Where horizontal and vertical surveillances meet: Sense-making of US COVID-19 contact-tracing apps during a health crisis

Jeeyun (Sophia) Baik
UC Berkeley School of Information, USA

Eugene Jang
University of Southern California, USA

Abstract
Analyzing user reviews of seven US digital contact-tracing apps for COVID-19, this article unpacks how the new form of surveillance technology is understood and experienced by individuals during a global health crisis. The findings suggest that the app users felt empowered via self-tracking capacity and expressed community-level care and concerns, including those regarding the marginalized. At the same time, the users were raising doubts over technical effectiveness, navigating varying levels of voluntary choice available, and negotiating privacy concerns depending on the (dis)trust they held of institutional entities behind the governance of the apps. We argue that it is critical to investigate how surveillance technologies are situated across horizontal and vertical relationships in people’s everyday lives to fully understand the individual and societal acceptance and/or refusal of the very systems during crises.

Keywords
COVID-19, mobile apps, digital contact tracing, surveillance, privacy, crisis informatics

Corresponding author:
Jeeyun (Sophia) Baik, Center for Long-Term Cybersecurity, UC Berkeley School of Information, Berkeley, CA 94720, USA.
Email: jsbaik@berkeley.edu
Introduction

COVID-19 rapidly spread across the world and resulted in more than 228.5 million confirmed cases in nearly 200 countries by September 2021 (“Covid map,” 2021). Since the outbreak of the pandemic, there have emerged various efforts to flatten the curve, and one of those attempts has centered around tracking individuals who were in close contact with confirmed patients (Ferretti et al., 2020). While traditional contact-tracing methods such as health officials manually recording information from patients about who they encountered in the past few weeks remain important, digital contact-tracing approaches were invented to complement the traditional methods as the spread of COVID-19 became unprecedented (Kleinman & Merkel, 2020). These digital contact-tracing methods often use Bluetooth-based and/or Global Positioning System (GPS)-based technologies, which inform people of their possibility of having been in close physical contact with those with positive test results during the previous weeks. The development of these apps is initiated by governments or driven by technology companies—in the United States (US), for example, Google and Apple worked together to build a Bluetooth-based application programming interface (API) system which is used for various contact-tracing apps (Sharon, 2020; Yang et al., 2020).

Previous studies have suggested that utilizing information communication technologies (ICTs) to trace contacts increases efficiency in health surveillance and risk assessment (Chua et al., 2020; Ferretti et al., 2020). As such, the discourse surrounding contact-tracing apps is heavily weighted on the technical effectiveness and efficiency of these technologies. While these newer contact-tracing methods are expected to help contain the spread of the virus if successful, they also raise several concerns over privacy of the users’ data as well as their effectiveness considering the digital divide and low download rates (Blasimme & Vayena, 2020; Ferretti et al., 2020; Sharon, 2020). Dilemmas are often brought up over a so-called “trade-off” between public health and privacy, coupled with long-term concerns such as increased state surveillance, discrimination, and reinforcement of self-discipline (French & Monahan, 2020; Rowe, 2020; Vitak & Zimmer, 2020). However, there has been a lack of attention given to actual individuals’ experiences using these apps, especially in terms of various relationships people are navigating (e.g., horizontal relations with self, family, or community, and vertical relations with government agencies or companies) as they decide to adopt or refuse the surveillance technology.

This study examines seven US digital contact-tracing apps developed to reduce the spread of COVID-19, focusing on the user perceptions and experiences of the surveillance technology through relational lenses. Analyzing user reviews available on the App Store and Google Play, we aim to interrogate diverse relational dimensions the contact-tracing apps are mediating, which has implications for our understanding of the use of mobile surveillance technology in the current pandemic. Bridging crisis informatics literature with privacy/surveillance studies, we deviate from a binary approach to surveillance technologies as either negative or positive, but instead suggest teasing out the horizontal and vertical relationships that are not equally perceived or lived along diverse lines of marginality and power. This study explores the following research questions:
1. How do contact-tracing app users perceive their own as well as other people’s experiences of the apps?
2. How do they make sense of institutional entities that develop and govern the apps?

Our analysis reveals that contact-tracing apps often function as affective and discursive sites of solidarity and empowerment in horizontal terms, while the users’ privacy concerns over vertical surveillance remain regarding institutional bodies behind the apps’ governance.

**Mobile technology during crises**

Crisis informatics is “broadly defined as the interconnectedness of people, organizations, information and technology during crises/disasters” (Hagar, 2014) and “views emergency response as an expanded social system where information is disseminated within and between official and public channels and entities” (Palen et al., 2009). Tan et al. (2017) conducted a systematic review of crisis informatics literature on “built-for-disaster-purpose” mobile applications (as opposed to general-purpose apps such as Twitter or Facebook) and discovered that these apps serve five main purposes, including crowdsourcing for data, fostering collaboration, notifying, alerting, and informing the public. In addition to serving different roles, these apps facilitate different types of interactions between the public and authorities. Notification apps such as “My112” are geared more towards a one-to-one interaction as the alert is sent from one entity/agent to an individual, whereas apps that are mainly used for information sharing or collaboration like “SignAlert” facilitate many-to-many interactions between its app users (Romano et al., 2016).

Contact-tracing apps do not fall under a clear-cut category in terms of interaction type, but rather present an example of a crossover where “many-to-one-to-many” interactions occur (Tan et al., 2017). Apps of this type aggregate information from the public (i.e., app users) and send it to an official channel/entity (e.g., local governments or health agencies), which is then redistributed back to the public. Contact-tracing apps, indeed, crowdsource and disseminate information from and to the public, while the information is mediated by an app built and managed jointly by government entities such as local governments or health departments as well as commercial tech companies like Google and Apple. Although in most cases personal information is encrypted and stored in a decentralized manner, the fact that it is mediated by a government-built app results in mixed reactions from the public, mainly due to privacy concerns.

