Original Paper

Post-COVID Public Health Surveillance and Privacy Expectations in the United States: Scenario-Based Interview Study

John S Seberger[1], PhD; Sameer Patil[2], PhD

[1]College of Communication Arts & Sciences, Michigan State University, East Lansing, MI, United States

[2]School of Computing, University of Utah, Salt Lake City, UT, United States

Corresponding Author:
John S Seberger, PhD
College of Communication Arts & Sciences
Michigan State University
404 Wilson Rd
East Lansing, MI, 48824
United States
Phone: 1 (517) 416 0743
Email: seberge1@msu.edu

Abstract

Background: Smartphone-based apps designed and deployed to mitigate the COVID-19 pandemic may become infrastructure for postpandemic public health surveillance in the United States. Through the lenses of privacy concerns and user expectations of digital pandemic mitigation techniques, we identified possible long-term sociotechnical implications of such an infrastructure.

Objective: We explored how people in the United States perceive the possible routinization of pandemic tracking apps for public health surveillance in general. Our interdisciplinary analysis focused on the interplay between privacy concerns, data practices of surveillance capitalism, and trust in health care providers. We conducted this analysis to achieve a richer understanding of the sociotechnical issues raised by the deployment and use of technology for pandemic mitigation.

Methods: We conducted scenario-based, semistructured interviews (n=19) with adults in the United States. The interviews focused on how people perceive the short- and long-term privacy concerns associated with a fictional smart thermometer app deployed to mitigate the "outbreak of a contagious disease." In order to elicit future-oriented discussions, the scenario indicated that the app would continue functioning "after the disease outbreak has dissipated." We analyzed interview transcripts using reflexive thematic analysis.

Results: In the context of pandemic mitigation technology, including app-based tracking, people perceive a core trade-off between public health and personal privacy. People tend to rationalize this trade-off by invoking the concept of "the greater good." The interplay between the trade-off and rationalization forms the core of sociotechnical issues that pandemic mitigation technologies raise. Participants routinely expected that data collected through apps related to public health would be shared with unknown third parties for the financial gain of the app makers. This expectation suggests a perceived alignment between an app-based infrastructure for public health surveillance and the broader economics of surveillance capitalism. Our results highlight unintended and unexpected sociotechnical impacts of routinizing app-based tracking on postpandemic life, which are rationalized by invoking a nebulous concept of the greater good.

Conclusions: While technologies such as app-based tracking could be useful for pandemic mitigation and preparedness, the routinization of such apps as a form of public health surveillance may have broader, unintentional sociotechnical implications for individuals and the societies in which they live. Although technology has the potential to increase the efficacy of pandemic mitigation, it exists within a broader network of sociotechnical concerns. Therefore, it is necessary to consider the long-term implications of pandemic mitigation technologies beyond the immediate needs of addressing the COVID-19 pandemic. Potential negative consequences include the erosion of patient trust in health care systems and providers, grounded in concerns about privacy violations and overly broad surveillance.

(JMIR Mhealth Uhealth 2021;9(10):e30871) doi: 10.2196/30871

KEYWORDS

COVID-19; pandemic-tracking apps; privacy concerns; infrastructure; health surveillance; scenario; interview; thematic analysis

Introduction

Background

The COVID-19 pandemic has raised profound concerns about the potential effects of app-based public health surveillance. On one hand, apps for contact tracing and exposure notification — which we refer to as "pandemic tracking apps" [1] — are potentially useful for pandemic mitigation [2-5] and preparedness for future pandemics [6]. In this regard, such apps are understood to contribute to "the greater good" by helping achieve stable and acceptable levels of public health [6,7]. On the other hand, the same technologies have stoked fears of mass surveillance with an ever-increasing scope [8-12]. In this regard, the relationship between pandemic tracking apps and the long-term greater good is less clear. Even positive assessments of such apps acknowledge their inherently "creepy" nature [13], implicitly underlining a parallel between the restoration of public health and the data-driven economics of surveillance capitalism [14].

Mobile health (mHealth) research is fertile ground for improving quality of life (eg, [15-17]). The relationship between short- and long-term forms of the greater good that may be achieved through the routinization of pandemic tracking apps deserves deeper consideration in terms of the broader quality of life these apps could foster. These considerations include people's beliefs about the right to privacy in an increasingly technology-mediated world, people's trust in the health care institutions that provide care to them, and the affective outcomes of such beliefs.

While other work at the intersection of privacy and pandemic mitigation technology has (rightfully) focused on the immediacy of the pandemic [7,18,19], we approach people's perceptions about pandemic tracking apps with a focus on the long-term implications. Echoing prior work in human-computer interaction (HCI) [1], we adopted a future-oriented lens to analyze how people understand the potential ramifications of app-based public health surveillance after the pandemic. We paid particular attention to the potential effects of such surveillance on everyday sociotechnical conditions (ie, the ways in which social norms and technological capabilities mutually influence each other and thereby shape daily life) [20,21].

We begin by covering salient literature in the sections that follow. Given the disciplinary intersectionality of this work, we discuss related work from several domains.

Health, Surveillance, and Pandemic Tracking Apps

Individual health, public health, and privacy converge within the field of health surveillance. The history of health surveillance (eg, [22,23]) shows a tendency toward general surveillance [24]. Although the ultimate object of health surveillance is a specific disease, such surveillance necessarily includes the person that carries that disease. Recent work has framed the COVID-19 pandemic as an opportunity for heightened general surveillance [8,12,25]. Such framing is appropriate because of 2 characteristics of technology use at the time of the COVID-19 pandemic. First, pandemic mitigation techniques, such as quarantines and shutdowns, have increased people's daily reliance on technology [26]. Second, technological solutions to the pandemic are entangled with institutions whose survival is predicated on data-driven "dehumanization" of the user [27] and corporate initiatives that foster people's resignation to accepting privacy violations as inevitable [28]. Both characteristics are broadly aligned with the data-fueled economics of surveillance capitalism [14], in which people are implicitly operationalized as monetizable sources of data that are trafficked and profited upon through practices such as personalized advertising.

For example, in the United States, Google and Apple have worked together to create an exposure notification infrastructure [5]. The infrastructure these parties have developed is privacy-preserving, but in a short-term way. That is, the proposed and implemented privacy protections focus on limiting the identifiability of data, rather than understanding people's perceptions of the data collection in the long term. Researchers have argued that the short-term measures taken by Google and Apple may limit the value of the data collected through such an infrastructure [2]. Such an argument implies that app-based data should be squeezed for all the information it might provide. Digital pandemic interventions elsewhere in the world have leveraged similarly large-scale corporate or military platforms [25]. Such collaborations between industry, military, and the government highlight the blurry line between health surveillance and the data-driven objectification of the user [8].

Despite the murkiness of the economic, institutional, and social realms in which pandemic tracking apps function, such apps are clearly aligned with the foundational logic of health surveillance (ie, [22,29-31]) and have well-defined benefits in terms of public health. However, they raise concerns about what is termed as "surveillance creep" (ie, the tendency for the surveillance abilities of a technology used in one context to transfer to a similar technology in a different context, thereby achieving subtle forms of social control [32]). For example, in the case of the Google/Apple collaboration, surveillance creep manifests as the extension of platform-specific surveillance capabilities (eg, user tracking, geolocation) into the domain of public health. Surveillance creep in public health may have a profound impact on the postpandemic everyday lives of users [11,24]. This is particularly apparent in light of medical-technical programs that prescribe smartphones as part of mitigation routines (cf. [33]).

Broad concerns about surveillance creep are manifested in short-term concerns about end-user privacy. By short-term concerns, we mean design-oriented concerns intended to increase the use of apps without sufficiently considering the long-term implications of widespread adoption. For example, recent work has shown that mHealth apps do not typically provide sufficient information about the third parties to whom data access might be provided [34]. Similar work has identified widespread insufficiencies in mHealth privacy policies [35]. However, no work to date has focused specifically on the potential routinization of pandemic tracking apps as infrastructure for public health surveillance. Two necessary areas of inquiry regarding the impact of routinization are (1) people's beliefs about their rights to privacy in an increasingly

technology-mediated world and (2) people's perceptions of the health care systems that provide care to them.

Pandemic Tracking Apps as Potential Infrastructure

Pandemic tracking apps may form future infrastructure for public health surveillance. As such, the concept of the "hopeful monster" is relevant to the potential routinization of pandemic tracking apps. The hopeful monster is a technology that aspires to the functional invisibility of infrastructure [36,37]. In this way, the hopeful monster exists as a precursor to a successful technology, where successful technologies are those that become invisible through routinization [38].

