from https://www.theguardian.com/world/2020/mar/06/more-scary-than-coronavirus-south-koreas-health-alerts-expose-private-lives.
[54] Sarah Knapton. 2020. How long will the UK coronavirus lockdown last? *Telegraph* (27 Apr. 2020). Retrieved from https://www.telegraph.co.uk/news/2020/04/24/how-long-will-uk-lockdown-last-summer/.
[55] Genia Kostka and Sabrina Habich-Sobiegalla. 2020. In times of crisis: Public perceptions towards COVID-19 contact tracing apps in China, Germany and the US. *Germany and the US (Sept. 16, 2020)* (2020).
[56] Stephanie Kramer. 2020. More Americans say they are regularly wearing masks in stores and other businesses. (27 Aug. 2020). Retrieved from https://www.pewresearch.org/fact-tank/2020/08/27/more-americans-say-they-are-regularly-wearing-masks-in-stores-and-other-businesses/.
[57] Susan Landau, Christy E. Lopez, and Laura Moy. 2020. The importance of equity in contact tracing. (1 May 2020). Retrieved from https://www.lawfareblog.com/importance-equity-contact-tracing.
[58] Alex Ledsom. 2020. New EU travel restrictions, country by country, as Europe locks down. (12 Nov. 2020). Retrieved from https://www.forbes.com/sites/alexledsom/2020/11/12/new-eu-travel-bans-country-by-country-covid-19-restrictions-as-europe-locks-down/?sh=34b75c466f80.
[59] Tianshi Li, Cori Faklaris, Jennifer King, Yuvraj Agarwal, Laura Dabbish, Jason I. Hong, et al. 2020. Decentralized is not risk-free: Understanding public perceptions of privacy-utility trade-offs in COVID-19 contact-tracing apps. *arXiv preprint arXiv:2005.11957*.
[60] Paul Mozur, Raymond Zhong, and Aaron Krolik. 2020. In coronavirus fight, China gives citizens a color code, with red flags. *The New York Times* (1 Mar. 2020). Retrieved from https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html.
[61] North Dakota. Retrieved from https://ndresponse.gov/covid-19-resources/care19.
[62] North Macedonia. Retrieved from https://stop.koronavirus.gov.mk/en.
[63] Norway. Retrieved from https://helsenorge.no/coronavirus/smittestop.
[64] Patrick Howell O'Neill. 2020. No, coronavirus apps don't need 60% adoption to be effective. (5 Jun. 2020). Retrieved from https://www.technologyreview.com/2020/06/05/1002775/covid-apps-effective-at-less-than-60-percent-download/.
[65] Patrick Howell O'Neill, Tate Ryan-Mosley, and Bobbie Johnson. MIT Technology Review Covid Tracing Tracker. Retrieved from https://docs.google.com/spreadsheets/d/1ATalASO8KtZMx__zJREoOvFh0nmB-sAqJ1-CjVRSCOw/.
[66] World Health Organization. Retrieved from https://covid19.who.int/table.
[67] Michael Edmund O'Callaghan, Jim Buckley, Brian Fitzgerald, Kevin Johnson, John Laffey, Bairbre McNicholas, Bashar Nuseibeh, Derek O'Keeffe, Ian O'Keeffe, Abdul Razzaq, et al. 2020. A national survey of attitudes to COVID-19 digital contact tracing in the Republic of Ireland. *Irish J. Med. Sci. (1971-)* (2020), 1–25.
[68] Lois Parshley. 2020. The magnitude of America's contact tracing crisis is hard to overstate. (1 Sept. 2020). Retrieved from https://www.nationalgeographic.com/science/2020/09/contact-tracing-crisis-magnitude-hot-mess-america-fixes-coronavirus-cvd/.
[69] Ramesh Raskar, Isabel Schunemann, Rachel Barbar, Kristen Vilcans, Jim Gray, Praneeth Vepakomma, Suraj Kapa, Andrea Nuzzo, Rajiv Gupta, Alex Berke, Dazza Greenwood, Christian Keegan, Shriank Kanaparti, Robson Beaudry, David Stansbury, Beatriz Botero Arcila, Rishank Kanaparti, Vitor Pamplona, Francesco M. Benedetti, Alina Clough, Riddhiman Das, Kaushal Jain, Khahlil Louisy, Greg Nadeau, Vitor Pamplona, Steve Penrod, Yasaman Rajaee, Abhishek Singh, Greg Storm, and John Werner. 2020. Apps gone rogue: Maintaining personal privacy in an epidemic. (2020). arXiv:arXiv:2003.08567.
