Privacy Attitudes and COVID Symptom Tracking Apps: Understanding Active Boundary Management by Users*

Jinkyung Park[0000−0002−0804−832X], Eiman Ahmed[0000−0002−7703−9005], Hafiz Asif[0000−0001−9674−7747], Jaideep Vaidya[0000−0002−7420−6947], and Vivek Singh[0000−0002−8194−2336]

Rutgers University, New Brunswick NJ 0890, USA

Abstract. Multiple symptom tracking applications (apps) were created during the early phase of the COVID-19 pandemic. While they provided crowdsourced information about the state of the pandemic in a scalable manner, they also posed significant privacy risks for individuals. The present study investigates the interplay between individual privacy attitudes and the adoption of symptom tracking apps. Using the communication privacy theory as a framework, it studies how users' privacy attitudes changed during the public health emergency compared to the pre-COVID times. Based on focus-group interviews (N=21), this paper reports significant changes in users' privacy attitudes toward such apps. Research participants shared various reasons for both increased acceptability (e.g., disease uncertainty, public good) and decreased acceptability (e.g., reduced utility due to changed lifestyle) during COVID. The results of this study can assist health informatics researchers and policy designers in creating more socially acceptable health apps in the future.

Keywords: COVID-19 · symptom tracking · privacy · boundary management · information boundary theory · communication privacy management theory

1 Introduction

On March 11, 2020, the World Health Organization (WHO) declared the novel Corona Virus Disease 2019 (COVID-19) outbreak a global pandemic, [29] and as of September 15, 2021, approximately 22.5 million confirmed cases of COVID-19, including more than 4.6 million deaths were reported worldwide [28]. In the early months of the pandemic, the population testing for COVID-19 was deficient. The low population testing led to the lack of information necessary to track and curb the spread of the virus. To fill this information gap, many COVID-19 symptom tracking mobile applications (apps) were developed worldwide to generate real-time data about the spread of the virus. Since then, these apps have assisted in

* This material is in part based upon work supported by the US National Science Foundation (Grant 2027789) and National Institutes of Health

identifying specific symptoms of COVID-19 and predicting new hot spots five to six days in advance [8]. On the other hand, these apps collect and utilize peoples' private and sensitive information, raising serious privacy concerns. Therefore, in this work, we study people's privacy attitudes towards COVID-19 symptom tracking apps.

The use of mobile apps in fighting the spread of infectious diseases is not new or specific to COVID-19. In the past, mobile apps have been used to curb the spread of flu, SARS, and H1N1 [32, 27]. Such mobile apps can be categorized into two types: symptom tracking apps and contract tracing apps — collectively, we refer to them as *disease monitoring apps*. A COVID-19 symptom tracking app collects self-reported personal information such as COVID-19 related symptoms, COVID-19 test results, demographic information, health history, and location from its users. It then uses this data to track the spread of the virus, identify emerging hot spots of COVID-19, and predict outbreaks [8, 2, 4]. A COVID-19 contact-tracing app, on the other hand, continuously tracks individuals (e.g., via Global Positioning System (GPS)) to identify and notify them about possible exposure to the virus [19]. Although the two types of apps work very differently, they share a common goal, i.e., to curb the pandemic.

Many users may have shared their information with these apps considering COVID-19 to be a "state of exception," [1] wherein temporary exceptions to existing rights (e.g., freedom of movement or some aspects of privacy) can be justified to preserve the health and security of citizens as a whole. At the same time, the general public and privacy-rights advocates raise concern for users' privacy due to the mass collection of sensitive health, demographic, and location data. They worry that the data collected via COVID-19 related apps could potentially be used for other purposes (e.g., health-insurance risk assessment) rather than to monitor the spread of the infectious disease [31].

Although disease monitoring apps claim to protect data through various privacy-preserving technologies [2, 22], many research studies show that these apps fail to guard the privacy of all people [5, 9, 27, 2]. For instance, Wen et al., [27] identified potential ways of re-identifying individuals in 41 different COVID-19 contact tracing apps. Asif [2] argued that symptom tracking apps that publicly release raw aggregates risk re-identification attacks. Even with advanced privacy-preserving technologies, COVID-19 monitoring apps could still raise individual users' privacy concerns.