Despite potential merits of contact-tracing apps, privacy concerns remain as a factor hindering the wide adoption of these apps (Redmiles, 2020; Walrave et al., 2020; Zhang et al., 2020). A survey showed that over half (54%) of US adults think it is unacceptable for the government to use people’s cell phones for contact tracing (Anderson & Auxier, 2020). Thus, what matters would be if adoption of digital contact tracing is voluntary or mandatory. Unlike many Asian countries (e.g., China and South Korea) where the use of contact-tracing apps is mandated to a certain extent, the adoption of contact-tracing apps in the US is largely voluntary and the app
designs differ from state to state (Yang et al., 2020). However, various institutional set-
ingings (e.g., schools or workplaces) in the US can make using digital contact tracing man-
datory or strongly recommended. Therefore, users’ perception of and willingness to use
contact-tracing apps are contingent on the complex dynamics among the public, local
institutions, state governments, tech companies, and the technology itself. The framework
of crisis informatics which analyzes the interconnectedness and intersecting trajectories
across diverse actors and information technology in times of uncertainty (Hagar, 2014)
can provide a useful lens to unpack how people are making sense of contact-tracing
apps to cope with a public health crisis.

Surveillance technologies in horizontal and vertical terms

Surveillance technologies such as contact-tracing apps, while often considered to be
monolithic, mediate various relationships and power in a society. It is important to inves-
tigate such relational dimensions of surveillance technologies if we hope to fully under-
stand their manifestations and implications. People’s acceptance or rejection of
surveillance is embedded in the complex relationships they are part of in everyday
lives. For example, studies on privacy calculus have suggested that individuals calculate
the costs and benefits of exchange between information and privacy, and called it a
“privacy paradox” when individuals opt into disclosure of personal information despite
their high valuation of privacy (Barnes, 2006; Chen, 2018). Even those who show
great concerns over privacy readily trade their information for other benefits such as grati-
fication, economic incentives, and social capital (Debatin et al., 2009; Ellison et al., 2011;
Lee et al., 2013). However, such conceptualization can lead to a dichotomous framing of
privacy as an individual value that can be or should not be traded off for other individual
or social advantages without any further contextualization.

In fact, when and why individuals accept or resist surveillance technologies and how
they perceive their experiences of the technologies are multi-faceted. Scholars have often
teed out the complexity of these relational dimensions by categorizing them into hori-
zontal and vertical terms (i.e., whether the relationships between the watcher and the
watched are horizontal or vertical) (Quinn et al., 2019). At an individual level, surveil-
lance technologies have provided people with self-tracking capabilities regarding their
health and wellbeing. With the growing wearable industry and the increased use of
Big Data analytics (Li et al., 2021), myriads of mobile applications have enabled
people to track health information about themselves ranging from dietary habits to
sleep patterns. Self-monitoring activities are at times critiqued to be too reliant on the
quantification of bodies, likely resulting in loss of “social and environmental complexity”
and reinforcement of “normative and normalizing ideals” about wellness (Sharon &
Zandbergen, 2017, p. 1697). In contrast, these activities can also positively affect indivi-
duals’ wellbeing and empower them (Ayobi et al., 2020; Nafus & Sherman, 2014; Sharon &
Zandbergen, 2017).

Studies have further suggested concepts of “lateral surveillance,” “participatory sur-
veillance,” “social surveillance,” or “participatory sensing” to describe the horizontal
type of surveillance. Lateral surveillance means peer-to-peer monitoring geared to
romantic partners, family, and friends or acquaintances (Andrejevic, 2004). Similarly, Albrechtslund (2008) suggested that surveillance can be “a mutual, horizontal practice” (i.e., “participatory surveillance”). He shed light on the ways surveillance within “flat” relationships can empower individuals to be active participants who “take action, seek information and communicate.” He particularly questioned the popular implicit understanding of surveillance as an “undesirable” state, pointing out that when individuals are “voluntarily engaging with other people and constructing identities,” their participatory surveillance is a “sharing practice” rather than an “information trade.” Marwick (2012) further developed the notion of “social surveillance” as an overarching term to explain such distinctive forms of micro-level, decentralized, and reciprocal surveillance enabled through social technology. Also, Shilton (2010) unpacked her concept of “participatory sensing,” explaining that data captured by technologies which embrace local control, participation, transparency, and social justice provide “possibilities for self-exploration, community discovery, and new knowledge creation” (p. 132). While horizontal surveillance systems may not be always voluntary, these studies speak to the social aspects of surveillance technologies individuals consider. Recent studies on diverse forms of contact-tracing systems in China and South Korea have found that people often approve these technologies to “care for” and “protect” others in the community (Kim et al., 2021; Liu & Graham, 2021).

When it comes to vertical surveillance, people’s perception and experience of surveillance can vary as well, depending on their level of trust in institutional entities. Trust has been identified as an important mediating factor in the adoption of a product, service, or technology in general (Fukuyama, 1995; van Velsen et al., 2015). Studies have found that trust in the authorities affects people’s willingness to adopt contact-tracing apps in the US (Hargittai et al., 2020), the UK (Horvath et al., 2020), and other European nations like France, Germany, and Italy (Altman et al., 2020). In addition, scholars have elucidated that people may accept vertical surveillance out of feeling helplessness when there are no practical options to choose otherwise (Draper & Turow, 2019). Moreover, discriminatory exclusions of people from benefits of surveillance systems have been documented as well (Gilman & Green, 2018; Madden et al., 2017; Sadowski, 2019). Gilman and Green (2018) pointed out that as much as “too little privacy” (i.e., unfair scrutiny) is problematic, certain populations experience “too much privacy” as they “remain outside of the mainstream data flows,” resulting in limited “societal protections, resources, and support” for them (p. 285).

In addition, the media’s discursive language inducing fear can lead to the legitimization and encouragement of surveillance. Agamben (2005) argued that during a crisis, exceptional state power is legalized (i.e., “state of exception”). A health crisis is often framed as a threat to homeland security, legitimizing nationwide surveillance. Harrison (2016) noted that discursive efforts of the state and media surrounding diseases such as HIV/AIDS and severe acute respiratory syndrome (SARS) deployed war metaphors and militaristic terminology. Similarly, the media has frequently framed the COVID-19 pandemic using war metaphors (Chapman & Miller, 2020). In fact, increased surveillance has been observed across both democratic and undemocratic countries after the outbreak of COVID-19, with varying levels of enforced or recommended (voluntary) measures (Akbari, 2021; Liu & Graham, 2021; Marciano, 2021; Trottier et al., 2021). For
instance, the Israeli government took safety-oriented, militaristic approaches as soon as the World Health Organization (WHO) declared the COVID-19 pandemic (Marciano, 2021), while the Iranian government showed a less oppressive, minimal response (Akbari, 2021).

