How the introduction of the COVID-19 tracing apps affects future tracking technology adoption

Christian Matt
Institute for Information Systems, University of Bern, Bern, Switzerland, and
Mena Teebken and Beril Özcan
Institute for Digital Management and New Media, LMU Munich, Munich, Germany

Received 14 May 2022
Revised 8 June 2022
Accepted 12 June 2022

Abstract

Purpose – Studies on the coronavirus disease 2019 (COVID-19) tracing apps have mostly focused on how to optimize adoption and continuous use, but did not consider potential long-term effects of their introduction. This study aims to analyse whether the characteristics of the recent introduction of tracing apps may negatively impact individuals' attitudes and intentions to adopt future tracking technology.

Design/methodology/approach – In an online experiment across three countries (Australia, Germany, UK), the authors measured how perceived benefits of COVID-19 tracing apps as well as specific government and campaign-related factors affect privacy concerns, attitude towards future tracking apps and intention to adopt. The authors manipulated the type of provider (governmental vs private) and the type of beneficiaries of the future tracking technology app (the individual alone or also the public) as determinants of adoption.

Findings – The authors find that privacy concerns towards the COVID-19 tracing apps negatively impact attitude and intention to adopt future tracking apps. Future adoption is more likely if the app is provided by the government, whereas additional benefits to the public do not positively stimulate adoption. Second, the study analyzed different factors, including perceptions on governments and the app introduction, as well as perceived benefits.

Originality/value – Taking the introduction of COVID-19 apps in different countries as a basis, the authors link both perceived benefits and contextual factors to privacy concerns, attitudes towards and intention to adopt the related technology in the future. The authors hereby clarify the responsibility of governmental actors who conduct large-scale technology introductions for the future diffusion of related technologies.

Keywords COVID-19 tracing apps, App campaigns, Tracking app adoption, Perceived benefits, Attitude

Paper type Research paper

1. Introduction

Since the beginning of the coronavirus disease 2019 (COVID-19) turning into the global pandemic in 2020, among other digital solutions, COVID-19 tracing apps have been seen as one of the main tools to contain the further spread of the virus (O'neill, Ryan-Mosley, & Johnson, 2020). More than 50 countries around the world opted for contact tracing applications as a supplementary method. Many developed their own contact tracing apps, which comprised

The authors want to thank the entire review team for their constructive feedback and excellent guidance throughout the review process. The project was funded by the German Federal Ministry of Education and Research (grant 16KIS0748).

Digital Transformation and Society
Emerald Publishing Limited
2755-0761
DOI 10.1108/DTS-05-2022-0015

different technologies (e.g. Bluetooth or Global Positioning System (GPS)) and architectures (e.g. centralized or decentralized data storage).

Since high adoption rates were claimed to be necessary to effectively contain the pandemic – ranging from 60% (Hinch *et al.*, 2020) to 15% of the population (Hurtz, 2020) – many governments provided extensive information campaigns both offline and online (Sacco, Christou, & Bana, 2020). Some governments were subject to public discussions of their ethical approaches (Matt, 2022). Simko, Calo, Roesner and Kohno (2020) found that users had feelings of unease and concerns over the government reach and the usage of personal data, leading to more reluctance and lower adoption rates for COVID-19 apps. While a plethora of studies have focused on adoption factors for the current COVID-19 apps (Cho, Ippolito, & Yu, 2020; Urbaczewski & Lee, 2020), the question emerges whether the recent introduction of COVID-19 apps has also had an impact on individuals' assessment of future tracking applications. It can be speculated that negative perceptions or experiences during the introduction of COVID-19 apps may have made individuals more likely to ignore risks during the introduction of future tracking apps (Li *et al.*, 2020; Rowe, Ngwenyama, & Richet, 2020). However, concrete empirical evidence is currently still missing. To fill the research gap, we draw on the APCO (Antecedents → Privacy concerns → Outcomes) model (Dinev, Mcconnell, & Smith, 2015) and the theory of planned behavior (Ajzen, 1991), and respond to the following research questions:

(1) Has the introduction of COVID-19 tracing apps affected individuals' intention to use future tracking apps?

(2) Are there differential effects stemming from (a) whether the government or a private firm provides the app, and (b) whether only the individual user benefits from the app or if there are also broader public benefits?