In fact, privacy concerns among people are an essential factor in the adoption of disease monitoring apps, as indicated by several recent studies on COVID-19 contact tracing apps. Simko et al., [23] conducted a survey and found that the privacy concerns reduce the likelihood to install a new COVID-19 contact tracing apps. Another survey study by Kaptchuk et al., [10] found that both accuracy and privacy of COVID-19 contact tracing apps are significant influencing factors for their adoption. Williams et al., [30] conducted a focus group study in the U.K. and discovered that privacy attitudes impacted people's willingness to use these apps.

While there is significant literature on users' privacy attitudes regarding health apps, *changes* that occur in individuals' privacy attitudes during pandemic (i.e., a public health emergency) settings are understudied. Hence, this exploratory study aims to understand users' privacy attitudes toward COVID-19 symptom tracking apps and how their privacy expectations change during the pandemic using focus group interviews in the U.S. The study uses communication privacy management as the underlying framework to examine elements of privacy that changed during the pandemic compared to a non-pandemic situation.

To do so, we focus on the notion of "informational privacy," which is concerned with controlling whether and how personal data can be gathered, stored, processed, and disseminated [11]. Furthermore, we focus on privacy attitudes rather than privacy concerns. Though closely related, they are different. Privacy concerns could be generic and, in most cases, are not bound to any specific context, while privacy attitudes refer to the appraisal of specific privacy behaviors in a particular context — here, COVID-19 symptom tracking apps [11].

2 Communication Privacy Management Theory

As online information can be easily obtained and integrated from disparate sources, research efforts have been conducted from various perspectives on informational privacy. Scholarly communities have utilized several theories concerning online information privacy research, including the theory of reasoned action [3], the privacy calculus theory [12], the social presence theory [20], and the protection motivation theory [21]. These theories conceptualize the formation of users' privacy concerns and their subsequent behaviors to provide personal information. Among existing theories of online privacy, a major stream of research that the current work builds upon is the communication privacy management theory (CPM) [16–18] and its adaptation as the information boundary theory (IBT) [24, 25]. These theories are utilized in the present study as constructs of the theories (e.g., privacy turbulence) that offer natural ways to study changes in individuals' privacy attitudes under exceptional circumstances, such as the COVID-19 pandemic.

Using the metaphor of a "boundary," CPM [16] presents a psychological process in which individuals manage their desire for both communication and privacy. According to CPM, individuals balance the tension between intimacy (e.g., revelatory processes through which an individual becomes known to others) and autonomy (e.g., behaviors to protect and separate oneself from others) by negotiating psychological boundaries between themselves and others. In this context, a boundary serves as a "psychological contract" [24] or "ownership line" [17] between oneself and others concerning the amount, nature, and circumstances of requesting, sending, and receiving personal information [24].

The idea of boundary management has been applied across different contexts from early work that focused on communication in close relationships (e.g., marital relationships) [16] to later work that considered the role of information tech-

nology in social relationships [24]. Stanton [24] extended CPM to organizational settings and developed a synthesized theory called the information boundary theory. Using the same boundary metaphor, IBT focuses on individuals' motivations to disclose personal information via a given medium (e.g., messaging system) and in particular social environments (e.g., workplace). The extension of CPM to IBT indicates that individuals frame their use of information technology to transmit information in similar terms to those used in interpersonal relationships (e.g., telling about oneself to others).

CPM and IBT explicate that individuals' decisions on how privacy boundaries are regulated follow the rules for "boundary opening" and "boundary closure" [24], depending on the degree of risk associated with privacy. The boundaries are opened when there is a high probability that people will allow access to private information; hence, information flows freely. In contrast, boundaries are closed when people are less likely to reveal private information; hence, information flow is restricted [18]. In the context of the current study, "boundary" can be seen as an individual's willingness to use the COVID-19 symptom tracking apps. A boundary can be described as "opening" when an individual is more likely to use the apps. On the contrary, a boundary can be "closing" when an individual is less likely to use the apps.

According to CPM and IBT, individuals can articulate a personal "calculus of boundary negotiation" [25] regarding the conditions under which disclosure of personal information is acceptable or unacceptable. Often referred to as "privacy calculus," this mental calculus model suggests that individuals tend to weigh two competing factors (e.g., risks and benefits) associated with the transmission of personal information when they determine whether to disclose personal information [7]. The boundary negotiation processes are not static, but rather "dynamic psychological processes of regulation" [24] that allow people to control the flow of personal information. When privacy rules do not meet an individual's expectations anymore, they are adjusted according to individuals and other people [18]. According to CPM, "privacy turbulence" occurs when "normal" privacy rules no longer work to achieve the expected outcomes of privacy management [18]. In the context of the current study, COVID-19 can be seen as a unique privacy turbulence situation in which individuals' privacy rules no longer operate as they did before and need to be adjusted.