However, the potential success of pandemic tracking apps, and therefore the likelihood of their invisibility, remains uncertain. In the short-term, pandemic tracking apps will be considered successful if they prove to be effective in controlling the current COVID-19 pandemic. In the long-term, however, it is naïve to assume that a successful, population-scale mode of health surveillance will be dismantled after the pandemic or used only for its originally intended purpose (ie, surveillance of the COVID-19 pandemic) [39]. Indeed, research is already underway to examine the applicability of pandemic tracking infrastructure for tracking other diseases including HIV/AIDS in the United States [40], the benefits of routinizing app-based surveillance in the form of smart technologies [41], and the development of international interoperability for pandemic tracking apps [42]. Recent work has further highlighted the likelihood of pandemic tracking apps being routinized as future means of pandemic preparedness and mitigation [6]. The effects that such apps have on their users will likely extend beyond the end of the current pandemic.

Technology adoption models have been employed to understand how and under what conditions individuals may adopt pandemic tracking apps [18,43,44]. Once a technology is adopted for use, the satisfaction that users feel when an adopted technology "does what it is supposed to do" fosters continued use [45], particularly in mHealth apps [44,46]. Moreover, people have been shown to approach apps that serve the greater good with less privacy wariness and greater willingness to overlook privacy concerns [6,47]. Assuming that adoption of pandemic tracking apps is effective for mitigating the spread of the COVID-19 pandemic, such apps are primed for continued use in nonpandemic circumstances and become typical means for public health surveillance [1,6].

Data collected from a sample of Amazon Mechanical Turk workers in the United States indicate a generally favorable expectation to continue using pandemic tracking apps for general health monitoring even after the COVID-19 pandemic has been controlled [1]. People demonstrating a collectivist social orientation are more likely to continue using such apps for general health monitoring. Similarly, younger users expect to continue using such apps after the pandemic [1], aligning with their higher inclination to adopt pandemic tracking apps [48].

At the same time, Seberger and Patil [1] found that privacy concerns regarding mobile apps are negatively correlated with the expectation to use pandemic tracking apps as infrastructure for general health surveillance. People who are more concerned about privacy when using mobile apps are less likely to use pandemic tracking apps for general health monitoring *after* the pandemic. However, no such relationship was found between privacy concerns and the perceived benefit or expected use of pandemic tracking apps *during* the pandemic [1]. Given the prevalence of hyperbolic discounting [49] (ie, people's general inability to judge future impacts of current privacy decisions), it is likely that the relaxation of privacy concerns caused by the immediacy of the pandemic implicitly fosters long-term routinization of pandemic tracking apps.

Apps are designed to be used, and success in meeting user needs fosters their continued use [44,45]. If pandemic tracking apps prove to be successful in the mitigation of COVID-19, then it is possible that they will form the core of a more general, app-based form of public health surveillance. As we begin transitioning beyond the pandemic, it is essential to examine how people understand the sociotechnical implications of such an app-based infrastructure for public health surveillance that extends into the future.

The Relevance of Privacy to Pandemic Tracking Apps

We consider people's privacy concerns as a lens through which we can understand their expectations of postpandemic public health infrastructure. Theoretical approaches to end-user privacy concerns vary widely across scholarly disciplines [50]. Recently, there has been an increased focus on the politics of definitions and theorizations of privacy [51]. Whether privacy is understood to be relational [52,53], normative [54-57], calculative [58-60], or affective [57,61], policies and practices derived from such approaches necessarily shape the daily expectations and practices of the worlds in which they are realized. Such expectations and practices are increasingly characterized by the economics of surveillance capitalism [14].

The pervasiveness of end-user privacy concerns that arise in relation to surveillance capitalism [14] has been demonstrated to contribute to digital resignation [28], learned helplessness [62], and security fatigue [63,64]. Digital resignation refers to a social stance toward technology in which people are resigned to the inevitability of negative effects of technology. Digital resignation is thus a form of learned helplessness, which has been demonstrated to arise in relation to negative user experiences. Similarly, security fatigue refers to the taxing effects of maintaining security and privacy over time. It is possible to extrapolate from security fatigue [63,64] to the longer-term fatigue that may arise in the context of an ever-changing ecology of devices, apps, and protocols. Further, privacy researchers often encounter the so-called privacy paradox [65]: People tend to *state* that they are concerned about privacy and *act* as though they are not. Similar to recent work [66], we consider the privacy paradox obliquely through one of its symptoms: fatalistic attitudes toward the inevitability of app-based privacy intrusions.

To frame our work, we drew on research about the experience of creepiness in relation to technology use [62,67]. More specifically, we explored the potential for creepiness in modern platforms (eg, Facebook, Google, Amazon) that are capable of increasing levels of surveillance [20,68,69]. We approached our research in terms of the varied and ad hoc groupings of

technologies used in a person's daily life (ie, assemblages [70]). We further consider 2 privacy-related phenomena: the appearance of hyperfunctional infrastructures [71] and hyperbolic scaling [66]. Hyperfunctional infrastructures work according to their intended purpose but do so in ways that render them visible through the affective conditions they bring about [71]. Relatedly, hyperbolic scaling refers to user tendencies to project the negative characteristics of 1 app or category of apps onto the whole app ecology [66].

Research Question

Future public health may well benefit from the routinization of app-based surveillance based on the infrastructure resulting from the deployment of apps to track the COVID-19 pandemic. Given the immediacy of triage and the severe impact of COVID-19 on public health, it is tempting to focus exclusively on the short-term need to stabilize public health to an acceptable level. However, improved or stable public health is only one possible outcome of app-based public health surveillance. Other outcomes play out on a longer temporal scale.

The goal of our research was to understand the interplay between perceived public health benefits of pandemic tracking apps and their potential effects on nonmedical concerns (eg, sociotechnical conditions, surveillance capitalism). To that end, we addressed one core research question: How can people's privacy concerns about pandemic tracking apps improve our understanding of the sociotechnical ramifications of a potential postpandemic technical infrastructure for public health surveillance?

We identified a need to engage in the present work for 2 reasons. First, prior work has shown that people are interested in continuing to use pandemic tracking apps as infrastructure for public health surveillance [1]. Second, people expect such continued use to occur within a broader economy of surveillance capitalism [14]. Given that technology often "moves fast and breaks things" [10,39], the academic research community should devote energy to understanding these possible outcomes before they are realized. We adopted such a stance with the hope of engaging with the broader health-related research community.

Methods

Overview

To answer the research question posed in the previous section, we conducted semistructured scenario-based interviews (n=19) during the spring and summer of 2020 with adult participants from the United States. All study procedures were approved by the Institutional Review Board of Indiana University (Protocol #1902443119). We present the research according to the Standards for Reporting Qualitative Research guidelines [72].

The pragmatic nature of our research called for bottom-up qualitative analysis [73]. Building on prior human-centered work in HCI, we engaged in inductive analysis to surface beliefs about the possible ramifications of developing infrastructure for public health surveillance on the back of pandemic tracking apps. Recent work has highlighted the value of such inquiries for understanding the user experience of mHealth devices [74]. We analyzed interview transcripts by engaging in the inductive and constructivist process of exploratory pragmatic research using reflexive thematic analysis [75].

Scenario Development

The use of scenarios is common in privacy-related research (eg, [1,66,76-78]). We developed a scenario that describes a fictional pandemic tracking application linked to a smart thermometer:

> *During the outbreak of a contagious disease, you start using a popular smart thermometer app. Apart from recording your temperature, the app allows you to input additional symptoms you might be experiencing. Based on your symptoms, you receive suggestions for actions you should take to protect yourself and others in the community from the contagious disease. The app uses a combination of Bluetooth and location data to measure exposure to the disease in communities. The app allows the data to be accessed by the authorities, doctors, and scientists so that it can be used to track the spread of the disease and enforce people's compliance with containment measures, such as quarantines. The app continues to operate in the same manner even after the disease outbreak has dissipated.*

We created the scenario in accordance with best practices for scenario-based research, such that it was open to interpretation, realistic, and did not elicit "right or wrong" responses [79]. The semantic content of the scenario was iteratively developed by both authors based on analyses of existing smart health devices (eg, thermometers, glucose monitors) that may be reasonably paired with contact tracing apps. We piloted the scenario with several individuals of diverse backgrounds, including different native languages, professions and education levels, and genders and ages. While changes based on the pilots were minimal, they helped us refine word choices and sentence structure for improved clarity and comprehension of the scenario.