We conducted an online experiment with more than 1,000 participants in three countries (Germany, Australia and the United Kingdom) to test our model. We respond to the call from Yun, Lee and Kim (2019) and explore privacy concerns related to emerging technologies in a specific context. We believe this will also pave the way for future research focusing on the adoption of large-scale socio-technical innovations concerning upcoming tracking applications. It has implications for governments and private firms to understand whether large-scale technology implementations may also affect the future diffusion of the underlying technology. The paper is structured as follows: We first introduce the conceptual foundations on the functioning and diffusion of contact tracing apps, as well as on information privacy concerns. Next, we present our conceptual framework and hypotheses, before we outline the methodology. Thereafter, we present and discuss the results and their theoretical and practical implications. Finally, we end with a short conclusion and the limitations.

2. Conceptual foundations

2.1 Functioning and diffusion of contact tracing apps

Contact tracing is a method to control infectious disease outbreaks by detecting infection chains through identifying and warning infected individuals and their potential contacts. The general principle is that user devices exchange tokens once a certain time is spent (e.g. 15 minutes) in proximity (e.g. less than two meters) where infections would be risky. Nevertheless, this requires users to be willing to disclose their information on the app, including declaring that they have the infection. The concepts of tracing and tracking emerged from the field of logistics, being based on shipment tracking. For contact tracing, the word "tracking" is less applicable as it relates to gaining knowledge in real-time, whereas "tracing" refers to gaining knowledge in retrospect (Van Dorp, 2002). Before the use of digital technologies, the tracing process was handled manually, for instance, in Africa during the Ebola epidemic. Manual contact tracing via paper

suffers from problems with contact identification, communication issues, such as delays, incomplete information transfer, loss of data and transcriptions being error-prone (Danquah *et al.*, 2019). Using smartphones for tracing is not only less labor-intensive, it can also be extended rapidly to a large crowd. From a technical perspective, a variety of methods have been discussed in terms of effectiveness, privacy and security risks, including using Bluetooth technology, GPS data or other wireless technologies (Raskar *et al.*, 2020). Bluetooth technology is preferred over GPS in most contact tracing apps due to privacy advantages (O'neill *et al.*, 2020; Ciucci & Gouardères, 2020). Another discussion has been whether the collected data should be stored and managed decentrally on the users' smartphones or on a central server hosted by the provider or by health authorities (Ciucci & Gouardères, 2020). The centralized structure faced concerns over privacy and security (Holmes, Mccurry, & Safi, 2020).

Wider adoption of COVID-19 tracing apps implies better tracing and control of the pandemic (Ferretti *et al.*, 2020). To motivate their adoption, extensive government campaigns were conducted across countries, often emphasizing the collective effort to fight the pandemic (Sharma *et al.*, 2020). However, non-governmental organization (NGOs) and public media have variously questioned tracing apps' general effectiveness, and their potential privacy and security risks (Amnesty International, 2020; Zhong, 2020), and accused some campaigns of being incomplete, biased or misleading (The Bogota Post, 2020; Zhong, 2020). Poorly designed tracing campaigns have been accused of leading the public to overestimate unfounded fears that deter their adoption. As a consequence, this may also affect individuals' subsequent receptiveness to adopting any future tracking technologies (Rowe *et al.*, 2020).

2.2 Information privacy concerns

Information privacy is defined as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (Malhotra, Kim, & Agarwal, 2004). Various scales have been developed to measure information privacy concerns. Concern for Information Privacy (CFIP) was proposed by Smith, Milberg and Burke (1996) as a multidimensional 15-item scale, incorporating collection, errors, unauthorized secondary use and improper access. Malhotra *et al.* (2004) developed Internet Users' Information Privacy Concerns (IUIPC), focusing on the privacy concerns on the internet context specifically, which includes the three dimensions control over personal information, awareness of organizational privacy practices and collection of personal information. Building upon the foundations of CFIP, IUIPC and Communication Privacy Management (CPM) theory, Xu, Gupta, Rosson and Carroll (2012) proposed the Mobile Users' Information Privacy Concerns (MUIPC) as a framework specifically for the mobile context, incorporating perceived surveillance, perceived intrusion and secondary use of personal information (Xu *et al.*, 2012).