Prior studies of IBT and CPM elaborated several sources of motivation to disclose or withhold personal information. Stanton [24] investigated the use of monitoring and surveillance technologies within organizational settings and suggested that both boundary opening and closing are affected by organizational justice considerations such as mission-relatedness of the information. Recent work by Walters and Markazi [26] focused on the boundary closing resulting from privacy turbulence (e.g., privacy violation) with an individual's voice-activated phone. They reported that the conditions for boundary closing are not stemming from a particular information system but an overall lack of trustworthiness toward the information systems.

While previous research has conceptualized and applied boundary management in different settings, no study has looked into how an extreme health scenario, such as the COVID-19 pandemic, influences the way individuals shift their information boundaries online. Similarly, while some work is emerging on privacy attitudes and COVID-19 tracking app adoption, it has not been undertaken from the lens of CPM and the dynamic boundary management process. Thus, the present study presents the following research question:

RQ1: *How did users' privacy attitudes toward health symptom tracking apps change during the COVID-19 pandemic?*

RQ2: *How did users rationalize their boundary closing and boundary opening behavior during the pandemic?*

3 Methods

3.1 Recruitment and Participants

The present study reports an exploratory study involving three focus groups (N = 21) with United States-based residents aged 18 years or older. Participants were recruited from mailing lists (e.g., alumni mailing lists, community mailing lists, social media) based on their interest in participating in a study related to COVID-19 symptom tracking applications. Interested participants were asked to complete a pre-screening survey to determine their eligibility to partake in the study. Participants 18 years or older, comfortable speaking English, and residing in the United States were deemed eligible to engage in the research. Eligible individuals were sent consent forms and demographic information surveys before the focus group interviews. The authors' Institutional Review Board granted ethical approval for the study, and research participants were provided 50 U.S. dollars as compensation for participating in the study.

Focus group interview sessions with 6–8 participants were arranged on an online video conferencing platform (Zoom) for about an hour each in February 2021, when the United States was primarily still in lockdown and vaccines had yet to be administered to the general public. Participants were divided into three focus groups depending on their usage of symptom tracking apps to facilitate conversations. For instance, participants that had never used an application (group 3, n = 8) were placed into a different group than those who stated having used or currently using a COVID-19 symptom tracking application (group 1, n = 6 / group 2, n = 7). The moderators (the research team) briefly reviewed ground rules before the interviews and informed participants that they could withdraw from the study at any point they wanted. The participants were also informed that they could request assistance in seeking counseling or mental health aid at any time during the focus group interviews. The moderators utilized semi-structured questions to ask participants about their relationship with symptom tracking applications, their symptom tracking application experiences, and the degree to which they feel either comfortable or uncomfortable sharing their personal health information on these applications.

The majority of participants were female (62%) with a mean age range of 18 to 21 (90%) and 1 to 3 years of college education (71%). In addition, most participants were either Asian or Asian American (48%) or Non-Hispanic or White (38%) residing in New Jersey and New York. The participants' family income ranged from less than $25,000 to $150,000 or more, with the median income range of $75,000 to $99,000. Finally, participants reported using four different COVID-19 symptom tracking applications (COVID Nearby, Pace Safe, COVID Alert NJ, My Campus Pass) that were recommended by friends, institutions, or the state.

3.2 Coding Process

The focus group interview questions were developed based on the detailed literature review and the study's goals. All the focus group sessions were video recorded and transcribed verbatim by the research team. The user numbers replaced participants' names to support confidentiality. Data were analyzed qualitatively; the research team compared participants' responses to uncover common themes. Finally, the team developed a coding scheme based on the iterative analysis. The final coding scheme consisted of 19 themes representing the main topics discussed from the three focus groups (see Table 1).

Once themes were established, the research team recruited a coder. Next, the team discussed the established themes with the coder over multiple iterations during March 2021. A sub-sample (10%) of the transcripts was selected to determine the reliability of the developed codes. Inter-coder reliability scores were calculated between the research team and the additional coder to ensure the consistency and validity of the uncovered themes. The average percent agreement was 0.87, and Krippendorff's alpha was 0.83. Both coefficients met the criteria suggested by the existing literature [15, 12] for a good agreement. Finally, the research team and the coder coded the complete transcripts.