The resulting scenario satisfies Meinert's [79] best practices for scenario development by being realistic: Several smart thermometer apps are available to end users and are easily discoverable through any search engine. Each of these real-world, smart thermometers is paired with a smartphone-based app that stores and analyzes the data collected using the smart thermometer. We informed participants that the fictional smart thermometer app described in the scenario was "popular." The provision of such information adheres to Meinert's [79] best practices for scenario development relative to realism and openness to interpretation.

We added information on the app's use of Bluetooth and location data to satisfy the openness to interpretation criterion of scenario development [79]. We further described data collected by the app as being available to a vague set of actors including "the authorities, doctors, and scientists." The inclusion of such information additionally satisfies the realism requirement: It is common to describe pandemic tracking apps as using location data (eg, [80]) that, according to prior work on hyperbolic scaling [66] and digital resignation [28], can be expected to be accessed by unknown third parties. Empirical work has similarly shown that mHealth apps often do not present

transparent or full accounts of third parties to whom data access may be granted [34].

Further, the scenario referenced the continued functionality of pandemic tracking apps after the pandemic has been controlled. The inclusion of this information is in line with current trends in mHealth research that examine the usefulness of pandemic tracking apps for postpandemic monitoring of health conditions (eg, [40]). We included the information in order to engage participants in a discussion of the long-term implications of digital contact tracing.

Recruitment, Participants, and Interviews

We recruited participants through ads posted on Craigslist, Reddit, Facebook, and LinkedIn. Recruitment was entirely online due to restrictions on in-person research activities during the COVID-19 pandemic. The advertisements directed interested individuals to a screening questionnaire that asked for basic demographics (eg, age, gender, employment status, duration of residence in the United States). The complete screening questionnaire is available in Multimedia Appendix 1.

We used the responses to the screening questionnaire to compose a diverse sample. Given the exploratory nature of our study, we strove for a diverse pool of interviewees to explore as much of the terrain as possible. The sample diversity helped us collect rich data that include multiple perspectives [73].

We invited the selected individuals to participate in one-on-one interviews for which participants were compensated US $10. We specifically chose the one-on-one format to be sensitive to participant comfort given the likelihood that participants would discuss sensitive information (eg, personal experiences with COVID-19, privacy concerns) [81]. All interviews took place over Zoom and lasted between 45 minutes and 60 minutes. During the interviews, participants discussed several separate scenarios, including the one described in the earlier section. We ensured that participants understood the fictional nature of the scenarios. We included several scenarios to develop an understanding of privacy concerns across a wide range of apps. Participants were free to spend as long as they wanted to answer questions related to each of the scenarios. The portions of the interview guide pertaining to the smart thermometer scenario are available in Multimedia Appendix 2.

Table 1 presents an overview of participant demographics. Of the 19 participants, 9 (48%) identified as female, 8 (42%) as male, and 2 (11%) as nonbinary. The median age of the participants was 30 years. Of the 19 participants, 5 (26%) were university students, while the remaining 12 (74%) were professionals in fields varying from web design to package handling.

Table 1. Participant demographics.

Participant ID	Gender	Age (years)	Occupation
A	Female	25	Student (law)
B	Female	26	Web designer
C	Female	27	Student (human-computer interaction [HCI])
D	Nonbinary	21	Student (history)
E	Male	26	Writer
F	Male	29	Systems analyst
G	Female	23	Student (pharmacy)
H	Male	31	Student (informatics)
I	Female	26	Business analyst
J	Male	47	Call support
K	Female	25	Student (HCI)
L	Male	30	Software quality assurance
M	Nonbinary	30	Model
N	Male	36	Database admin
O	Female	42	Court clerk
P	Male	37	Sales executive
Q	Female	36	Homemaker
R	Male	36	Package handler
S	Female	46	Admin assistant

Analysis

We analyzed the transcripts of the interviews using thematic analysis, adhering to the multistage process described by Braun and Clarke [75]. Initial engagement with the data took the form of repeated and collaborative readings of interview transcripts among 5 members of the research team. This phase culminated

in open coding of the complete corpus of interview transcripts. The researchers then condensed the codes and identified emergent themes, arriving at a group of 5 initial themes. Upon further analysis, we reduced the initial 5 to the 3 themes we present in detail in the next section.

Results

In this section, we present the results of the thematic analysis. We begin with findings surfaced through the consideration of pandemic tracking apps as part of a broader app-enabled health care system. We proceed to analyze the privacy concerns that emerge from the relationship between pandemic tracking apps and the broader ecology of smartphone apps to which they belong. We build upon this narrative by introducing and analyzing contradictory forms of the greater good that emerge from participant responses. Our findings highlight that perceptions of pandemic tracking apps indicate an expectation that such apps will form another brick in the wall of surveillance that people increasingly experience in their everyday lives.

Public Health Versus Individual Privacy: The Perceived Trade- Off

Participants saw the use of pandemic tracking apps as a potentially effective way of interfacing with the health care system. For example, the fictional smart thermometer app described in the scenario was understood to serve a triage function that indicates when an individual should seek medical attention:

> *…it's really important to resolve worries that people might have on a personal level, but then also if their fears are justified and they might have a disease or something like that. I think it's also important for them to know that so that they can receive medical care or do what they need to do.* [Participant D, nonbinary, 21 years old, student (history)]

Participant D's perception of the relationship between pandemic tracking apps and the broader health care system is generally positive. However, further analysis of this common sentiment expressed by several participants revealed a bigger picture. The entanglement of pandemic tracking app data with institutions, including but not limited to health care systems, implies the presence of unknown third parties who may gain access to user or patient data. Such privacy concerns are inherited from the broader app culture [66] and present users with difficult choices:

> *I'm feeling a bit conflicted. Part of me is like, "Okay, interesting." Another part of me is like, "Oh, this is a little bit like Big Brother."* [Participant B, female, 26 years old, web designer]

People routinely expect apps to collect data about them and to share those data with third parties [66] as part of surveillance capitalism [14]. Through Participant B's invocation of "Big Brother," it is apparent that pandemic tracking apps are not an exception to this expectation. Participants were concerned about who would have access to the data generated by pandemic tracking apps during, as well as after, the pandemic. They were similarly concerned about what those unknown third parties might do with the data:

> *I think just being aware of who's using it, where is it being used, and how they're using it is one thing. Like, what are their practices, who is using it, and what company is it being used for? Is it being used by just health workers? Is it being used to be able to track and sell information to further recommend products to us?* [Participant K, female, 25 years old, student (HCI)]

Indeed, supported by the implicit connectivity of pandemic tracking apps, each participant raised concerns about who would ultimately gain access to any data generated and collected by these apps. Participants raised similar concerns about the kinds of data that might be generated, collected, and stored. Such concerns ultimately frame the deployment of public health surveillance infrastructure built on the back of pandemic tracking apps as a "slippery slope":

> *An acceptable purpose to me would be just to gather data on the disease and how it behaves in different communities and stuff. A malicious purpose would be them using this information to figure out where you live or more information about you, such as your age. Just in any way revealing your identity would be, to me, way more on the malicious side, although it's not necessarily malicious outright. But to me, it's a slippery slope.* [Participant F, male, 29 years old, systems analyst]

Participants further demonstrated the belief that data collected by contact tracing apps could be shared for profit with advertisers or as-yet-unknown third parties:

> *They could probably give it to advertisers or other people that I probably don't want it to go into the hands of. ...I can't think of a reason why it would be bad, but it just sounds bad, you know? It sounds sketchy. I don't know what advertisers could use other than for advertising like vitamin C or other get-well things. But either way, it just seems bad.* [Participant G, female, 23 years old, student (pharmacy)]

In discussing concerns that public health apps would share user data with unknown third parties, participants referred to a category of unknown third parties that would gain access to data, but rarely identified specific actors who might belong to that category. Instead, participants expressed the belief that public health apps would work "too well," thus facilitating the trafficking of data to unknown parties:

> *…it's just knowing that the application is working and doing its thing, but potentially it's working too well and that power getting into the hands of individuals that weren't necessarily designed to have that information to begin with.* [Participant G, female, 23 years old, student (pharmacy)]