[70] Elissa M. Redmiles. What does it mean for a COVID app to "work"? Retrieved from http://www.cs.umd.edu/~eredmiles/how-good-good-enough.pdf.
[71] Elissa M. Redmiles. 2020. User concerns & tradeoffs in technology-facilitated COVID-19 response. 2, 1 (2020). Retrieved from https://doi.org/10.1145/3428093.
[72] Elissa M. Redmiles, Yasemin Acar, Sascha Fahl, and Michelle L. Mazurek. 2017. *A Summary of Survey Methodology best Practices for Security and Privacy Researchers*. Technical Report. University of Maryland.
[73] Elissa M. Redmiles, Sean Kross, and Michelle L. Mazurek. 2019. How well do my results generalize? Comparing security and privacy survey results from MTurk, web, and telephone samples. In *Proceedings of the IEEE Symposium on Security and Privacy (SP)*. IEEE, 1326–1343.
[74] Nicolás Rivero. US states are finally rolling out Covid-19 exposure notification apps.
[75] Ronald L. Rivest, Hal Abelson, Jon Callas, Ran Canetti, Kevin Esvelt, Daniel Kahn Gillmor, Louise Ivers, Yael Tauman Kalai, Anna Lysyanskaya, Adam Norige, Bobby Pelletier, Ramesh Raskar, Adi Shamir, Emily Shen, Israel Soibelman, Michael Specter, Vanessa

Teague, Ari Trachtenberg, Mayank Varia, Marc Viera, Daniel Weitzner, John Wilkinson, and Marc Zissman. Retrieved from pact.mit.edu.
[76] Joel Ross, Lilly Irani, M. Silberman, Andrew Zaldivar, and Bill Tomlinson. 2010. Who are the crowdworkers?: Shifting demographics in Mechanical Turk. In *Proceedings of the CHI'10 Extended Abstracts on Human Factors in Computing Systems*. ACM, 2863–2872.
[77] Uptin Saiidi. 2020. Hong Kong is putting electronic wristbands on arriving passengers to enforce coronavirus quarantine. *CNBC* (18 Mar. 2020). Retrieved from https://www.cnbc.com/2020/03/18/hong-kong-uses-electronic-wristbands-to-enforce-coronavirus-quarantine.html.
[78] Yukiko Sawaya, Mahmood Sharif, Nicolas Christin, Ayumu Kubota, Akihiro Nakarai, and Akira Yamada. 2017. Self-confidence trumps knowledge: A cross-cultural study of security behavior. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*. 2202–2214.
[79] Rob Schmitz. 2020. In Germany, high hopes for new COVID-19 contact tracing app that protects privacy. Retrieved from https://www.npr.org/sections/coronavirus-live-updates/2020/04/02/825860406/in-germany-high-hopes-for-new-covid-19-contact-tracing-app-that-protects-privacy.
[80] Tanusree Sharma and Masooda Bashir. 2020. Use of apps in the COVID-19 response and the loss of privacy protection. *Nat. Med.* (2020), 1–2.
[81] Michael D. Shear. 2020. Trump extends social distancing guidelines through end of April. Retrieved from https://www.nytimes.com/2020/03/29/us/politics/trump-coronavirus-guidelines.htmll.
[82] Selena Simmons-Duffin. 2020. COVID-19 contact tracing workforce barely "inching up" as cases surge. Retrieved from https://www.npr.org/sections/health-shots/2020/10/14/923468159/covid-19-contact-tracing-workforce-barely-inching-up-as-cases-surge.
[83] Natasha Singer. 2020. The hot new covid tech is wearable and constantly tracks you. Retrieved from https://www.nytimes.com/2020/11/15/technology/virus-wearable-tracker-privacy.html?referringSource=articleShare.