4 Findings

Participants from the three focus groups discussed their experience with COVID-19 symptom tracking apps. Given the focus of this study on the *changes* in privacy management during the COVID-19 pandemic, the discussion below focuses on two dimensions of privacy management (boundary opening and boundary closing), along with their central themes and sub-themes.

4.1 Boundary Opening

The first dimension of CPM and IBT explored was "boundary opening," in which individuals are more willing to share their personal information during the pandemic than non-pandemic situations. The five main themes that emerged from the focus group conversations were: (1) severity of the COVID-19 pandemic, (2) uncertainty of the COVID-19 pandemic, (3) protecting themselves and people around them, (4) contributing to the public good, and (5) mandatory use.

Theme	**Definition [example quotation]**
Personal Safety	*Safety of one's self* (health) ["I just wanted to be on the safe side and uh just know if anybody around me has COVID"]
Family Safety	*Safety of family* (health) ["I also use uh the same app because um my family has some health issues and I just wanted to be on the safe side"]
Public Good	*Using applications* (apps) *to contribute to the public good* ["try to contribute as much data as possible"]
Uncertainty	*Uncertainty related to spreading or risk of illness* ["I'm afraid of possibly getting it or possibly give, you know, possibly giving it to someone else even walking by"]
Severity	*Severity and danger of illness* ["It's not as deadly as like um COVID right now"]
Anonymization	*De-linking identity from person's shared data* ["As long as my name and identity remain anonymous, I will be okay with them"]
Data Protection	*How data is protected from unauthorized access* ["Maybe emphasize that like your identity won't be shared with anybody else"]
Mandatory Use	*Using apps because they are required* ["I'm contractually obligated to use it"]
Voluntary Use	*Using apps out of own free-will* ["I just like use it to track the cases and everything"]
Normalization of Loss of Privacy	*Normalization due to society or other applications* ["I think um location tracking is kind of like normalized for me because there are like other apps that like Find my iPhone"]
Desire for Control	*The desire for some control over personal information* ["I think I would want to have control over my own location... so like I'd want like an option for that"]
Transparency	*Clear communication of how data is protected* ["Be like upfront like this is exactly who um has access to your information and... tell us when our information is accessed also, and who accessed it."]
Accuracy	*Whether reported information is accurate* ["I don't know if I believe that every single person at Pace who walks in this building, isn't just like lying on these questions."]
Cost-Benefit Analysis	*Comparing the cost and the benefit of apps* ["Why give my location data if it's not going to benefit me"]
App-Provided Data Coverage	*The scope of the data provided by the app* ["If ... everyone had to download the app and ... (get tested regularly) and then would have to put the results in the app. That'd be amazing"]
User-Provided Data Coverage	*The scope of data collected by the app* ["It was a check-in or whatever and it just said: Do you have any symptoms, yes, no...and that was it. So it was not very comprehensive"]
Utility	*Usefulness of apps in everyday life* ["I don't really leave my house much,... That's probably another reason but I'm not against it."]
Necessity	*Whether data collected is necessary for the app* ["It has to be relevant to you... If I'm shopping for something and they say, oh, can we access your camera? Then it's like, there's no point."]
Easy Availability	*How easily understandable data protection process is* ["I guess like a short blurb or summary of like the data that they would probably collect"]

Table 1: Coding Themes Developed by the Research Team

Severity of the COVID-19 Pandemic. Individuals considered the severity of the COVID-19 pandemic when deciding whether to open their privacy boundaries. One participant noted, *"with COVID it's a lot more deadlier so that's why, that was also one of my main reasons for why I downloaded it because I was just concerned with COVID (user 1, group 1)."* Another participant added that *"I think just because it's like all about COVID. That's why I'm more willing to use this app (user 2, group 1)."*

This major theme was closely related to the benefit factor in the boundary negotiation. The perceived benefit of sharing personal information (e.g., family safety) functioned as the decision criteria that individuals use to open their privacy boundaries. For example, one participant mentioned this change in privacy boundary: *"I don't think I'd use it to track like a cold or flu because like I'm honestly using the app to like, protect my family from like any, like, really severe illness (user 3, group 2)."*

Uncertainty of the COVID-19 Pandemic. Similarly, participants discussed the uncertainty of the COVID-19 pandemic as a criterion that they used to open their privacy boundaries. As an example of this theme, one participant said that *"I probably wouldn't have used anything else besides right now, because there's still so much uncertainty with the pandemic and the virus in general (user 4, group 1)."*