COVID-19 tracing apps fostered discussions on privacy issues with the usage of personal health information, including location data or health data, as well as surveillance concerns (Trang, Trenz, Weiger, Tarafdar, & Cheung, 2020; Cho *et al.*, 2020). Thereby, privacy concerns have been found to be one of the most significant barriers to their adoption (Matt, 2022). To study privacy in such complex contextual settings, Smith, Dinev and Xu (2011) developed the APCO macro model. This model has been widely adapted and is used to explain the effects of privacy policies or the General Data Protection Regulation (GDPR) on privacy concerns (Paul, Scheibe, & Nilakanta, 2020) or to investigate how privacy concerns affect the usage of mobile payment solutions (Reith, Buck, Walther, Lis, & Eymann, 2019), social networking websites (Alashoor, Han, & Joseph, 2017) and fitness trackers (Reith, Buck, Lis, & Eymann, 2020). Our theoretical basis is twofold: Together with the APCO model, we use the theory of planned behavior (Ajzen, 1991), since it has not only been one of the most prominent theories linking beliefs to behavior, but also since it has seen many successful applications in the fields of ethical aspects of technology use, consumer trust and privacy (Cheung & To, 2017; Jafarkarimi, Saadatdoost, Sim, & Hee, 2016).

3. Conceptual framework model and hypotheses development

Previous studies have shown that both the benefits associated with the COVID-19 app (Matt, 2022; Trang *et al.*, 2020), as well as the particular organization that provides the app play a significant role in user adoption (Horvath, Banducci, & James, 2020; Li *et al.*, 2020; Redmiles, 2021). For our research model, we therefore integrate factors from both categories. First, we differentiate two beneficiary perceptions: perceived benefits for the individual user and perceived benefits for the public (Figure 1). Second, we integrate perceptional factors regarding the provider and the provision of the COVID-19 app: trust in the government as well as the perceived campaign transparency. All these factors are expected to influence privacy concerns that, in turn, affect attitude and behavioral intention to use future tracking apps. We further distinguish usage based on whether the future tracking app benefits only the individual or in addition also the public, and whether the government or a private firm is the provider. We describe our hypotheses in the following.

3.1 Perceived benefits of COVID-19 tracing apps

Successful adoption of technologies is closely linked with the perceived benefits that individuals associate with their use (Venkatesh *et al.*, 2003, 2012). Since technology use can entail the disclosure of personal information, this has been extensively studied in the contexts of personalized offerings, location-based services (Xu, Teo, Tan, & Agarwal, 2009), as well as health services and applications (Adu, Mills, & Todorova, 2017; Zhang *et al.*, 2018; Kordzadeh & Warren, 2017; Chiu, Hsu, & Wang, 2006). As benefits, COVID-19 contact tracing apps offer (1) knowledge of risk, (2) knowledge of hotspots, (3) feeling of altruism, and helps (4) improving environment safety, (5) protecting loved ones and (6) contributing epidemiological data (Redmiles, 2021). While some of the benefits affect the individual user as a beneficiary, others affect society at large. We define perceived personal benefits of COVID-19 apps as the positive outcomes that users receive by using these apps and sharing personal information with these apps (Chiu *et al.*, 2006). It has been found that individuals' likelihood to use digital contact tracing apps increases with a higher expectation of personal benefits (Sharma *et al.*, 2020). In contrast, public benefit refers to the positive outcomes the community will receive (Kordzadeh & Warren, 2017). In the context of COVID-19 apps, the challenges to activate user perceptions of public benefits have been discussed (Matt, 2022; Trang *et al.*, 2020).

From the privacy calculus, we know that perceived benefits can have an attenuating effect on privacy concerns (Dinev & Hart, 2006). For young consumers, expected benefits through tracing apps can compensate for related privacy concerns (Jahari, Hass, Hass, & Joseph, 2022). It is also known that users' focus of privacy trade-offs is often more geared towards the benefits of the app rather than the privacy risks (Naous, Bonner, Humbert, & Legner, 2022). Barth and De Jong (2017) found that users are willing to compromise their privacy based on cost–benefit trade-offs. Therefore, the higher the perceived benefits of COVID-19 tracing apps