What these studies suggest for the investigation of digital contact-tracing apps is that, in addition to the varied manifestation of technologies, the ways individuals accept or resist the very technologies on the ground will not always show coherent and consistent patterns. Their perception and experience of digital contact-tracing apps are imagined, negotiated, and contested by various social relationships they are situated in. Building upon insights from these studies, we aim to understand how contact-tracing app users experience and imagine their use of the apps.

Method

This study collected publicly available user reviews from seven US digital contact-tracing apps launched on the App Store and Google Play (see Table 1). We chose to focus on the seven apps based on their roll-out dates before September 2020, so that by the time we were collecting reviews, the apps were exposed to users for a minimum of two months. Data was collected from October 21 to October 22, 2020. A total of 457 reviews and 787 reviews were collected from the App Store and Google Play, and the average lengths of the reviews were 53.31 words (App Store) and 26.95 words (Google Play), respectively. Data was scraped using a software called Octoparse, and the collected data include: (a) store type (i.e., App Store, Google Play); (b) date of review; (c) username; and (d) review comment. The username was used only for cross-checking purposes to see if there were multiple reviews left by the same individuals. We did not incorporate any usernames, and paraphrased direct quotes from the reviews when presenting the findings to make it hard to search for them. The study was approved by the Institutional Review Board of the university the researchers are affiliated with.

We conducted a qualitative thematic analysis, which is a method identifying meaningful themes and patterns that emerge across a dataset. It is a method suitable to explore participants’ lived experiences, analyze their views about a certain phenomenon, and examine dominant patterns of meaning surrounding it (Braun et al., 2019). We first closely read the reviews of HealthyTogether, and collectively identified emerging themes and agreed upon a set of preliminary codes. Then, each of us was allocated a portion of remaining reviews and individually identified which thematic category the reviews fall under. After finishing individual coding, we discussed and clarified the results together in terms of any discrepancies and insights, synthesizing newly added codes and existing codes. We repeated this process until we reached an agreement. We organized the findings around two major threads: horizontal surveillance and vertical surveillance. We do not provide quantitative reporting of the distribution of negative and positive reviews as our unit of analysis was not ‘a review’ per se but rather phrases or sentences within a review, and a single review can comment on both positive and negative aspects of an app.
| Contact-tracing app        | State(s)                               | Technology                        | Developer                        | Roll-out date<sup>b</sup> | Number of reviews | Average review length (in words) | Number of installs<sup>c</sup> |
|----------------------------|----------------------------------------|-----------------------------------|----------------------------------|---------------------------|-------------------|-------------------------------|-------------------------------|
| Care19 Diary               | North & South Dakota                   | Location                          | ProudCrowd                       | April 7, 2020            | 140               | 48.01                         | 50,000+                       |
| Healthy Together           | Utah                                   | Bluetooth & Location              | Twenty Inc                       | April 22, 2020           | 129               | 47.06                         | 100,000+                      |
| COVID WISE                 | Virginia                               | Bluetooth<sup>a</sup>             | SpringML                         | August 5, 2020           | 138               | 36.33                         | 100,000+                      |
| Care19 Alert               | North Dakota, Wyoming                  | Bluetooth<sup>a</sup>             | ProudCrowd                       | August 12, 2020          | 4                 | 50.50                         | 10,000+                       |
| GuideSafe                  | Alabama                                | Bluetooth<sup>a</sup>             | MotionMobs (University of Alabama at Birmingham) | August 16, 2020          | 11                | 72.19                         | 100,000+                      |
| Covid Watch                | Arizona                                | Bluetooth<sup>a</sup>             | COVID Watch (non-profit)         | August 18, 2020          | 15                | 64.47                         | 5,000+                        |
| Covid Trace                | Nevada                                 | Bluetooth<sup>a</sup>             | Dudley Carr, Wes Carr, Josh Gummersall | August 22, 2020          | 20                | 54.60                         | 100,000+                      |

<sup>a</sup>Google-Apple API; <sup>b</sup>based on App Store; <sup>c</sup>based on Google Play (as of January 13, 2021).

The dates the reviews were collected (October 21–22, 2020) and the numbers of installs that were recorded (January 13, 2021) are not identical. Thus, the install numbers should not be expected to be correlated with the number of reviews we were able to collect. This information is only shared to provide an additional context as to which states might have been more successful in garnering the individuals’ awareness of and interest in the technology.
We acknowledge the limitation of using selected app reviews for our research. As the individuals who left reviews were likely motivated enough to leave the comments based on their positive or negative engagements with apps, our analysis of the reviews might be skewed with a self-selection bias. Also, the collected reviews only covered the period between April and October 2020. Thus, we do not attempt to generalize our findings to the larger population’s experience or to the entire pandemic period. Instead, we focused on exploring possible accounts of contact-tracing apps as reflected in the reviews from the earlier stage of the pandemic. While we recognize that the user perception and experience of the same apps may have evolved over the extended pandemic period, examining the early discourse around digital contact tracing is beneficial to comprehend how the new form of surveillance technology was accepted, resisted, and negotiated by everyday people at its introduction stage.

The “many”: user perception and experience of horizontal surveillance

*Empowerment through self-monitoring*

Considering an individual’s relationship to self in the context of horizontal surveillance, users across the contact-tracing apps were often feeling empowered as they coped with the uncertainty of the pandemic by monitoring and interacting with their own health data. These users expressed that they gained psychological relief or peace of mind. Some of them specifically mentioned their chronic conditions or personal attributes such as having health issues or diseases, being elderly, or having a high-risk occupation. For instance, a HealthyTogether user said: “I’m 74, a diabetic and frankly, overweight. Thanks for the boots on the ground.” Another user said: “Being high risk, it’s just another way I feel I can stay safe and know I can be informed if I come in contact with someone with the virus.” Users further talked about the confidence they gained to fight the pandemic: “Having this app makes me feel more confident that our community leaders are working to keep us safe” (HealthyTogether). These findings are in line with previous studies which showed that self-tracking activities can positively affect individuals’ emotional well-being, help them deal with everyday life, and foster meaningful experiences with their personal health (Anderson & Auxier, 2020).