In considering the routinization of pandemic tracking apps as infrastructure for postpandemic public health surveillance, participants were faced with a difficult and contradictory set of possibilities. In particular, we observed a fundamental perceived trade-off between personal privacy and public health. This core trade-off appeared as an either/or condition: People can expect either personal privacy or better public health. Achieving both

simultaneously did not seem realistic to participants. Moreover, participants seemed to place values in a hierarchy wherein public health was superior to personal privacy:

> *I value public health and public safety over personal privacy.* [Participant A, female, 25 years old, student (law)]

Participants routinely reported such higher consideration for public health over personal privacy even when expressing deep wariness regarding existing pandemic tracking infrastructure:

> *Google and Apple have added their tracing APIs to their operating system so that governments and health authorities could start pushing out these apps that do this tracing to track down where you've been and who you've been around to understand contagious disease, disease control, and all that stuff. I understand the benefit of it. But it's highly intrusive, right? It's tracking all your data, it's tracking who you're coming in contact with, it's tracking your location. It's kind of Big Brother-ish, in a way.* [Participant G, female, 23 years old, student (pharmacy)]

This quote from Participant G demonstrates that people are aware of pandemic tracking apps as they exist in the real world but generally hold an inaccurate understanding of their functionality. Participants expected pandemic tracking apps to trade identifiable data, even though the Apple/Google collaboration in the United States goes to great lengths to maintain user anonymity. Such inaccurate understanding likely arises from the pervasiveness of apps that use the sale of access to data as a primary economic motive [14,66]. However, that which is perceived to be real is real in its consequences. As such, when understanding people's perceptions and expectations of routinized pandemic tracking apps, our focus is the way in which people believe such apps to work, regardless of whether the actual functionality matches these beliefs [82].

The perception of pandemic tracking apps as inherently privacy-intrusive constitutes a core component of the discourse of such apps. Indeed, being wary of the privacy implications of pandemic-tracking apps has real-world consequences:

> *You said that you saw someone voicing some concerns. What was that concern?* [Interviewer]
>
> *Oh, this is somebody that I personally know, and she kind of is an outlier in terms of her thinking. But she had something on there. She knew these apps, she had named some, and I did not. I have not heard of the specific names of the apps, but she had some of the apps listed, and she said that if you have any of these apps and you're thinking about using them too, please delete me from your contacts, because I will not be traced and all this kind of stuff. It was kind of really out there.*" [Participant O, female, 42 years old, court clerk]

Despite general wariness and expectations that pandemic tracking apps will violate privacy by virtue of their connectivity with unknown third parties, participants routinely justified the necessity and use of pandemic tracking apps by referring to a nebulous concept — the greater good:

> *I'm fine with [using the app] for this particular reason, just because it's for the greater good of society to know who's sick and who could potentially be sick. I think that something that could help a lot of people and save lives kind of outweighs your right to privacy in some ways, so I don't have a problem.* [Participant O, female, 42 years old, court clerk]

As we describe in the next subsection, participants routinely employed "the greater good" as a means of justifying or overlooking the perceived long-term privacy concerns raised by pandemic tracking apps. Yet, we found that this greater good is multifaceted, and the relationship between the different facets of the greater good is contradictory, highlighting pandemic tracking apps as a potential site for surveillance creep: the colonization of health by the economics of surveillance capitalism [14].

Rationalizing the Health/Privacy Trade-Off With the Greater Good

Pandemic tracking apps exist within a wider ecology of apps. Therefore, privacy concerns that emerge from user interactions with this wider ecology color perceptions and expectations of pandemic tracking apps [66]. When pandemic tracking apps are expected to align with the economic practices of surveillance capitalism (ie, monetizing user data by selling it to third parties), privacy concerns about pandemic tracking apps take center stage. Such concerns include wariness regarding unknown third parties who may gain access to the data generated, collected, and stored by pandemic tracking apps and inaccurate, but nonetheless meaningful and deep-seated, perceptions of how such apps function. The greater good is the primary means by which people rationalize and justify engaging in what they perceive as the inherently privacy-affecting decision to use pandemic tracking apps. The use of the greater good to rationalize the adoption or routinization of pandemic tracking apps can be rather sharp, demonstrating frustration with the complexity of issues raised by such apps:

> *But at the same time, yeah, actually no ... I think it's fine because it just seems to take small vitals like temperature, and if they're probably sick, it might be fine. We'll say it's fine because it's for the greater good.* [Participant G, female, 23 years old, student (pharmacy)]

This excerpt depicts a trade-off in motion. Participant G quickly reverted to the greater good as a means of rationalization. She vacillated between further expressing her concerns about the fictional smart thermometer app — "but at the same time, yea, actually no" — and finding an easier conversational way out of such expression. Participant G's use of the phrase, "We'll say it's fine," indicates a clear tension: the implicit recognition of privacy-related problems and the desire to achieve the greater good despite them.

The scenario suggested that pandemic tracking apps may be used as a foundation for postpandemic public health monitoring. Participants generally reacted negatively to this possibility:

> *It would be most useful for you to share everything or as much as you can during a pandemic, but outside of a pandemic, it starts to be kind of a gray area.* [Participant F, male, 29 years old, systems analyst]

Invocation of the greater good is not sufficient to rationalize the long-term implications of pandemic tracking apps should their use be routinized as a means of health surveillance in general. The greater good that pandemic tracking apps serve appears to have a shelf life:

> *So, during the outbreak of a contagious disease, I would think it's worth it to give up privacy and data and information. If it's an app that will really help and literally save lives, I'd be happy to do that. But I don't like the last part that it continues to operate in this way after the outbreak has dissipated.* [Participant A, female, 25 years old, student (law)]

The greater good appears to refer specifically to the mitigation and control of the pandemic, but does not necessarily extend to the routinization of pandemic tracking apps as a form of postpandemic public health surveillance:

> *Obviously when there's an outbreak of a contagious disease, everyone's focus is really just on that. Now, of course, you never know that 100%. Other people can still utilize that data for malicious reasons or their own reasons. But you would think that there's something bad going on there. Everyone's trying to help as much as possible. You're okay with it. You're okay with exposing yourself in this way. It's just the app being able to be used in the same manner after disease outbreak has dissipated … that part is more uncomfortable.* [Participant L, male, 30 years old, software quality assurance]

It is not, however, Participant L's expected or experienced discomfort that takes the center stage. Rather, it is what such discomfort implies. While our scenario intentionally primed participants to consider postpandemic routinization of pandemic tracking apps, the phrasing was ambiguous as to postpandemic functionality of such apps. We allowed participants to extrapolate from their contemporary perceptions and expectations of pandemic tracking apps in order to understand what routinization of such apps might mean.

When read in terms of people's expectation that data collected by pandemic tracking apps will be shared with third parties for financial gain, Participant L's discomfort signals the expectation that the apps will contribute to a broader culture of surveillance. Yet, participants generally accepted the likelihood of such apps being routinized for public health surveillance after the pandemic, with phrases such as, "We'll get to that when we get to that."

> *It's just the app being able to be used in the same manner after disease outbreak has dissipated…that part is more uncomfortable because it's unnecessary information being exposed when it doesn't really need to be unless the app can sort of justify it, right? If it's justified and valid, let's say let's see. Doctors and scientists and authorities. Who are you? Well, I don't know who the authorities are, but I guess it is the police. I don't know. I guess we'll get to that when we get to that.* [Participant L, male, 30 years old, software quality assurance]

Taken together, participant discussion of the greater good and their willingness to forego privacy concerns for that greater good can be troubling. Even though it is defined only implicitly, the greater good becomes a floating signifier used to justify and rationalize the perceived privacy risks of contact-tracing applications:

> *The app continues to operate in the same manner even after the disease outbreak has disappeared? Doing something for the greater good always gets my vote. So, exposing my information like this, if it's toward a greater good like this, I will tell you, again, like I sort of mentioned before, I know what's happening.* [Participant L, male, 30 years old, software quality assurance]

People understand and even expect privacy breaches as a result of app-based contact tracing. Further, they see the possibility of "Big Brother" levels of surveillance as real. The invocation of "Big Brother" refers to the expectation that contact tracing apps will result in heightened surveillance. That is, people perceive that the routinization of pandemic tracking apps for public health surveillance will lead to oversurveillance by a heterogeneous set of actors (eg, technology corporations, government bodies, health care organizations, insurance providers, third-party advertisers) variously responsible for app maintenance, data analysis, public health regulation, and health care delivery. This amounts to a future that is not accurately characterized by widespread positive affective experience despite that future's roots in the greater good:

> *What do you imagine the enforcement with compliance could mean?* [Interviewer]
>
> *Nothing that I want to imagine in real life.* [Participant M, nonbinary, 30 years old, model]

Participant M implies that public health surveillance achieved through the routinization of pandemic tracking apps would lead to outcomes too negative to even imagine. Such expectations directly call into question the short- and long-term forms of the greater good to which adoption of pandemic tracking apps contributes. On one hand, the adoption of pandemic tracking apps can contribute to the greater good of public health during a pandemic. On the other hand, the long-term adoption of such apps as infrastructure for public health surveillance contributes to widespread concerns of mass surveillance and privacy violations that cannot reasonably be described as a greater good. In fact, the privacy ramifications could arguably erode the greater good.