For some participants, the uncertainty related to the transmission of the virus was the primary motivation to use the COVID-19 symptom tracking app. As one participant elaborated: *"I'm afraid of possibly getting it or possibly giving it to someone else even walking by. So I'd be more compelled to use it (user 5, group 1)."*

Protecting Themselves or People Around Them. As the risk perception regarding the COVID-19 increased, it motivated personal- and family- safety-conscious individuals to open their privacy boundaries. Some individuals were more willing to use the COVID-19 symptom tracking app to safeguard their health. For example, one participant noted: *"I feel like it's a good thing to just have on your phone and for your for your own safety (user 6, group 3)."*

Participants were also willing to use COVID-19 symptom tracking apps to protect people around them (e.g., family members) from the pandemic. They mentioned that *"my family has some health issues and I just wanted to be on the safe side (user 3, group 2)." "I got kind of nervous because my mom is a high-risk patient. So, I started using it just to make sure that, what kind of cases are around me and what spots I should be careful at (user 1, group 1)."*

Contributing to the Public Good. The public good was another decision criterion that participants used to open their privacy boundaries. Some participants were willing to share their location and health information to contribute to the public's well-being. They noted that *"it would be good to just share location for that. Just because the intention is for the general health, and overall*

greater good (user 11, group 3)," and that "at least you know it benefits a large population of people in the end which is sick (user 2, group 1)".

Other participants mentioned that they decided to use the tracking app to provide their health and location data for research purposes with the hope of going back to normalcy: *"my health information could be used for um research purposes or just to help like you know extension of like scientific knowledge (user 5, group 1)." "you're taking the steps to try to help society, get back to some sort of normalcy (user 6, group 3)."*

Mandatory Use. Finally, mandatory use to support the community functioned as a decision criterion that participants used to open their privacy boundaries. For example, some participants used a COVID-19 symptom tracking app because they were required to use them for the well-being of their community during the pandemic.

*"I also use the COVID app cause I also got a call from the state and they asked me to also use it ... in addition to that since I also work for *institution name*, they make me use the *name of the pass* ... I'd be more compelled to use it and make sure just try to contribute as much data as possible. Just to help them out (user 7, group 2)".*

4.2 Boundary Closing

At the same time, multiple participants mentioned that they have become even less likely to install COVID-19 symptom tracking apps during the pandemic than before, which corresponds with the "boundary closing" dimension of CPM and IBT. The two main themes that emerged from the focus groups were: 1) lifestyle changes and 2) data quality. The theme of data quality included the sub-themes of user-provided data coverage and app-provided data coverage.

Lifestyle Changes. The lifestyle change was one decision criterion used to close their privacy boundaries. Participants mentioned that they were unwilling to use a COVID-19 symptom tracking app because their lifestyles had changed. Many felt as though tracking was not crucial since they did not engage with the "outside" world as much since the beginning of the pandemic.

One participant elaborated: *"I'm only going out like uh once or twice a month ... so it's not really worth me having to like manage a COVID tracking app for that one instance (user 8, group 3)."*

Another participant mentioned that the utility of the app decreased for them as the pandemic became more prominent, and they started spending most of their time in a lockdown: *"prior to this, I was using, I think it was called *name of an app* ... and I just stopped using it because um well I'm not on campus anymore so it's not really relevant (user 3, group 2)."*

Furthermore, some participants explicitly elaborated on the privacy calculus regarding the use of the COVID-19 symptom tracking app: *"I don't leave my house that much either unless it's for a necessity ... so why give my information and location data if it's not going to benefit me (user 9, group 3)."*

Data Quality. The data quality was another decision criterion that participants used to close their privacy boundaries. Participants were also less willing to use a COVID-19 symptom tracking app and share their personal information because they were skeptical about the quality of data provided by the app. There were two different scenarios described wherein the participants did not find the data provided by the application to be of high enough quality: app-provided data coverage and user-provided data coverage.

App-provided Data Coverage. Some participants were unwilling to use a COVID-19 symptom tracking app during the pandemic because of the limited amount of data that an application provided. They felt as though applications did not always show enough statistics regarding COVID-related symptoms: *"for the *name of an app*, I think I ended up deleting it from my phone just because I didn't really see much stats within it. So I couldn't find it really useful." (user 2, group 1).*

Other participants pointed out that apps need to be used by many others to be beneficial enough for them to use: *"If we all use it, then it will be beneficial, and if not, then I don't think there's a lot of benefit to it (user 9, group 3)." "everyone needs to participate in it, in order to get like an accurate representation (user 10, group 3)."*

User-provided Data Coverage. Some participants mentioned that they were even less likely to use the COVID-19 symptom tracking apps because they were not satisfied with the apps' questions. More specifically, they thought that many of these apps did not provide a comprehensive set of questions about the COVID-19 symptoms.