Individuals also felt less like a victim and more secure. A HealthyTogether user said: “I’m proud of your work that keeps me safe. The app, the masks, the updates, the guidelines all are empowering. I don’t feel like a victim.” Likewise, a COVIDWISE user stated: “I feel safe as this will add an extra layer to our health!” Moreover, users often believed that these apps could help curb the pandemic and let them return to a normal life. A COVIDWISE user optimistically said: “This will take us back to as close to normal as we can.” As reflected in these reviews, contact-tracing apps were empowering their users by mitigating anxiety, letting them feel safer, and giving a sense of hope that their life will soon be normalized. The users not only perceived contact tracing as a tool to control their body’s potential exposures to the virus, but
also envisioned it as a facilitator that helps go back to normal. Like other self-tracking technologies, contact-tracing apps appear to foster the restoration of agency and autonomy over individual bodies in this unsettling health crisis (Sharon & Zandbergen, 2017), and the identity of each individual (e.g., health condition, age, occupation) plays a role in their perception of the surveillance technology.

Community-level care and concerns

Contact-tracing apps also mediate many-to-many interactions among citizens, helping them cope with a health crisis through collaborating with and concern for community members. “Community” here refers to not only the app user community in which the user reviews inform others by offering feedback regarding the app (Khalid et al., 2015; Vasa et al., 2012), but also a broader community perceived by each user such as their family, neighbors, or fellow state residents. These apps operate on the basis of health information voluntarily reported by individuals (i.e., COVID test results) which are then sent back to fellow citizens as proximity alerts through the apps. Due to this crowdsourced nature, we observed a community-level identity in action, as the concept of “participatory surveillance” suggests (Albrechtslund, 2008). Users encouraged others to download the app in hopes of mass adoption, for example. A user of HealthyTogether claimed: “Everyone needs to download this app to keep each other safe. Please stay strong and continue to follow recommendations from our health officials. We can emerge stronger if we do this together.” Some users tried to persuade those who are reluctant to use the app by sharing their own perspectives: “It is safe, secure, and helpful. It doesn’t infringe on personal data while just using Bluetooth, (just phone to phone), so it’s a no brainer. The toll will be WASTED if we do not participate” (COVIDWISE). There were users who further encouraged others to promote this app to people around them: “Let your beloved ones know this app and ask them to download it. It can save their life. The more people download it, the better” (COVIDWISE).

Also, users emphasized citizens’ responsibility and obligation to curb the pandemic as a member of society without being polarized or segregated. A COVIDWISE user contended: “Our species is dying. We can beat this together. Stay six feet apart. Wear your masks. Stop taking sides along politics, skin color, or gender. Bless u all.” Indeed, adopting a contact-tracing app was seen as a critical way to contribute to community health:

With this app, I can help ensure others’ well-being, especially the well-being of the most vulnerable among us. Happy to help fight COVID-19. (HealthyTogether)

I gladly signed up for COVIDWISE … what can I personally do to help fight the spread of Covid-19? COVIDWISE helps me do MY part in my community. (COVIDWISE)

As such, users often conceived their participation not as a burden but rather as a matter of course. Users’ acceptance and promotion of the surveillance technology was in consideration of a broader community around the app users, such as their beloved ones,
neighbors, the vulnerable, and even the human species as a whole. In this regard, some users were criticizing fellow state residents who they think threaten community health with irresponsible behaviors: “I’m so glad Utah is doing this! Too many people in the state’s southern and rural parts aren’t taking COVID-19 seriously enough … people are gathering to have fun without social distancing or wearing masks” (HealthyTogether). These reviews imply that digital contact tracing has embodied lateral or participatory surveillance (Albrechtslund, 2008; Andrejevic, 2004); users formed their identity as responsible members of the community and started to reproach those who deviated from it (Trottier et al., 2021).

Considering that the US digital contact-tracing apps varied from state to state, such identity construction/manifestation was often based on one’s state residency. For example, there was a demand for wider implementation of contact tracing by expanding these apps to other states or developing a nationwide app. An individual from a state that did not have an equivalent app suggested: “It is awesome that Utah is doing this, but will you make it available for Massachusetts? [W]e really need this too!” (HealthyTogether). Likewise, another user asked: “It’s ridiculous that we have only state apps. I don’t see an app for California. Also, what about people who cross state borders? We need a unified federal App, but I can’t see it happening” (COVIDWISE). As such, the existence of contact-tracing apps in some states and lack thereof in other states might have been inviting senses of both solidarity and alienation in the US, as those who live in the states with contact-tracing apps encourage fellow residents to adopt them while those who live in the states without any apps cannot reap perceived benefits of the surveillance technology.

Certain technical and user experience (UX) limitations also made users concerned about their alienating effects for some community members (e.g., vulnerable populations or the elderly). Users pointed out the lack of awareness and the limited accessibility of the apps. A Care19Diary user said: “The poor and the elderly won’t use this … so there will be limited information.” Another user also mentioned that “[i]f you’re designing an app that requires everyone to use it, you should make sure that you have considered the needs of all users, including those with disabilities or visually impaired.” The individuals were worried about the exclusion of those at the margins of society caused by inadequate outreach efforts and non-inclusive app designs. Marginalization problems arose when people tried to download the apps as well, since the apps usually work only on the most recent software:

While this app is promising and can help with contact tracing, it is not compatible with older OS [operating systems] & phone systems. This leaves out a large group of people and data points, which will also disproportionately affect vulnerable populations. (GuideSafe)

Considering the expensive average price of newer smartphones, such software requirements are inevitably excluding those who cannot afford these devices. Surveillance through contact tracing was perceived by its users as a way to care for and protect community members, including the most vulnerable. The individuals perceived that the exclusion of anyone would impair the collective benefits of being in the surveillance system as a community.
The “one”: contact-tracing apps as a mediator of vertical surveillance

Contact-tracing apps are crowdsourcing close contact information and disseminating it back to citizens as alerts, while functioning as a mediator (the “one”) in the many-to-one-to-many interaction model. These apps function as a hub where individuals’ information flows before reaching fellow citizens. Even though these apps make it clear that data is encrypted and stored in a decentralized manner, the apps can raise concerns of vertical surveillance as they were initiated by government entities. Our findings reflect that the user perceptions of vertical surveillance were intertwined with several different factors.