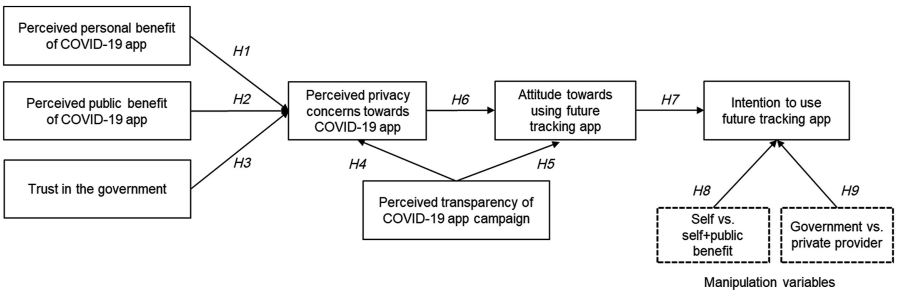


Figure 1.
Research model

– both for the individual but also for society – the more should individuals be likely to suppress their privacy concerns towards the apps. We hold:

H1. Perceived personal benefit of using COVID-19 tracing apps has a negative effect on perceived privacy concerns.

H2. Perceived public benefit of using COVID-19 tracing apps has a negative effect on perceived privacy concerns.

3.2 Trust in the government and campaign transparency

In the context of privacy, trust has seen various conceptual understandings and model-based implementations, some of which include trust as a mediator between privacy concerns and data disclosure (Bansal, Zahedi, & Gefen, 2010; Liu, Marchewka, Lu, & Yu, 2004; Malhotra *et al.*, 2004), as moderating factor (Bansal, Zahedi, & Gefen, 2008), or as an antecedent to privacy (Reith *et al.*, 2019). The success of COVID-19 tracing app adoption has been linked to trust in the government (Riemer, Ciriello, Peter, & Schlagwein, 2020). Individuals have concerns about governments' handling of their data (Simko *et al.*, 2020). For instance, Horvath *et al.* (2020) found that trust in the UK National Health Service has overridden privacy concerns for COVID-19 tracing apps. We integrate trust as the extent to which users are confident that the government, as the provider of COVID-19 apps, will handle their personal data with competence, reliability and safety (Dinev & Hart, 2006), and we argue that higher trust in the government will be negatively associated with privacy concerns.

H3. Trust in the government issuing the COVID-19 tracing apps has a negative effect on perceived privacy concerns towards COVID-19 tracing apps.

Also, the circumstances of COVID-19 tracing app campaigns have received particular attention, especially concerning their transparency about the apps' purpose, functionality and data processing (Zhong, 2020). Studies have discovered that app providers and responsible authorities often fail to communicate important information on data storage and management, privacy and security risks (Fahey & Hino, 2020). Surveys show that only 58% of respondents believe the information communicated by their national governments automatically, or after seeing it twice or less (Edelman, 2021). Policymakers in governments should take necessary precautions to transparently inform the users regarding the apps' features and the collected data, how the data are used and handled, and with whom the data are shared (Lucivero *et al.*, 2020).

Leins, Culnane and Rubinstein (2020) highlighted the requirements for clear and transparent communication based on factual aspects to build trust and overcome concerns regarding the COVID-19 apps and the underlying technology. The complex structure and the lack of clarity of the concrete functionality of COVID-19 tracing apps, as well as the extent of the data collection, triggered misunderstandings that resulted in fear of data privacy and surveillance issues (Zimmermann *et al.*, 2021). Weaknesses of perceived transparency, combined with privacy concerns, have led to resistance to install tracing apps (Rowe *et al.*, 2020). In line with this, we argue that transparent introduction campaigns can help reduce privacy concerns. Given the susceptibility that individuals demonstrated towards governments based on their negative experiences, we also hold that there is also a direct positive link between the transparency of introduction campaigns and individuals' attitude towards using a future tracking app.

H4. Perceived transparency with COVID-19 tracing app campaigns has a negative effect on perceived privacy concerns towards COVID-19 tracing apps.

H5. Perceived transparency with COVID-19 tracing app campaigns has a positive effect on the attitude towards the future use of tracking apps.