"I think it was like a check in or whatever and it just said: Do you have symptoms, yes, no and, just that was that was it. So it wasn't very comprehensive. So if it was like a little bit more detailed at least, then I'd be more inclined to use it but as of right now (user 11, group 3)."

Other participants felt that the accuracy of self-reported health information that the users provided was not guaranteed: *"I think also along with that there's always going to be those people who don't really give the most like accurate representation or their symptoms (user 12, group 3)."*

5 Discussion

The first RQ for this work was: *RQ1: How did users' privacy attitudes toward health symptom tracking apps change during the COVID-19 pandemic?*

The focus group interviews provided strong evidence of changes in individuals' privacy attitudes during the pandemic. IBT suggests that boundary opening and closing are "dynamic psychological processes of regulation" [24] that allow people to control the flow of personal information to others in the social environment. The COVID-19 pandemic can be interpreted as a "privacy turbulence" in terms of the IBT/CPM since it affected how individuals closed/opened their information boundaries.

The current study captured the dynamicity in the processes of boundary management among the focus group participants. Besides multiple participants choosing to become less (or more) open with their boundaries, some participants went through cycles within the pandemic. One participant noted deleting a COVID-19 symptom tracking app they were using once they did not find it useful anymore. The participant mentioned that *"I think just because it's like all about COVID. That's why I'm more willing to use this app ... I think I ended up deleting it from my phone just because I didn't really see much stats within it. So I couldn't find it really useful" (user 2, group 1).* In this conversation, the information boundary was first opened because of the severity of the pandemic and then closed due to a lack of utility to the app. Hence, acknowledging and understanding the dynamicity of privacy attitudes during health emergencies is a significant trend worth exploring further in future work.

As privacy turbulence, the COVID-19 pandemic had different meanings for different people. A clear variation in the needs and priorities of different users was observed. As reported in other areas, individuals' perceived risks and threats associated with the pandemic heavily influenced the risk-benefit ratio individuals used to regulate information boundaries during the pandemic.

The more risks individuals perceived, the more benefit they anticipated from sharing health and location information with COVID-19 symptom tracking apps. In this way, the risk perception regarding the pandemic and the benefit of sharing personal information went hand-in-hand. For example, participants described different levels of perceived risks of the COVID-19 pandemic; hence, different levels of perceived benefits of sharing personal information depending on their health conditions. For those who perceived that they were at a greater risk of contracting or being impacted by the pandemic, the benefit of having information that could aid them in staying safe was the primary decision criteria to open their information boundaries. One even called privacy concerns a "luxury" during the public health crisis. On the other hand, for those who perceived that they were not at high risk, the benefit of safety was not a significant motivator to modify their information boundaries. Those who did not perceive high risks from the COVID-19 pandemic prioritized other decision criteria (e.g., mandatory use, quality of the data, etc.) to open and close their information boundaries.

The second research question for this work was: *RQ2: How did users rationalize their boundary closing and boundary opening behavior during the pandemic?*

Boundary opening occurred when individuals were more willing to use health tracking apps than before, while boundary closing occurred when individuals were less willing to use health symptom tracking apps. Participants opened and closed their boundaries based on several decision criteria. The uncertainty and severity of COVID-19 posed an immediate and consequential risk to the health of individuals and their loved ones. The threat of COVID-19 and the benefit of having COVID-19 preventing information led users to engage in the increased act of boundary opening. These findings are consistent with recent work that suggests that perceived threats to life or health during a pandemic may be

an important predictor of acceptance of potentially helpful yet controversial technologies such as COVID-19 tracking technologies [31].

Participants primarily opened their boundaries for information that they considered valuable. At the same time, participants closed their boundaries, which may have once been opened, if the information they received was no longer useful (e.g., due to lifestyle changes) or did not meet their expectations. These findings suggest that although users may open their privacy boundaries, these boundaries can just as quickly be closed and are contingent on the users' expectations, needs, and desires at any given time. In other words, boundaries may be both socially and contextually situated.