Discussion

Two facets of our findings are particularly worthy of discussion. First, we describe the benefits and necessity of taking a long-term, sociotechnical approach to understanding the potential routinization of mobile apps as part of the public health infrastructure. Second, we describe how user privacy concerns

constitute a productive means for identifying long-term implications of an emergent class apps used for public health surveillance.

People Expect Privacy-Related Infrastructural Problems in Public Health Surveillance

Direct consideration of people's privacy concerns about pandemic tracking apps indicates their wariness about the routinization of such apps as infrastructure for postpandemic public health surveillance. Although users are willing to justify the use of apps that raise privacy concerns with the concept of the greater good, such justification has a limited shelf life. By stating expectations that privacy concerns related to pandemic tracking apps extend to mHealth apps in general, participants highlighted the need to decouple or disentangle mHealth infrastructure from the privacy-invasive practices of surveillance capitalism.

People are wary of pandemic tracking apps because they might "work too well" (Participant G) and therefore demonstrate hyperfunctionality as identified by Seberger and Bowker [71]: conditions wherein infrastructures function within the boundaries of their designed functionality but do so in a way that gives rise to unexpected outcomes. In other words, if pandemic tracking apps achieve the form of control over the spread of the pandemic that they are designed to achieve, such success might spill over to other uses. In our scenario, we pointed out the potential for such other uses in the form of postpandemic public health surveillance that uses such apps as its infrastructure.

Participants routinely assumed that data collected via pandemic tracking apps would be shared with an identified-but-unknown category of third parties. We interpret participant concerns over third-party access to data collected by pandemic tracking apps as a form of hyperbolic scaling [66], where concerns regarding privacy violations transfer from known apps to new apps. In this logic, if App A (a known app) demonstrates problematic functions relative to end-user privacy, then *all* apps are assumed to demonstrate the same characteristics.

Stakeholders Should Take a Long-Term View of Public Health Surveillance

A pandemic often affects people's daily lives and routines in profound ways. Because the conditions of a pandemic can be all-encompassing, it can be difficult to take a long-term perspective. Yet infrastructure, like surveillance, creeps. It is learned and normalized through use [37]. The misalignment between short- and long-term concerns is compounded by the immediacy of the language used to communicate and frame the threats of the pandemic [83]. With visions of large-scale pandemic tracking already being considered (eg, [6,40-42]), it is poised to become infrastructure for public health surveillance. We suggest that it is necessary to understand the impact of public health surveillance at a temporal scale aligned more closely with the long-term one of infrastructure [84]. People's judgments related to trade-offs that unfold at the scale of the short- and long-term are notoriously problematic [85]. The severity of the pandemic and its social effects emphasize the urgency of triage to fix the most immediate problems first by focusing on the greater good of public health. Yet, given the combined power of medicine and technology to achieve social change, it is not entirely appropriate to focus solely on the immediate threats posed by the pandemic. The immediate actions that governments, corporations, and institutions take in service of pandemic mitigation will reverberate in the sociotechnical structures of the postpandemic world [86].

People's perceptions of a core trade-off between individual privacy and public health highlight a need for long-term thinking about public health surveillance. People are willing to forego privacy concerns for the greater good even though they are uncomfortable with surveillance by the technologies used to achieve that greater good. Our study therefore supports the findings of prior work on the mitigating effects of health concerns on people's privacy concerns [87]. We provide further support for findings derived from a study with UK participants who saw the greater good as a motivating factor for app use [7]. We extend the work of Williams et al [7] by adding practical nuance to the role that the greater good plays in pandemic mitigation and surfacing the potentially slippery slope toward increased and routinized public health surveillance.

The likely impacts of app-based public health surveillance extend beyond public health itself. This extension includes potential impact on people's expectations of privacy as well as colonization of mHealth by the economics of surveillance capitalism. Such colonization may lead to diminished trust between patients and health care providers. Given people's deep-seated privacy concerns, app creators, policy makers, and health institutions should engage in detailed and transparent public relations work to communicate the ways in which user privacy is protected. Such communications should describe exactly which third parties, if any, will be given access to data collected through apps used for public health surveillance and under what circumstances. While privacy concerns raised by pandemic tracking apps are likely as widespread as the pandemic itself, the steps described should be taken within existing local legal frameworks (eg, Health Insurance Portability and Accountability Act [HIPAA], General Data Protection Regulation [GDPR]). Overall, our insight highlights the need for an interdisciplinary approach to the development and deployment of app-based public health surveillance.

It is Necessary to Disentangle Public Health Surveillance From Surveillance Capitalism

People's perceptions of the alignment between public health apps and the economics of surveillance capitalism may have a detrimental effect on the relationship between patients and health care systems. Trust between patients and health care providers is foundational to effective medical care [88]. As such, the enrollment of patients as users in a sociotechnical system contextualized by potential mistrust serves neither the patient nor health care professionals. In a way, it breaches the core medical credo of "first do no harm."

Users are inherently vulnerable to the power structures instantiated by the apps that they use [66]. But, when users are also patients, they are doubly vulnerable: vulnerable to the conditional empowerment implicit in app use [66] and vulnerable to the loss of control that comes with the status of

being a patient [89] (perhaps they are also vulnerable to the dehumanization of data-driven representation [27]). If pandemic tracking apps achieve the status of infrastructure — invisibility through successful deployment and adoption [37,38] — they may do so at the risk of solidifying the vulnerability-inducing conditions of surveillance capitalism within a medical context [14]. Such solidification would directly contrast with the notion of care central to medical practice. In this light, a broader, socially oriented approach to the medical credo, "first do no harm," would benefit end users of pandemic tracking apps.

We contend that people's expectation of, and resignation to, being used may foreshadow the colonization of public health surveillance by the data-hungry and profit-driven mechanics of surveillance capitalism. We further contend that this is as much a public health issue as the maintenance of more narrowly defined bodily health. We therefore suggest the development of public health policies that account for the long-term sociotechnical effects of public health surveillance. Such policies, developed within the legal frameworks of specific regions, would necessarily view patients not solely with the medical gaze, but through a more sensitive lens that considers end-user empowerment, trust in digital systems, and the emerging broader relationship between health care and surveillance capitalism.

We further suggest that the activation of infrastructure for public health surveillance be legislatively limited to times of scientifically defined public health crises. It would be unwise to discard infrastructure that's already been built. The Google and Apple collaboration in the United States, for example, likely constitutes a useful resource for pandemic preparedness. However, such infrastructure does not necessarily present an ethical or beneficial means of general public health surveillance, given the profound privacy concerns about pandemic tracking apps. The routinization of pandemic tracking apps as infrastructure for public health surveillance has the potential for profound negative impact on the trust that should characterize the relationship between patients and health care providers. We found that people believe that health surveillance apps will operate according to the economics of surveillance capitalism, wherein access to data is sold for profit, typically without much regard for user privacy concerns. When people believe that health surveillance apps align with surveillance capitalism, it is unreasonable to expect them to trust the system that profits from the sale of their data. Such a dynamic sets up the potential for such apps to diminish patient trust in the health care systems that ostensibly care for them.

Given the dangers present in the perceived alignment between app-based public health surveillance and surveillance capitalism, we suggest that the activation of public health surveillance be limited to populations that meet specific criteria. Such criteria might include population density, smartphone saturation, and rate of disease transmission. In this way, an app for public health surveillance might be utilized to the greatest effect, while minimizing the potential for surveillance creep. Beyond meeting well-defined medical standards, such population-specific deployment should be overseen by multidisciplinary teams capable of assessing the sociotechnical and surveillance-related impact on populations who are already, by virtue of an infectious agent, fundamentally at risk.