3.3 Privacy concerns towards COVID-19 apps

Li (2012) points out that privacy concerns are an important behavioral belief that influences privacy-related attitudes. Privacy concerns motivate certain privacy-related behaviors, including privacy protection behaviors (Chen, Beaudoin, & Hong, 2017), a decrease in willingness to share information online (Li & Chen, 2010) or using a technology (Palanisamy, 2014). Examining privacy concerns regarding embedded tracking technology, Ketelaar and Van Balen (2018) found negative user attitudes as a result of privacy concerns. Privacy concerns are also negatively associated with the attitude towards and adoption of location-based services (Dhar & Varshney, 2011), and other health technologies (Xu, 2019). The negative effects of privacy concerns on behavioral outcomes have also been confirmed by empirical studies in the context of disclosing personal health information (Anderson & Agarwal, 2011; Dinev, Albano, Xu, D'atri, & Hart, 2016). In the context of COVID-19 tracing apps, Simko *et al.* (2020) found that even with perfect privacy conditions, individuals show negative attitudes and are still hesitant to install apps due to privacy concerns. We hold:

H6. Perceived privacy concerns towards COVID-19 tracing apps have a negative effect on the attitude towards the use of future tracking apps.

3.4 Attitude and intention towards using future tracking apps

As "the degree to which a person has a favorable or unfavorable evaluation or appraisal of the behavior in question" (Ajzen, 1991), favorable attitudes generally result in higher behavioral intention. Also, the technology acceptance model (TAM) indicates that a technology's actual usage is driven by peoples' intentions, which in turn are determined by their attitude (Aloudat, Michael, Chen & Al-Debei, 2014; Davis, 1989). Therefore, it can be assumed that attitudes towards a certain technology determine intentions to use that technology. This relation is well-established across different research contexts and technologies used. Also, previous studies in the context of privacy concerns confirm the positive effect of attitude on intention, for instance, Angst and Agarwal (2009) in the context of electronic health records, or Aloudat *et al.* (2014) for location-based services. Drawing from these previous studies, we hypothesize:

H7. Attitude towards using future tracking apps has a positive effect on the intention to use those apps.

The literature on privacy has placed a strong focus on benefit structures, showing that individuals calculate risks and benefits (privacy calculus) before disclosing personal information (Dinev & Hart, 2006). Individuals tend to perceive the risks to be lower when the benefits they receive are immediate (Wilson & Valacich, 2012). However, many people are unable to evaluate the risks and benefits when making a privacy decision due to incomplete information and bounded rationality (Acquisti & Grossklags, 2005). In the case of immediate benefits, user attitudes towards privacy can change rapidly (Kokolakis, 2017). For COVID-19 tracing apps, empirical evidence shows that users focus more on the benefits of the app and less on privacy risks and costs (Naous *et al.*, 2022). Previous studies have shown that individuals' perceived benefit for themselves has a stronger influence on their adoption intention than the perceived benefits for others (Matt, 2022; Trang *et al.*, 2020). However, promising additional benefits for the public in addition to what is already promised as benefits for individuals should still lead to a higher overall usage intention. We hypothesize:

H8. Perceived benefits for both the individual and the public have a stronger positive effect on the intention to use future tracking apps than benefits for the individual alone.

Previous studies indicated the significant effect of government involvement on usage intention (Simko *et al.*, 2020). James and Jilke (2020) found that delivery of public services on co-production is preferred when being provided by public organizations instead of for-profit service providers. They suggest that, in order to revive the citizens' willingness to cooperate, public organizations may emphasize their public ownership of the provided service (James & Jilke, 2020). On the other hand, Simko *et al.* (2020) found that users feel more comfortable with Google as COVID-19 tracing app providers. Similarly, US citizens showed a high degree of trust toward Google and Apple as providers for COVID-19 apps (Newton, 2020). There also exist concerns by individuals regarding the government handling their data (Simko *et al.*, 2020). Approximately, 42% of individuals are worried about the future use of contact tracing apps due to possible government surveillance through these apps (Altmann *et al.*, 2020). However, Yun *et al.* (2019) pointed out that commercial firms have been the subject of privacy research while privacy concerns towards governments were overlooked. Therefore, specifically in health contexts, there is only limited knowledge regarding this relationship (Yun *et al.*, 2019). Also, Google and other large tech companies have been widely criticized for their privacy practices (Dwyer, 2011; Clemons & Wilson, 2015), given that those firms follow strict commercial interests. Thus, we believe in the credibility of public institutions for sensitive health data and hold:

H9. Governments as providers of future tracking technology have a positive effect on individuals' intention to use.