A lack of adoption by a critical mass was cited as a rationale for boundary closing, which connects with previous research on network externalities [14] discussing how reaching a critical mass of users in specific platforms incentives new users to join that platform. Hence, there is a need to explore ways for multiple stakeholders to identify ways to support privacy-aware data sharing mechanisms that can ensure high coverage of the apps. Similarly, the participants were well-informed about their requirements for adopting such apps and when/how they will consider opening their privacy boundaries to install them. Thus, the paradigm of participatory design [6] will be especially relevant in the creation of future symptom tracking apps.

Lastly, public good, which can be perceived as an individual's willingness to sacrifice one's privacy for the greater good, was identified as a key factor that led users to open their privacy boundaries. This finding connects with theoretical literature suggesting that privacy presupposes the existence of others and the possibility of a relationship between personal privacy and societal good [13, 18, 24]. Therefore, future apps can consider highlighting the social aspects (e.g., protecting those around them) and public good (e.g., helping science fight pandemics) in their descriptions and design to support better adoption.

The current study is considered to be exploratory and has some limitations. Participants consisted of 21 (majority young) individuals residing in the Northeastern U.S. Although they were diverse in race/ethnicity, they do not constitute a representative sample. Similarly, the current study discusses privacy concerns based on a small number of COVID-19 symptom tracking applications during a specific phase of the pandemic. Therefore, caution needs to be applied in interpreting the findings for other contexts.

Despite the above limitations, this study has important implications for both information privacy discourse and the specific instance of a public health emergency (COVID-19). The current study contributes to the IBT and CPM literature by (1) applying the theories to the context of public health emergencies such as COVID-19 and (2) empirically identifying conditions for privacy boundary opening and closing during health emergencies. For instance, it adds an interpretation of health emergencies as "privacy turbulence." The work also identified personal and social aspects of privacy boundary management and interconnections between the two. Similarly, it highlights the dynamic nature of the boundary management process. Thus, this work adds a new interpretation

of boundaries and empirical evidence to CPM/IBT in public health settings. An improved understanding of privacy attitudes during the pandemic can motivate further research on similar topics in different contexts.

Many people are downloading and using tracking apps, and the privacy aspects of such apps are of great importance for the different stakeholders engaged with information systems. However, building apps serves little purpose unless the greater public adopts them. The current study identifies factors that will increase or decrease the adoption of such apps. Identifying these factors is vital for health policy designers (including US CDC, EU Information Commission), health professionals, and mobile app designers. Better health app design is also beneficial to the broader public and good for the health of society.

6 Conclusion

The primary purpose of the present study was to understand the changes in individual privacy attitudes toward mobile health apps during the COVID-19 pandemic. Drawing upon CPM and IBT, the study analyzed focus group interview inputs from 21 participants. The participants described the pandemic as a phenomenon that caused significant changes in their attitudes toward the acceptability of symptom-tracking health apps, which resonates with "boundary turbulence" in the CPM literature. Further, the participants identified multiple reasons for being more accepting ("boundary opening" as per CPM) and less accepting ("boundary closing") of the health apps. Rationales for the boundary opening included aspects like the severity and the uncertainty of the pandemic and contributing to the global good. Rationales for boundary closing included aspects like the reduced utility due to lifestyle changes and the quality of the data. The results can help policy designers and health information system designers understand the reasons for accepting and rejecting mobile apps in health emergencies. This knowledge can be vital for designing future health apps and supporting societal well-being.

References

1. Agamben, G.: The state of exception. Duke University Press (2005)
2. Asif, H.: Chapter 7, Privacy or Utility? How to Preserve both in Outlier Analysis. Ph.D. thesis, Rutgers University-Graduate School-Newark (2021)
3. Azjen, I.: Understanding attitudes and predicting social behavior. Englewood Cliffs (1980)
4. Berglund, J.: Tracking covid-19: there's an app for that. IEEE pulse **11**(4), 14–17 (2020)
5. Cho, H., Ippolito, D., Yu, Y.W.: Contact tracing mobile apps for covid-19: Privacy considerations and related trade-offs. arXiv preprint arXiv:2003.11511 (2020)
6. Davis, S., Peters, D., Calvo, R., Sawyer, S., Foster, J., Smith, L.: "kiss myasthma": Using a participatory design approach to develop a self-management app with young people with asthma. Journal of Asthma **55**(9), 1018–1027 (2018)