Limitations and Future Work

We collected data during a specific period from a relatively small group of participants. Since the COVID-19 pandemic is still ongoing, additional studies are needed to investigate how the trajectory of the pandemic might influence these matters. Public health and privacy concerns are inherently cultural. Further studies involving participants from other populations would add greater context to our findings. In particular, it is possible that our findings may be specific only to the United States. Many social norms and expectations in the United States differ from those in other countries. In the United States, perceived economic relationships between government agencies, health care providers, and for-profit corporations (eg, app makers, health insurance companies) create a structure in which people may expect their privacy to be breached. Such relationships qualify people's trust (or lack thereof) in government that may be different than that in other regions across the world. Nonetheless, our findings highlight the need for further work regarding the role of trust in institutions and the possible success of app-based public health surveillance after the pandemic has ended. Further work is required to understand perceptions and expectations of public health apps in other cultural contexts.

Given the exploratory nature of this work, we did not consider ethnicity as a factor in our sample construction. However, when choosing interviewees from a pool of eligible participants, we did strive for diversity in ages, genders, professions, and educational backgrounds. Prior work [7] has not analyzed the effect of ethnicity either nor can a qualitative study of limited sample size such as ours yield robust findings relative to such a sensitive topic. That said, we recognize the profound importance of ethnicity in matters pertaining to the greater good and identify this as an important area for further research.

Conclusion

Given that pandemic tracking apps have been promoted as a useful tool for pandemic mitigation, it is likely that such apps will form the backbone of postpandemic infrastructure for public health surveillance. While it is clearly important to understand the short-term, pandemic-specific privacy concerns that arise from such apps, we contend that it is equally important to understand their long-term sociotechnical implications. People frame the use of pandemic tracking apps in terms of achieving a greater good: acceptable levels of public health. However, such framing is contextualized by a core trade-off with individual privacy. The trade-off reveals a deep-seated tension in the use of the greater good rationalization: the perception that pandemic tracking apps implicitly align with the data-hungry economics of surveillance capitalism. To make matters worse, people are resigned to viewing such alignment as inevitable, which may harm their trust in the institutions that provide health care. We highlight the relevance of analyzing privacy concerns when considering the potential routinization of apps for public health surveillance and call for the multidisciplinary application of medically influenced ethics in

the design, development, deployment, and data use of mHealth apps designated for everyday use.

Acknowledgments

The research described in this paper was undertaken while the authors were affiliated with Indiana University Bloomington. We thank the participants of the study for their time and insight. We acknowledge Marissel Llavore and Nicholas Nye Wyant for their contributions to data collection. We are grateful to the anonymous reviewers for their feedback that helped improve this paper. This research was supported by a grant from Indiana University Office of the Vice President for Research. Open access to this article is funded in part by the Indiana University Open Access Fund. Contents of the paper are the work of the authors and do not necessarily reflect the views of the sponsors.

Conflicts of Interest

None declared.

Multimedia Appendix 1

Screening questionnaire.
[DOCX File , 15 KB-Multimedia Appendix 1]

Multimedia Appendix 2

Scenario.
[DOCX File , 18 KB-Multimedia Appendix 2]

References

1. Seberger JS, Patil S. Us and Them (and It): Social Orientation, Privacy Concerns, and Expected Use of Pandemic-Tracking Apps in the United States. 2021 Presented at: Conference on Human Factors in Computing Systems; May 8-13, 2021; Yokohama, Japan. [doi: 10.1145/3411764.3445485]
2. Seto E, Challa P, Ware P. Adoption of COVID-19 Contact Tracing Apps: A Balance Between Privacy and Effectiveness. J Med Internet Res 2021 Mar 04;23(3):e25726 [FREE Full text] [doi: 10.2196/25726] [Medline: 33617459]
3. Mahmood S, Hasan K, Colder Carras M, Labrique A. Global Preparedness Against COVID-19: We Must Leverage the Power of Digital Health. JMIR Public Health Surveill 2020 Apr 16;6(2):e18980 [FREE Full text] [doi: 10.2196/18980] [Medline: 32297868]
4. Ferretti L, Wymant C, Kendall M, Zhao L, Nurtay A, Abeler-Dörner L, et al. Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing. Science 2020 May 08;368(6491):eabb6936 [FREE Full text] [doi: 10.1126/science.abb6936] [Medline: 32234805]
5. Virtual Workshop on Privacy Aspects of Contact Tracing. ProperData. 2020. URL: https://properdata.eng.uci.edu/events/privacy-contact-tracing/ [accessed 2021-09-23]
6. Utz C, Becker S, Schnitzler T, Farke FM, Herbert F, Schaewitz L, et al. Apps Against the Spread: Privacy Implications and User Acceptance of COVID-19-Related Smartphone Apps on Three Continents. Cornell University. 2021 Feb 01. URL: https://arxiv.org/abs/2010.14245 [accessed 2021-09-23]
7. Williams S, Armitage C, Tampe T, Dienes K. Public attitudes towards COVID-19 contact tracing apps: A UK-based focus group study. Health Expect 2021 Apr;24(2):377-385 [FREE Full text] [doi: 10.1111/hex.13179] [Medline: 33434404]
8. Desai BC. Pandemic and big tech. 2020 Presented at: 24th Symposium on International Database Engineering & Applications; August 12-14, 2020; Seoul, Republic of Korea. [doi: 10.1145/3410566.3410585]
9. French MA. Woven of War-Time Fabrics: The globalization of public health surveillance. Surveillance & Society 2009 Feb 27;6(2):101-115. [doi: 10.24908/ss.v6i2.3251]
10. COVID-19 apps pose serious human rights risks: recommendations for governments considering technology in addressing pandemic tech. Human Rights Watch. 2020 May 13. URL: https://www.hrw.org/news/2020/05/13/covid-19-apps-pose-serious-human-rights-risks [accessed 2021-09-23]
11. Leslie D. Tackling COVID-19 through responsible AI innovation: Five steps in the right direction. Harvard Data Science Review 2020. [doi: 10.1162/99608f92.4bb9d7a7]
12. Kitchin R. Civil liberties or public health, or civil liberties or public health? Using surveillance technologies to tackle the spread of COVID-19. Space and Polity 2020 Jun 03;24(3):362-381. [doi: 10.1080/13562576.2020.1770587]
13. Bell G. We need mass surveillance to fight COVID-19 - but it doesn't have to be creepy. MIT Technology Review. 2020 Apr 12. URL: https://www.technologyreview.com/2020/04/12/999186/covid-19-contact-tracing-surveillance-data-privacy-anonymity/ [accessed 2021-09-23]
14. Zuboff S. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. London, England: Profile Books; 2019.