Questioning technical effectiveness

First, users expressed frustration about the ineffectiveness of vertical surveillance through contact-tracing apps due to technical malfunctions. The informativeness and accuracy of contact tracing mattered to users. For example, users were often confused about what metrics mean (e.g., “risk level ranking” in COVIDWatch) or what an “exposure notification” tells them when it does not offer any specifics (e.g., GuideSafe). A user criticized:

> Notification offers no information! I was notified of a possible exposure, but the app only told me the day. It did not provide how long or at what distance. […] Please give me more information if you want me to take your recommendation to quarantine seriously! (GuideSafe)

Lack of explanation was making the users feel frustrated and even discouraged from taking other necessary actions. Moreover, there were reported cases of inaccurate tracking in the case of Care19Diary in particular. The inaccuracy provoked users’ doubts over the effectiveness of contact tracing. One Care19Diary user said: “Saved locations are inaccurate, and the app is not accurately tracking exposure risk.” The app did not provide users with any features that allow them to manually edit locations either. As such, the breach of technological promise made by institutional entities (i.e., technical glitches and the resultant ineffectiveness of contact-tracing apps) can function as a barrier to individuals’ adoption or continued use of contact-tracing apps.

Implications of voluntariness

The issue of voluntary versus mandated use can further complicate how users perceive contact-tracing apps. For instance, technical malfunctions can be particularly detrimental to people who are required to use the app for institutional purposes. Several users expressed their frustrations as below:

> Terrible. Because of this app’s malfunctions, I cannot enter any of the buildings at my school. I couldn’t even eat today because of it. Some universities require this app to be working correctly to even be on campus. So, these problems are unacceptable. (GuideSafe)
In fact, GuideSafe has promoted institutional use of the app since its early days, officially partnering with various organizations, most of which are schools and universities. Some mandate the use of the app (e.g., Alabama State University) while others encourage it (e.g., University of Alabama). Thus, institutional entities behind vertical surveillance are multi-folded since the level of “voluntariness” in adopting digital contact-tracing apps in the US may differ from local organizations to state and federal governments. Adoption of contact-tracing apps may not be a matter of choice for an individual who works in an organization that mandates its use even though it is voluntary at the state level.

We additionally located users feeling helpless about the general lack of meaningful choices for them to opt out of surveillance technologies. Users acknowledged the pervasive nature of corporate and government data practices even in non-pandemic times. A COVIDWISE user said: “For all you people worried about the government tracking you, if you have a cell phone you are trackable, so not installing this app or any other is not going to make you safe from being tracked.” This implies that people often feel “helpless” about ubiquitous surveillance where individuals are not given meaningful options (Draper & Turow, 2019), and instead choose to leverage what they could do in times of crisis given the context. There were more sarcastic comments, like “Do the reviewers that are worried about privacy realize they’re using google now? You already sold your soul.” As such, the users’ adoption of or resistance to the contact-tracing surveillance technology was often due to the broader societal state of always-on vertical surveillance that individuals perceive as something they cannot escape effectively. These all point to the complexity of meaningful and voluntary choices available to individuals for digital contact tracing as they need to navigate multi-faceted vertical relationships.

Trust and distrust

Another factor that affects individuals’ perceptions on vertical surveillance is the level of trust they have in institutional entities. On the one hand, users showed trust in local governments and technology companies behind contact-tracing apps for taking their health seriously and crystallizing a safety measure in a timely fashion. For example, HealthyTogether users applauded the Utah government for enabling them “to fight this pandemic and restart the economy in responsible ways” and also thanked developers for building the app “so quickly AND polished.” These reviews allude to their trust in institutional entities: people adopt the surveillance technology when they trust those behind it, but they also start to trust institutions more as they see the surveillance technology as a necessity in times of a crisis like the current pandemic.

At the same time, using Bluetooth technology that does not collect location data as well as privacy policies that detail how personal data are handled appeared to facilitate user trust. For example, users often tried to explain the Bluetooth technology to skeptics, highly emphasizing that Google-Apple’s system does not collect any geolocation data and does not share any sensitive information:

I value my privacy very much, and this app respects that. It doesn’t record any locations. It generates an anonymous ID on each phone and uses Bluetooth to tell which other IDs you
were near … It does not track location or the owner of the phone, only the anonymous IDs.
(COVIDWISE)

These users tried to unpack how Bluetooth-based contact tracing works, and encouraged the others to study the technology before criticizing the apps for privacy issues. Some users were also explicitly calling out those who are skeptical of the Bluetooth-based apps. A COVIDWISE user said: “Please try to learn about the technology … instead of believing conspiracy theories, thinking everyone is out to steal your data.” On the flipside, distrust of non-Bluetooth-based systems existed as well. A HealthyTogether user said:

The HealthyTogether app ignores what Apple and Google built. It sends location data to a centralized server, and this location data is linked to personal data. It’s built by a small social media startup—if they’re hacked, all our personal data will be at risk.

The users of HealthyTogether frequently shared their privacy concerns over various types of personal data being collected by the app beyond location data, including contact lists, phone numbers, and information about medical conditions (e.g., heart disease, weight). These concerns were in part due to HealthyTogether being a location-based app in the beginning. Another possible reason is that HealthyTogether offers a symptom-check feature where users are encouraged to self-report any symptoms daily. HealthyTogether users often urged the app developer and the local government to switch over to Google-Apple’s system. A user asserted: “Switch to the privacy-first Apple and Google’s system, and I will gladly participate.”

As these concerns center around misuse of sensitive data, users emphasized the importance of privacy policies to trust digital contact-tracing apps. A COVIDWISE user said: “The privacy policy is a breath of fresh air. I was glad to see this app that doesn’t take advantage of this pandemic to collect and sell user data.” A HealthyTogether user also commented: “I was a little skeptical at first until I read that everything gets deleted after 30 days.” As such, the users were actually reading privacy policies of these apps offered by institutional entities, and the policies provided some level of comfort to them.