7. Dinev, T., Hart, P.: An extended privacy calculus model for e-commerce transactions. Information systems research **17**(1), 61–80 (2006)
8. Drew, D.A., Nguyen, L.H., Steves, C.J., Menni, C., Freydin, M., Varsavsky, T., Sudre, C.H., Cardoso, M.J., Ourselin, S., Wolf, J., et al.: Rapid implementation of mobile technology for real-time epidemiology of covid-19. Science **368**(6497), 1362–1367 (2020)
9. Gvili, Y.: Security analysis of the covid-19 contact tracing specifications by apple inc. and google inc. IACR Cryptol. ePrint Arch. **2020**, 428 (2020)
10. Kaptchuk, G., Goldstein, D.G., Hargittai, E., Hofman, J., Redmiles, E.M.: How good is good enough for covid19 apps? the influence of benefits, accuracy, and privacy on willingness to adopt. arXiv preprint arXiv:2005.04343 (2020)
11. Kokolakis, S.: Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. Computers & security **64**, 122–134 (2017)
12. Landis, J.R., Koch, G.G.: The measurement of observer agreement for categorical data. biometrics pp. 159–174 (1977)
13. Laufer, R.S., Wolfe, M.: Privacy as a concept and a social issue: A multidimensional developmental theory. Journal of social Issues **33**(3), 22–42 (1977)
14. Lin, K.Y., Lu, H.P.: Why people use social networking sites: An empirical study integrating network externalities and motivation theory. Computers in human behavior **27**(3), 1152–1161 (2011)
15. Neuendorf, K.A.: The content analysis guidebook. sage (2017)
16. Petronio, S.: Communication boundary management: A theoretical model of managing disclosure of private information between marital couples. Communication theory **1**(4), 311–335 (1991)
17. Petronio, S.: Boundaries of privacy: Dialectics of disclosure. Suny Press (2002)
18. Petronio, S.: Communication privacy management theory. In: The International Encyclopedia of Interpersonal Communication, pp. 1–9. American Cancer Society (2015)
19. Ramakrishnan, A.M., Ramakrishnan, A.N., Lagan, S., Torous, J.: From symptom tracking to contact tracing: A framework to explore and assess covid-19 apps. Future Internet **12**(9), 153 (2020)
20. Rice, R.E.: Media appropriateness: Using social presence theory to compare traditional and new organizational media. Human communication research **19**(4), 451–484 (1993)
21. Rogers, R.W.: A protection motivation theory of fear appeals and attitude change1. The journal of psychology **91**(1), 93–114 (1975)
22. Sharma, T., Bashir, M.: Use of apps in the covid-19 response and the loss of privacy protection. Nature Medicine **26**(8), 1165–1167 (2020)
23. Simko, L., Calo, R., Roesner, F., Kohno, T.: Covid-19 contact tracing and privacy: studying opinion and preferences. arXiv preprint arXiv:2005.06056 (2020)
24. Stanton, J.M.: Information technology and privacy: A boundary management perspective. In: Socio-technical and human cognition elements of information systems, pp. 79–103. Igi Global (2003)
25. Stanton, J.M., Stam, K.R.: Information technology, privacy, and power within organizations: A view from boundary theory and social exchange perspectives. Surveillance & Society **1**(2), 152–190 (2003)
26. Walters, K., Markazi, D.M.: Insights from people's experiences with ai: Privacy management processes. Diversity, Divergence, Dialogue **12645**, 33 (2021)
27. Wen, H., Zhao, Q., Lin, Z., Xuan, D., Shroff, N.: A study of the privacy of covid-19 contact tracing apps. In: International Conference on Security and Privacy in Communication Systems. pp. 297–317. Springer (2020)

28. WHO: World Health Organization: Who coronavirus (covid-19) dashboard, https://covid19.who.int/, last accessed 15 Sep 2021
29. WHO: World Health Organization: Who director-general's opening remarks at the media briefing on covid-19 - 11 march 2020, https://www.who.int/director-general/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19—11-march-2020, last accessed 15 Sep 2021
30. Williams, S.N., Armitage, C.J., Tampe, T., Dienes, K.: Public attitudes towards covid-19 contact tracing apps: A uk-based focus group study. Health Expectations **24**(2), 377–385 (2021)
31. Wnuk, A., Oleksy, T., Maison, D.: The acceptance of covid-19 tracking technologies: The role of perceived threat, lack of control, and ideological beliefs. PloS one **15**(9), e0238973 (2020)
32. Yoneki, E., Crowcroft, J.: Epimap: Towards quantifying contact networks for understanding epidemiology in developing countries. Ad Hoc Networks **13**, 83–93 (2014)