[84] Natasha Singer and Choe Sang-Hun. 2020. As coronavirus surveillance escalates, personal privacy plummets. (23 March 2020). Retrieved from https://www.nytimes.com/2020/03/23/technology/coronavirus-surveillance-tracking-privacy.html.
[85] Ashkan Soltani, Ryan Calo, and Carl Bergstrom. 2020. Contact-tracing apps are not a solution to the COVID-19 crisis. Retrieved from https://www.brookings.edu/techstream/inaccurate-and-insecure-why-contact-tracing-apps-could-be-a-disaster/.
[86] Jay Stanley and Jennifer Stisa Granick. 2020. The limits of location tracking in an epidemic. Retrieved from https://www.aclu.org/aclu-white-paper-limits-location-tracking-epidemic.
[87] Ruoxi Sun, Wei Wang, Minhui Xue, Gareth Tyson, Seyit Camtepe, and Damith Ranasinghe. 2020. Vetting security and privacy of global COVID-19 contact tracing applications. *arXiv preprint arXiv:2006.10933*.
[88] Craig Timberg, Drew Harwell, and Safarpour Alauna. 2020. Most Americans are not willing or able to use an app tracking coronavirus infections. That's a problem for big tech's plan to slow the pandemic. *The Washington Post* (29 Apr. 2020). Retrieved from https://www.washingtonpost.com/technology/2020/04/29/most-americans-are-not-willing-or-able-use-an-app-tracking-coronavirus-infections-thats-problem-big-techs-plan-slow-pandemic/.
[89] The New York Times. 2020. See which states are reopening and which are still shut down. *The New York Times*. Retrieved from https://www.nytimes.com/interactive/2020/us/states-reopen-map-coronavirus.html.
[90] TraceTogether. Retrieved from https://www.tracetogether.gov.sg.
[91] Carmela Troncoso, Mathias Payer, Jean-Pierre Hubaux, Marcel Salathé, James Larus, Edouard Bugnion, Wouter Lueks, Theresa Stadler, Apostolos Pyrgelis, Daniele Antonioli, Ludovic Barman, Sylvain Chatel, Kenneth Paterson, Srdjan Čapkun, David Basin, Jan Beutel, Dennis Jackson, Bart Preneel, Nigel Smart, Dave Singelee, Aysajan Abidin, Seda Guerses, Michael Veale, Cas Cremers, Reuben Binns, and Ciro Cattuto. 2020. Decentralized privacy-preserving proximity tracing. Retrieved from https://github.com/DP-3T/documents/blob/master/DP3T%20White%20Paper.pdf.
[92] Utah.gov. 2020. State of Utah releases "healthy together" beta app. Retrieved from https://coronavirus.utah.gov/state-of-utah-releases-healthy-together-beta-app/.
[93] Serge Vaudenay. 2020. Centralized or decentralized? The contact tracing dilemma. Retrieved from https://eprint.iacr.org/2020/531.pdf.
[94] Haohuang Wen, Qingchuan Zhao, Zhiqiang Lin, Dong Xuan, and Ness Shroff. 2020. A study of the privacy of Covid-19 contact tracing apps. In *Proceedings of the International Conference on Security and Privacy in Communication Networks*.
[95] Caroline Wiertz, Aneesh Banerjee, Oguz A. Acar, and Adi Ghosh. 2020. Predicted adoption rates of contact tracing app configurations-insights from a choice-based conjoint study with a representative sample of the UK population. Retrieved from *SSRN 3589199*.
[96] Wikipedia. Retrieved from https://en.wikipedia.org/wiki/COVID-19_apps.
[97] Wikipedia. Exposure Notification. Retrieved from https://en.wikipedia.org/wiki/Exposure_Notification.
[98] Simon N. Williams, Christopher J. Armitage, Tova Tampe, and Kimberly Dienes. 2020. Public attitudes towards COVID-19 contact tracing apps: A UK-based focus group study. *medRxiv* (2020).
[99] Baobao Zhang, Sarah Kreps, and Nina McMurry. 2020. Americans' perceptions of privacy and surveillance in the COVID-19 pandemic. (2020).

Received 23 November 2020; revised 7 June 2021; accepted 5 August 2021