However, it was still not clear to users as to who has access to their personal data collected by the apps and to what extent the data may be used, reinforcing/resulting in distrust of the institutional entities. A HealthyTogether user asked: “I want to know where my information goes. Who checks this? Department of health?” A COVIDWISE user also claimed: “This app takes your metadata and assigns it a number. It reports your information to the government … DELETE.” Individuals also talked about long-term implications of the apps. Several HealthyTogether users drew an analogy between the app and George Orwell’s novel 1984, calling it “intrusive,” “Big-brother,” or “Draconian 1984 Spyware.” These privacy concerns ranging from data misuses to an Orwellian worldview speak to the varying levels of institutional distrust the US public have. The app reviews showed public distrust in federal and local governments as well as technology companies:
No one should track private citizens. It is an unconstitutional overreach by our local, state and federal governments. (HealthyTogether)

The developers are willing to share your data with the authorities. (Care19Diary)

As shown in the examples, users considered the governments’ tracking of private citizens to be “unconstitutional” and flagged slippery data sharing between public and private sectors. Studies have identified trust to be a core value for people to negotiate whether and to what extent they would share personal information with institutions (Marwick & Hargittai, 2019), and such institutional (dis)trust is related to people’s willingness to adopt contact-tracing apps (Hargittai et al., 2020). Our findings similarly found that users of the US contact-tracing apps often expressed their privacy concerns along with their distrust in corporations and governments.

**Discussion: the relational turn of surveillance technology in crisis**

The findings of this study show that, while contact-tracing apps often raise privacy concerns in terms of vertical surveillance (i.e., surveillance by institutional entities), they are also considered an infrastructure that allows individuals, in horizontal terms, to feel empowered and care for their community. Users across the apps reported feeling safer and empowered as they could self-track their health, encouraging others to download the apps to ensure the surveillance technology’s effectiveness for society at large. Such sense-making of the apps was particularly expressed in forms of identification and solidarity with community members, facilitated by the crowdsourced or “many-to-many” nature of digital contact tracing (Tan et al., 2017). As Albrechtslund (2008) suggested, these app users were “voluntarily engag[ing] with other people and construct[ing] identities” as a member of the larger community, embracing “participatory surveillance” as a “sharing practice” rather than an “information trade.” In this context, the users were also criticizing the apps’ alienating effects. Individuals enthusiastic about doing their part for society questioned how the apps could be more inclusive of vulnerable populations (e.g., those who cannot afford the latest devices, elderly people, or people with disabilities). The issue of exclusion was also mentioned regarding the gap between residents who are living in states that released contact-tracing apps and those who are not. These imply that people’s acceptance or rejection of surveillance is embedded in various self-perceptions and interpersonal relationships they are part of in everyday lives.

Users’ perceptions and experiences of the apps were situated in their vertical relationships with institutions as well. On the one hand, technical malfunctions were leading users to question the effectiveness of digital contact tracing as they adopted vertical surveillance in expectation of informative and accurate tracking. The breach of technological promise can discourage the individuals’ continued use of the surveillance app. On the other hand, whether the contact-tracing apps give individuals meaningful choices was questioned. While contact-tracing apps in the US remain largely voluntary (which may have led to more positive responses among those who opt-in to it, compared to other countries mandating it), some institutional settings (e.g., schools, workplaces) were
requiring the use of contact-tracing apps, thus complicating these users’ experience of the surveillance technology. Users further expressed their “helplessness” (Draper & Turow, 2019) in meaningfully choosing privacy in an era where surveillance is by default regardless of crisis. As they felt their data is always surveilled anyway, they accepted digital contact tracing to help contain the spread of the virus. Here, (dis)trust in institutional entities behind contact-tracing apps mattered. Some users appreciated local governments and corporate developers for their rapid and tangible responses to the public health crisis (i.e., early roll-out of contact-tracing app). The Google-Apple’s Bluetooth-based system which does not collect location data as well as privacy policies of the contact-tracing apps appeared to help foster trust. Other users still raised privacy concerns as the apps function as a mediator (the “one”) in the many-to-one-to-many information flow during the crisis (Tan et al., 2017). These users considered the governments’ tracking of private citizens to be concerning and flagged slippery data sharing between public and private sectors. They also warned of Orwellian long-term implications of the surveillance technology introduced and fixated in society.

All these findings point to the importance of teasing out a complex set of relationships a surveillance technology intersects with. We cannot fully understand how surveillance technology is made sense of and used by people on the ground, unless we look at various relational dimensions the technology mediates and the context of crisis communication the technology emerges from. What digital contact tracing promises to people is the protection of not only the individuals, but also those they are connected to as either households, neighbors, fellow state residents, or even a human species. Furthermore, individuals hold different relationships with corporations and governments that introduce the technology and govern the data processed through it. Therefore, neither blanket societal approval nor refusal of the surveillance technology will ever suffice. We argue that individuals’ acceptance of or resistance to surveillance technologies in practice will not be coherent. The very divergence can imply (un)expected marginalization of certain populations for both “too little privacy” and “too much privacy” (Gilman & Green, 2018). Most recent studies on COVID-19 tracking apps/algorithms in Asian countries have suggested such a relational turn to the understanding of digital contact tracing as a surveillance technology (Kim et al., 2021; Liu & Graham, 2021), and the need for relational examination of surveillance technologies is not and should not be limited to a particular culture (e.g., collectivist vs. individualistic cultures). Our study identified patterns of both “care” and “concern” for community members together with institutional (dis)trust and ongoing privacy concerns in the US context that is not generally deemed a collectivist culture. Thus, more nuanced investigation of how surveillance technologies are embedded across horizontal and vertical relationships is a key area for ongoing research at the intersection of mobile communication, crisis informatics, and privacy/surveillance. We believe that this study illustrates the merits of such conversations going forward.

**Acknowledgements**

We appreciate Media as a Socio-Technical System (MASTS) research collective at the University of Southern California which provided a space for us to incubate the project idea. We also would like to thank two anonymous reviewers for their valuable feedback on the manuscript.
Funding
The authors received no financial support for the research, authorship and/or publication of this article.

ORCID iD
Jeeyun (Sophia) Baik https://orcid.org/0000-0001-5057-1432

Notes
1. My112 is an application developed by Madrid’s local government that sends emergency notifications to users and allows the users to directly contact an official emergency center. SignAlert is a “social platform among citizens in the same neighborhood with the aim of sharing messages about any kind of disasters with photos, texts and locations” (Romano et al., 2016, p. 5).
2. As of December 2021, there are 50 organizations officially partnering with GuideSafe (see https://www.guidesafe.org/about/about-participants/ for more details). While other apps do not provide clear partnership information, it is also known that the University of Oklahoma strongly encourages the use of HealthyTogether (see https://www.ou.edu/together/healthy-together), for instance.
3. HealthyTogether later added Bluetooth-based tracing, but it was still not built on Google-Apple’s API system.