4. Methodology

4.1 Research design and operationalization

We implemented a vignette-based online experiment through Qualtrics since online vignette-based scenarios are commonly utilized to explore behavioral outcomes (Meulendijk, Meulendijks, Jansen, Numans, & Spruit, 2014; Udesky, Boronow, Brown, Perovich, & Brody, 2020). We used a 2 (app provider: government vs private company) × 2 (communicated beneficiary: self-benefit vs self and public benefit) between-subject design (Table 1).

The measurement items were adopted from existing literature and relied on reflective measurements using a seven-point Likert scale ranging. Items for the perceived public and self-benefit of COVID-19 apps were adopted from Kordzadeh and Warren (2017), being understood as "expected positive community-related outcomes of sharing PHI (personal health information)" and "expected positive personal outcomes of sharing PHI". Trust in the government issuing COVID-19 apps was measured with items adopted from Hong and Thong (2013) and Malhotra *et al.* (2004). To measure perceived transparency with the COVID-19 app campaigns, we drew from Schnackenberg, Tomlinson and Coen (2020). We adopted perceived privacy concerns from Dinev and Hart (2006). The items used to measure attitude were based on prior scales from Venkatesh *et al.* (2003). Measurement items for intention to use future tracking apps were adopted from Malhotra *et al.* (2004) and Venkatesh *et al.* (2003).

App provider	Communicated beneficiary Self benefit	Self and public benefit
Government	Group 1a	Group 1b
Private company	Group 2a	Group 2b

Table 1.
Treatment groups

4.2 Sample and data collection

Prior to the data collection, we conducted a pilot test with 20 participants to ensure the comprehensibility and clarity of the survey questions and the manipulations, leading to minor design and flow modifications. The final study was distributed on Prolific in February 2021 in English and German.

In the beginning, all participants were informed about the scope of the study, followed by demographic questions, and information on the current usage of a COVID-19 tracing app. We integrated an attention check, asking the participants to mark "strongly disagree" as the right option. Subsequently, questions on perceived public benefit, perceived personal benefit, trust in the government issuing the COVID-19 tracing app and transparency of COVID-19 tracing app campaigns were presented to the users. We later asked the participants about their feelings and attitude towards future tracking apps in general, presenting them with a simple image and describing the tracking apps as "*applications that use GPS/location tracking technologies, and/or contact tracing technologies*". Before proceeding with the experiment, we integrated a second attention check, and the participants who failed both attention checks were automatically dismissed from the survey.

Next, participants were provided with a cover story informing them that they would be presented with a mobile application that is available in the future from major app stores. The subjects were now randomly assigned to one of the four treatment scenarios and provided with a mobile application download page provided on the App Store, which included the app logo, app name and app provider information (i.e. Google, the domestic Ministry of Health), and a detailed description of the app features and benefits (Figure 2). The app providers were indicated on the upper left-hand side, while the benefits of use that participants could expect were illustrated with a logo as well as in textual form.

5. Data analysis

5.1 Data cleaning and sample description

We conducted data cleaning prior to any statistical analysis with the aim of expanding the validity and quality of the results, using the following criteria: No missing data from participants, correct attention check questions, realistic completion time and realistic response pattern. From a total of 1,203 participants who completed the study, 79 participants were excluded, leading to a final sample of 1,124 participants, of which 515 were male (45.8%), 598 were female (53.2%), and 11 participants either chose other or preferred not to mention their gender (1.0%) (Table 2). Participants had their residence in Australia (366), Germany (380) or the United Kingdom (378). The majority of participants were within the 25–34 age group. In total, 490 participants had a COVID-19 tracing app installed at the time of the study (43.6%), while 18.9% stated that they were users before but uninstalled the app. Table 3 provides an overview of the overall and the country-specific means for the main constructs.