15. Stoyanov SR, Zelenko O, Staneva A, Kavanagh DJ, Smith C, Sade G, et al. Development of the Niggle App for Supporting Young People on Their Dynamic Journey to Well-being: Co-design and Qualitative Research Study. JMIR Mhealth Uhealth 2021 Apr 20;9(4):e21085 [FREE Full text] [doi: 10.2196/21085] [Medline: 33877050]
16. Shalaby R, Vuong W, Hrabok M, Gusnowski A, Mrklas K, Li D, et al. Gender Differences in Satisfaction With a Text Messaging Program (Text4Hope) and Anticipated Receptivity to Technology-Based Health Support During the COVID-19 Pandemic: Cross-sectional Survey Study. JMIR Mhealth Uhealth 2021 Apr 15;9(4):e24184 [FREE Full text] [doi: 10.2196/24184] [Medline: 33750738]
17. MacIsaac A, Mushquash AR, Mohammed S, Grassia E, Smith S, Wekerle C. Adverse Childhood Experiences and Building Resilience With the JoyPop App: Evaluation Study. JMIR Mhealth Uhealth 2021 Jan 04;9(1):e25087 [FREE Full text] [doi: 10.2196/25087] [Medline: 33393908]
18. Walrave M, Waeterloos C, Ponnet K. Adoption of a Contact Tracing App for Containing COVID-19: A Health Belief Model Approach. JMIR Public Health Surveill 2020 Sep 01;6(3):e20572 [FREE Full text] [doi: 10.2196/20572] [Medline: 32755882]
19. Liu C, Graham R. Making sense of algorithms: Relational perception of contact tracing and risk assessment during COVID-19. Big Data & Society 2021 Feb 17;8(1):205395172199521. [doi: 10.1177/2053951721995218]
20. Tene O, Polonetsky J. A theory of creepy: technology, privacy and shifting social norms. Yale JL & Tech 2013;16:59.
21. Berg M, Aarts J, van der Lei J. ICT in Health Care: Sociotechnical Approaches. Methods Inf Med 2018 Feb 08;42(04):297-301. [doi: 10.1055/s-0038-1634221]
22. Langmuir AD. The Surveillance of Communicable Diseases of National Importance. N Engl J Med 1963 Jan 24;268(4):182-192. [doi: 10.1056/nejm196301242680405]
23. Langmuir AD. Communicable Disease Surveillance. Proceedings of the Royal Society of Medicine 2016 Sep;64(6):681-684. [doi: 10.1177/003591577106400646]
24. French M, Monahan T. Disease Surveillance: How Might Surveillance Studies Address COVID-19? Surveillance & Society 2020 Mar 16;18(1):1-11. [doi: 10.24908/ss.v18i1.13985]
25. Calvo RA, Deterding S, Ryan RM. Health surveillance during covid-19 pandemic. BMJ 2020 Apr 06;369:m1373. [doi: 10.1136/bmj.m1373] [Medline: 32253180]
26. Goldkind L, LaMendola W, Taylor-Beswick A. Tackling COVID-19 is a crucible for privacy. Journal of Technology in Human Services 2020 May 02;38(2):89-90. [doi: 10.1080/15228835.2020.1757559]
27. Chancellor S, Baumer EPS, De Choudhury M. Who is the "Human" in Human-Centered Machine Learning. Proc ACM Hum-Comput Interact 2019 Nov 07;3(CSCW):1-32. [doi: 10.1145/3359249]
28. Draper NA, Turow J. The corporate cultivation of digital resignation. New Media & Society 2019 Mar 08;21(8):1824-1839. [doi: 10.1177/1461444819833331]
29. Foege WH, Hogan RC, Newton LH. Surveillance projects for selected diseases. Int J Epidemiol 1976 Mar;5(1):29-37. [doi: 10.1093/ije/5.1.29] [Medline: 944166]
30. Lee LM, Thacker SB, Centers for Disease ControlPrevention (CDC). The cornerstone of public health practice: public health surveillance, 1961-2011. MMWR Suppl 2011 Oct 07;60(4):15-21. [Medline: 21976162]
31. Lee LM. An Ethics for Public Health Surveillance. Am J Bioeth 2020 Oct 18;20(10):61-63. [doi: 10.1080/15265161.2020.1806382] [Medline: 33016826]
32. Marx GT. Undercover: police surveillance in America. Oakland, CA: University of California Press; 1988:2.
33. Kazevman G, Mercado M, Hulme J, Somers A. Prescribing Phones to Address Health Equity Needs in the COVID-19 Era: The PHONE-CONNECT Program. J Med Internet Res 2021 Apr 06;23(4):e23914 [FREE Full text] [doi: 10.2196/23914] [Medline: 33760753]
34. Hutton L, Price BA, Kelly R, McCormick C, Bandara AK, Hatzakis T, et al. Assessing the Privacy of mHealth Apps for Self-Tracking: Heuristic Evaluation Approach. JMIR Mhealth Uhealth 2018 Oct 22;6(10):e185 [FREE Full text] [doi: 10.2196/mhealth.9217] [Medline: 30348623]
35. Benjumea J, Ropero J, Rivera-Romero O, Dorronzoro-Zubiete E, Carrasco A. Assessment of the Fairness of Privacy Policies of Mobile Health Apps: Scale Development and Evaluation in Cancer Apps. JMIR Mhealth Uhealth 2020 Jul 28;8(7):e17134 [FREE Full text] [doi: 10.2196/17134] [Medline: 32720913]
36. Law J. A Sociology of monsters: Essays on power, technology, and domination. London, England: Routledge; 1991.
37. Star SL, Ruhleder K. Steps Toward an Ecology of Infrastructure: Design and Access for Large Information Spaces. Information Systems Research 1996 Mar;7(1):111-134. [doi: 10.1287/isre.7.1.111]
38. Weiser M. The computer for the 21st century. SIGMOBILE Mob. Comput. Commun. Rev 1999 Jul 01;3(3):3-11. [doi: 10.1145/329124.329126]
39. Khosla R. Technology, Health, and Human Rights: A Cautionary Tale for the Post-Pandemic World. Health Hum Rights 2020 Dec;22(2):63-66 [FREE Full text] [Medline: 33390694]
40. Nosyk B, Armstrong W, Del Rio C. Contact Tracing for COVID-19: An Opportunity to Reduce Health Disparities and End the Human Immunodeficiency Virus/AIDS Epidemic in the United States. Clin Infect Dis 2020 Nov 19;71(16):2259-2261 [FREE Full text] [doi: 10.1093/cid/ciaa501] [Medline: 32339245]

41. Vedaei SS, Fotovvat A, Mohebbian MR, Rahman GME, Wahid KA, Babyn P, et al. COVID-SAFE: An IoT-Based System for Automated Health Monitoring and Surveillance in Post-Pandemic Life. IEEE Access 2020;8:188538-188551. [doi: 10.1109/access.2020.3030194]
42. Du L, Raposo VL, Wang M. COVID-19 Contact Tracing Apps: A Technologic Tower of Babel and the Gap for International Pandemic Control. JMIR Mhealth Uhealth 2020 Nov 27;8(11):e23194. [doi: 10.2196/23194]
43. Walrave M, Waeterloos C, Ponnet K. Ready or Not for Contact Tracing? Investigating the Adoption Intention of COVID-19 Contact-Tracing Technology Using an Extended Unified Theory of Acceptance and Use of Technology Model. Cyberpsychol Behav Soc Netw 2021 Jun;24(6):377-383. [doi: 10.1089/cyber.2020.0483] [Medline: 33017171]
44. Woldeyohannes HO, Ngwenyama OK. Factors Influencing Acceptance and Continued Use of mHealth Apps. In: Nah FH, Tan CH, editors. HCI in Business, Government and Organizations. Interacting with Information Systems. HCIBGO 2017. Lecture Notes in Computer Science, vol 10293. Cham, Switzerland: Springer; 2017:239-256.
45. Chaouali W. Once a user, always a user: Enablers and inhibitors of continuance intention of mobile social networking sites. Telematics and Informatics 2016 Nov;33(4):1022-1033. [doi: 10.1016/j.tele.2016.03.006]
46. Vaghefi I, Tulu B. The Continued Use of Mobile Health Apps: Insights From a Longitudinal Study. JMIR Mhealth Uhealth 2019 Aug 29;7(8):e12983 [FREE Full text] [doi: 10.2196/12983] [Medline: 31469081]
47. Baig K, Mohamed R, Theus AL, Chiasson S. "I'm hoping they're an ethical company that won't do anything that I'll regret": Users Perceptions of At-home DNA Testing Companies. 2020 Presented at: Conference on Human Factors in Computing Systems; April 25-30, 2020; Honolulu, HI. [doi: 10.1145/3313831.3376800]
48. Jonker M, de Bekker-Grob E, Veldwijk J, Goossens L, Bour S, Rutten-Van Mölken M. COVID-19 Contact Tracing Apps: Predicted Uptake in the Netherlands Based on a Discrete Choice Experiment. JMIR Mhealth Uhealth 2020 Oct 09;8(10):e20741 [FREE Full text] [doi: 10.2196/20741] [Medline: 32795998]
49. Acquisti A, Grossklags J. Losses, gains, and hyperbolic discounting: an experimental approach to information security attitudes and behavior in 2nd Annual Workshop on Economics and Information Security-WEIS;3(Berkeley, CA)?27UC Berkeley 2003. 2003 Presented at: 2nd Annual Workshop on “Economics and Information Security”; March 18, 2003; Berkeley, CA.
50. Igo SE. The known citizen: A history of privacy in modern America. Cambridge, MA: Harvard University Press; 2018.
51. McDonald N, Forte A. The politics of privacy theories: moving from norms to vulnerabilities. 2020 Presented at: Conference on Human Factors in Computing Systems; April 25-30, 2020; Honolulu, HI. [doi: 10.1145/3313831.3376167]
52. Gove WR, Altman I. The Environment and Social Behavior: Privacy, Personal Space, Territory, Crowding. Contemporary Sociology 1978 Sep;7(5):638. [doi: 10.2307/2065073]
53. Bannerman S. Relational privacy and the networked governance of the self. Information, Communication & Society 2018 May 29;22(14):2187-2202. [doi: 10.1080/1369118x.2018.1478982]
54. Petronio S. Boundaries of privacy: Dialectics of disclosure. Albany, NY: SUNY Press; 2002.
55. Nissenbaum H. Privacy in context: Technology, policy, and the integrity of social life. Redwood City, CA: Stanford University Press; 2009.
56. Crabtree A, Tolmie P, Knight W. Repacking 'Privacy' for a Networked World. Comput Support Coop Work 2017 May 29;26(4):453-488 [FREE Full text] [doi: 10.1007/s10606-017-9276-y] [Medline: 32025101]
57. Nippert-Eng CE. Islands of privacy. Chicago, IL: University of Chicago Press; 2010:0226586537.
58. Margulis ST. Privacy as a social issue and behavioral concept. Journal of Social Issues 2003;59:261. [doi: 10.1111/1540-4560.00063]
59. Solove DJ. A Taxonomy of Privacy. University of Pennsylvania Law Review 2006;154(3):477-564. [doi: 10.2307/40041279]
60. Solove DJ. Understanding privacy. Cambridge, MA: Harvard University Press; 2008.
61. Stark L. The emotional context of information privacy. The Information Society 2015 Dec 22;32(1):14-27. [doi: 10.1080/01972243.2015.1107167]
62. Shklovski I, Mainwaring SD, Skuladottir HH, Borgthorsson H. Leakiness and creepiness in app space: perceptions of privacy and mobile app use. 2014 Presented at: SIGCHI Conference on Human Factors in Computing Systems; April 26-May 1, 2014; Toronto, Ontario, Canada p. 2347-2356. [doi: 10.1145/2556288.2557421]
63. Stanton B, Theofanos MF, Prettyman SS, Furman S. Security Fatigue. IT Prof 2016 Sep;18(5):26-32. [doi: 10.1109/mitp.2016.84]
64. Furnell S, Thomson K. Recognising and addressing ‘security fatigue’. Computer Fraud & Security 2009 Nov;2009(11):7-11. [doi: 10.1016/s1361-3723(09)70139-3]
65. Norberg PA, Horne DR, Horne DA. The privacy paradox: personal information disclosure intentions versus behaviors. The Journal of Consumer Affairs 2007;41:126. [doi: 10.1111/j.1745-6606.2006.00070.x]
66. Seberger JS, Llavore M, Wyant NN, Shklovski I, Patil S. Empowering Resignation: There’s an App for That. 2021 Presented at: Conference on Human Factors in Computing Systems; May 8-13, 2021; Yokohama, Japan. [doi: 10.1145/3411764.3445293]
67. Paasonen S. As Networks Fail. Television & New Media 2014 Oct 08;16(8):701-716. [doi: 10.1177/1527476414552906]
68. Cumbley R, Church P. Is “Big Data” creepy? Computer Law & Security Review 2013 Oct;29(5):601-609. [doi: 10.1016/j.clsr.2013.07.007]