References
Agamben, G. (2005). *State of exception*. Chicago.
Akbari, A. (2021). Authoritarian surveillance: A corona test. *Surveillance & Society*, 19(1), 98–103. https://doi.org/10.24908/ss.v19i1.14545
Albrechtslund, A. (2008). Online social networking as participatory surveillance. *First Monday*, 13(3). https://doi.org/10.5210/fm.v13i3.2142
Altmann, S., Milsom, L., Zillessen, H., Blasone, R., Gerdon, F., Bach, R., Kreuter, F., Nosenzo, D., Toussaert, S., & Abeler, J. (2020). Acceptability of app-based contact tracing for COVID-19: cross-country survey study. *JMIR MHealth and UHealth*, 8(8), e19857. https://doi.org/10.2196/19857
Anderson, M., & Auxier, B. (2020). Most Americans don’t think cellphone tracking will help limit COVID-19, are divided on whether it’s acceptable. Pew Research Center. 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/
Andrejevic, M. (2004). The work of watching one another: lateral surveillance, risk, and governance. *Surveillance & Society*, 2(4), 479–497. https://doi.org/10.24908/ss.v2i4.3359
Ayobi, A., Marshall, P., & Cox, A. L. (2020, April). Trackly: A customisable and pictorial self-tracking app to support agency in multiple sclerosis self-care. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (pp. 1–15). https://doi.org/10.1145/3313831.3376809
Barnes, S. B. (2006). A privacy paradox: social networking in the United States. *First Monday*, 11(9). https://doi.org/10.5210/fm.v11i9.1394
Blasimme, A., & Vayena, E. (2020). What’s next for COVID-19 apps? Governance and oversight. *Science* 370(6518), 760–762. https://doi.org/10.1126/science.abd9006
Braun, V., Clarke, V., Hayfield, N., & Terry, G. (2019). Thematic analysis. In P. Liamputtong (Ed.), *Handbook of research methods in health social sciences* (pp. 843–860). Springer. https://doi.org/10.1007/978-981-10-5251-4_103.

Chapman, C. M., & Miller, D. M. S. (2020). From metaphor to militarized response: The social implications of “we are at war with COVID-19”—crisis, disasters, and pandemics yet to come. *International Journal of Sociology and Social Policy, 40*(9–10), 1107–1124. https://doi.org/10.1108/IJSSP-05-2020-0163.

Chen, H.-T. (2018). Revisiting the privacy paradox on social media with an extended privacy calculus model: The effect of privacy concerns, privacy self-efficacy, and social capital on privacy management. *American Behavioral Scientist, 62*(10), 1392–1412. https://doi.org/10.1177/0002764218792691.

Chua, A. Q., Tan, M. M. J., Verma, M., Han, E. K. L., Hsu, L. Y., Cook, A. R., Teo, Y. Y., Lee, V. J., & Legido-Quigley, H. (2020). Health system resilience in managing the COVID-19 pandemic: lessons from Singapore. *BMJ Global Health, 5*(9), 1–8. http://dx.doi.org/10.1136/bmjgh-2020-003317.

Covid map: Coronavirus cases, deaths, vaccinations by country (2021, September 24). *BBC News*. https://www.bbc.com/news/world-51235105.

Debatin, B., Lovejoy, J. P., Horn, A.-K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication, 15*(1), 83–108. https://doi.org/10.1111/j.1083-6101.2009.01494.x.

Draper, N. A., & Turow, J. (2019). The corporate cultivation of digital resignation. *New Media & Society, 21*(8), 1824–1839. https://doi.org/10.1177/1461444819833331.

Ellison, N. B., Vitak, J., Steinfield, C., Gray, R., & Lampe, C. (2011). Negotiating privacy concerns and social capital needs in a social media environment. In Trepte, S., & Reinecke, L. (Eds.), *Privacy online* (pp. 19–32). Springer.

Ferretti, L., Wymant, C., Kendall, M., Zhao, L., Nurtay, A., Abeler-Dörner, L., Parker, M., Bonsall, D., & Fraser, C. (2020). Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing. *Science, 368*(6491), 1–7. https://doi.org/10.1126/science.abb6936.

French, M., & Monahan, T. (2020). Dis-ease surveillance: How might surveillance studies address COVID-19? *Surveillance & Society, 18*(1), 1–11. https://doi.org/10.24908/ss.v18i1.13985.

Fukuyama, F. (1995). *Trust: The social virtues and the creation of prosperity*. Free Press.

Gilman, M., & Green, R. (2018). The surveillance Gap: The harms of extreme privacy and data marginalization. *NYU Rev. L. & Soc. Change, 42*(2), 253–308. https://socialchangenyu.com/review/the-surveillance-gap-the-harms-of-extreme-privacy-and-data-marginalization/

Hagar, C. (2014). Crisis informatics. *Journal of Geography & Natural Disasters, 4*(1), 1. https://doi.org/10.4172/2167-0587.1000e115.

Hargittai, E., Redmiles, E. M., Vitak, J., & Zimmer, M. (2020). Americans’ willingness to adopt a COVID-19 tracking app: The role of app distributor. *First Monday, 25*(11). https://doi.org/10.5210/fm.v25i11.11095.

Harrison, M. (2016). Pandemics. In M. Jackson (Ed.), *The Routledge history of disease* (pp. 129–146). Routledge.

Horvath, L., Banducci, S., & James, O. (2020). Citizens’ attitudes to contact tracing apps. *Journal of Experimental Political Science*. Advance online publication. https://doi.org/10.1017/XPS.2020.30.

Khalid, M., Shehzaib, U., & Asif, M. (2015). A case of mobile app reviews as a crowdsource. *International Journal of Information Engineering and Electronic Business, 7*(5), 39–47. https://doi.org/10.5815/ijieeb.2015.05.06.
Kim, Y., Chen, Y., & Liang, F. (2021). Engineering care in pandemic technogovernance: The politics of care in China and South Korea’s COVID-19 tracking apps. *New Media & Society.* Advance online publication. https://doi.org/10.1177/14614448211020752

Kleinman, R. A., & Merkel, C. (2020). Digital contact tracing for COVID-19. *Canadian Medical Association Journal,* 192(24), E653–E656. https://doi.org/10.1503/cmaj.200922

Lee, H., Park, H., & Kim, J. (2013). Why do people share their context information on social network services? A qualitative study and an experimental study on users’ behavior of balancing perceived benefit and risk. *International Journal of Human–Computer Studies,* 71(9), 862–877. https://doi.org/10.1016/j.ijhcs.2013.01.005

Li, C., Lin, S. H., & Chib, A. (2021). The state of wearable health technologies: A transdisciplinary literature review. *Mobile Media & Communication,* 9(2), 353–376. https://doi.org/10.1177/205157920966023

Liu, C., & Graham, R. (2021). Making sense of algorithms: Relational perception of contact tracing and risk assessment during COVID-19. *Big Data & Society,* 8(1). https://doi.org/10.1177/2053951721995218

Madden, M., Gilman, M., Levy, K., & Marwick, A. (2017). Privacy, poverty, and big data: A matrix of vulnerabilities for poor Americans. *Washington University Law Review,* 95(1), 53–125.

Marciano, A. (2021). Israel’s mass surveillance during COVID-19: A missed opportunity. *Surveillance & Society,* 19(1), 85–88. https://doi.org/10.1177/2053951721995218

Marwick, A. (2012). The public domain: surveillance in everyday life. *Surveillance & Society,* 9(4), 378–393. https://doi.org/10.24908/ss.v9i4.4342

Marwick, A., & Hargittai, E. (2019). Nothing to hide, nothing to lose? Incentives and disincentives to sharing information with institutions online. *Information, Communication & Society,* 22(12), 1697–1713. http://dx.doi.org/10.1080/13691183.2018.1450432

Nafus, D., & Sherman, J. (2014). Big data, big questions! this one does not go up to 11: The quantified self movement as an alternative big data practice. *International Journal of Communication,* 8, 1784–1794. https://ijoc.org/index.php/ijoc/article/view/2170

Palen, L., Vieweg, S., Liu, S. B., & Hughes, A. L. (2009). Crisis in a networked world: Features of computer-mediated communication in the April 16, 2007, Virginia tech event. *Social Science Computer Review,* 27(4), 467–480. https://doi.org/10.1177/0894439309332302

Quinn, K., Epstein, D., & Moon, B. (2019). We care about different things: Non-elite conceptualizations of social media privacy. *Social Media + Society,* 5(3), 1–14. https://doi.org/10.1177/2056305119866008

Redmiles, E. M. (2020). User concerns 8 tradeoffs in technology-facilitated COVID-19 response. *Digital Government: Research and Practice,* 2(1), 1–12. https://doi.org/10.1145/3428093

Romano, M., Onorati, T., Aedo, I., & Diaz, P. (2016). Designing mobile applications for emergency response: Citizens acting as human sensors. *Sensors,* 16(3), 406. https://doi.org/10.3390/s16030406

Rowe, F. (2020). Contact tracing apps and values dilemmas: A privacy paradox in a neo-liberal world. *International Journal of Information Management,* 55, 1–5. https://doi.org/10.1016/j.ijinfomgt.2020.102178

Sadowski, J. (2019). When data is capital: Datafication, accumulation, and extraction. *Big Data & Society,* 6(1), 2053951718820549. https://doi.org/10.1177/2053951718820549

Sharon, T. (2020). Blind-sided by privacy? Digital contact tracing, the apple/google API and big tech’s newfound role as global health policy makers. *Ethics and Information Technology,* 23(Suppl 1), S45–S57. https://doi.org/10.1007/s10676-020-09547-x


Sharon, T., & Zandbergen, D. (2017). From data fetishism to quantifying selves: self-tracking practices and the other values of data. *New Media & Society, 19*(11), 1695–1709. https://doi.org/10.1177/1461444816636090

Shilton, K. (2010). Participatory sensing: building empowering surveillance. *Surveillance & Society, 8*(2), 131–150. https://doi.org/10.24908/ss.v8i2.3482

Tan, M. L., Prasanna, R., Stock, K., H Doyle, E., Leonard, G., & Johnston, D. (2017). Mobile applications in crisis informatics literature: A systematic review. *International Journal of Disaster Risk Reduction, 24*, 297–311. https://doi.org/10.1016/j.ijdrr.2017.06.009

Trottier, D., Huang, Q., & Gabdulhakov, R. (2021). Covidiots as global acceleration of local surveillance practices. *Surveillance & Society, 19*(1), 109–113. https://doi.org/10.24908/ss.v19i1.14546

van Velsen, L., van der Geest, T., van de Wijngaert, L., van den Berg, S., & Steehouder, M. (2015). Personalization has a price, controllability is the currency: Predictors for the intention to use personalized eGovernment websites. *Journal of Organizational Computing and Electronic Commerce, 25*(1), 76–97. https://doi.org/10.1080/10919392.2015.990782

Vasa, R., Hoon, L., Mouzakis, K., & Noguchi, A. (2012, November). A preliminary analysis of mobile app user reviews. In Proceedings of the 24th Australian Computer–Human Interaction Conference, 241–244. https://doi.org/10.1145/2414536.2414577

Vitak, J., & Zimmer, M. (2020). More than just privacy: using contextual integrity to evaluate the long-term risks from COVID-19 surveillance technologies. *Social Media + Society, 6*(3), 2056305120948250. https://doi.org/10.1177/2056305120948250

Walrave, M., Waeterloos, C., & Ponnet, K. (2020). Adoption of a contact tracing app for containing COVID-19: A health belief model approach. *JMIR Public Health and Surveillance, 6*(3), e20572. https://doi.org/10.2196/20572

Yang, Y., Baik, J. S., Ahn, S. Y., & Jang, E. (2020). Tracing digital contact tracing: Surveillance technology and privacy rights during COVID-19 in China, South Korea, and the United States. *SSRN Electronic Journal, 1–31*. https://doi.org/10.2139/ssrn.3743491

Zhang, M., Chow, A., & Smith, H. (2020). COVID-19 contact-tracing apps: Analysis of the readability of privacy policies. *Journal of Medical Internet Research, 22*(12), e21572. https://doi.org/10.2196/21572

**Author Biographies**

**Jeeyun (Sophia) Baik** (PhD, University of Southern California) is a Postdoctoral Researcher at the University of California Berkeley Center for Long-Term Cybersecurity. Her research examines the politics of technology governance and social justice across stakeholders and regional boundaries, focusing on the issues of data privacy and networked surveillance.

**Eugene Jang** is a PhD student at USC Annenberg School for Communication and Journalism. Her research interests include communication technology, AI-mediated communication, social networks, social support, and issues of inequalities/marginalization.