69. West E. Amazon: Surveillance as a Service. SS 2019 Mar 31;17(1/2):27-33. [doi: 10.24908/ss.v17i1/2.13008]
70. Haggerty K, Ericson R. The surveillant assemblage. Br J Sociol 2000 Dec;51(4):605-622. [doi: 10.1080/00071310020015280] [Medline: 11140886]
71. Seberger JS, Bowker GC. Humanistic infrastructure studies: hyper-functionality and the experience of the absurd. Information, Communication & Society 2020 Feb 21;24(12):1712-1727. [doi: 10.1080/1369118x.2020.1726985]
72. O'Brien BC, Harris IB, Beckman TJ, Reed DA, Cook DA. Standards for reporting qualitative research: a synthesis of recommendations. Acad Med 2014 Sep;89(9):1245-1251 [FREE Full text] [doi: 10.1097/ACM.0000000000000388] [Medline: 24979285]
73. Levitt HM, Motulsky SL, Wertz FJ, Morrow SL, Ponterotto JG. Recommendations for designing and reviewing qualitative research in psychology: Promoting methodological integrity. Qualitative Psychology 2017 Feb;4(1):2-22. [doi: 10.1037/qup0000082]
74. Dick S, O'Connor Y, Thompson MJ, O'Donoghue J, Hardy V, Wu TJ, et al. Considerations for Improved Mobile Health Evaluation: Retrospective Qualitative Investigation. JMIR Mhealth Uhealth 2020 Jan 22;8(1):e12424 [FREE Full text] [doi: 10.2196/12424] [Medline: 32012085]
75. Braun V, Clarke V. Using thematic analysis in psychology. Qualitative Research in Psychology 2006 Jan;3(2):77-101. [doi: 10.1191/1478088706qp063oa]
76. Ackerman MS, Cranor LF, Reagle J. Privacy in E-Commerce: Examining User Scenarios and Privacy Preferences. 1999 Presented at: 1st ACM Conference on Electronic Commerce; November 3-5, 1999; Denver, CO. [doi: 10.1145/336992.336995]
77. Hine C. Privacy in the Marketplace. The Information Society 1998 Nov;14(4):253-262. [doi: 10.1080/019722498128700]
78. Martin K, Shilton K. Putting mobile application privacy in context: An empirical study of user privacy expectations for mobile devices. The Information Society 2016 Apr 13;32(3):200-216. [doi: 10.1080/01972243.2016.1153012]
79. Meinert S. Field manual - Scenario building. European Trade Union Institute. 2014. URL: https://www.etui.org/publications/guides/field-manual-scenario-building [accessed 2021-09-23]
80. Kaptchuk G, Goldstein DG, Hargittai E, Hofman J, Redmiles EM. How good is good enough for COVID19 apps? The influence of benefits, accuracy, and privacy on willingness to adopt. Cornell University. 2020 May 18. URL: https://arxiv.org/abs/2005.04343 [accessed 2021-09-23]
81. Allmark P, Boote J, Chambers E, Clarke A, McDonnell A, Thompson A, et al. Ethical Issues in the Use of In-Depth Interviews: Literature Review and Discussion. Research Ethics 2009 Jun 01;5(2):48-54. [doi: 10.1177/174701610900500203]
82. Wash R, Radar E. Influencing mental models of security: a research agenda. 2011 Presented at: New Security Paradigms Workshop; September 12-15, 2011; Marin County, CA. [doi: 10.1145/2073276.2073283]
83. Halpern SD, Truog RD, Miller FG. Cognitive Bias and Public Health Policy During the COVID-19 Pandemic. JAMA 2020 Jul 28;324(4):337-338. [doi: 10.1001/jama.2020.11623] [Medline: 32597963]
84. Bowker GC. Temporality. Society for Cultural Anthropology. 2015 Sep 24. URL: https://culanth.org/fieldsights/temporality [accessed 2021-09-23]
85. Acquisti A, Grossklags J. Privacy and rationality in individual decision making. IEEE Secur. Privacy Mag 2005 Jan;3(1):26-33. [doi: 10.1109/MSP.2005.22]
86. Latour B. Imaginer les gestes-barrieres contre le retour a la production d'avant-crise. AOC. 2020 Mar 30. URL: https://aoc.media/opinion/2020/03/29/imaginer-les-gestes-barrieres-contre-le-retour-a-la-production-davant-crise/ [accessed 2021-09-23]
87. Zhang X, Liu S, Chen X, Wang L, Gao B, Zhu Q. Health information privacy concerns, antecedents, and information disclosure intention in online health communities. Information & Management 2018 Jun;55(4):482-493. [doi: 10.1016/j.im.2017.11.003] [Medline: 30872122]
88. Clark CC. Trust in medicine. J Med Philos 2002 Feb 1;27(1):11-29. [doi: 10.1076/jmep.27.1.11.2975] [Medline: 11961684]
89. Irurita VF. The problem of patient vulnerability. Collegian 1999 Jan;6(1):10-15. [doi: 10.1016/s1322-7696(08)60310-8]

Abbreviations

GDPR: General Data Protection Regulation
HCI: human-computer interaction
HIPAA: Health Insurance Portability and Accountability Act
mHealth: mobile health

Edited by L Buis; submitted 01.06.21; peer-reviewed by M Lotto, M Holter; comments to author 28.06.21; revised version received 19.07.21; accepted 05.08.21; published 05.10.21

Please cite as:
Seberger JS, Patil S
Post-COVID Public Health Surveillance and Privacy Expectations in the United States: Scenario-Based Interview Study
JMIR Mhealth Uhealth 2021;9(10):e30871
URL: https://mhealth.jmir.org/2021/10/e30871
doi: 10.2196/30871
PMID: 34519667