5.2 Manipulation check

To test whether the four treatment groups could be considered independent, we compared participants' demographical data between the groups. There were no significant differences between the four treatment groups concerning gender ($\chi^2 = 0.323$), age ($\chi^2 = 0.292$) and education ($\chi^2 = 0.575$). To test the success of the manipulation of our experimental treatments, government involvement and communicated beneficiary, we asked two binary questions. First, we asked about the highlighted advantages of the app (for my own safety and health vs for my own and the societies' safety and health), which was adapted from Trang *et al.* (2020), and second, by whom the app was provided (government vs private company) to check the manipulation for government involvement, adapted from (Hvidman &

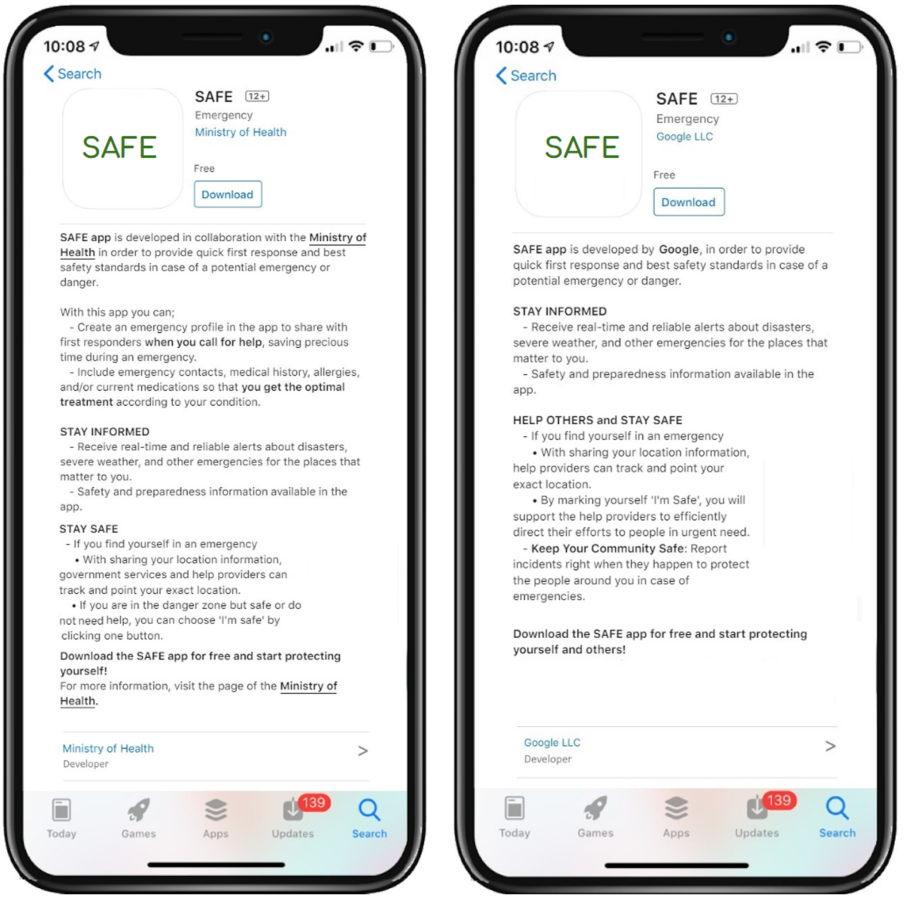


Figure 2.
Government – self-benefit case (left) and private company – self and public benefits case (right)

Andersen, 2016). Two independent samples *t*-tests revealed significant group differences for app providers and communicated beneficiaries on a 0.05 significance level. We can therefore conclude that the effectiveness of the manipulation was stronger for the app provider manipulation. Because we pre-tested the manipulation design and found realistic response patterns, we decided to exclude only participants who had not correctly responded to both manipulation checks, since also for other apps, users may not always be able to pay full attention to all incoming information and user dialogs but still be seen as committed users (Table 4).

6. Results

6.1 Measurement model analysis

Using Cronbach's alpha (CA) and composite reliability (CR), we evaluated the internal consistency reliability. For CA, all constructs exceeded the threshold of 0.7 (Tavakol & Dennick, 2011; Mackenzie, Podsakoff, & Podsakoff, 2011). Similarly, with CR, the lowest value was 0.896, exceeding the threshold of 0.7 (Table 5).

Variable		Frequency	Percent
Age	18–24	319	28.4
	25–34	458	40.7
	35–44	217	19.3
	45–54	82	7.3
	55–65	41	3.6
	66 or higher	7	0.6
Gender	Male	515	45.8
	Female	598	53.2
	Other	9	0.8
	Prefer not to say	2	0.2
Residence	Australia	366	32.6
	Germany	380	33.8
	The United Kingdom	378	33.6
Education	Secondary school	84	7.5
	High school degree or equivalent	334	29.7
	Bachelor	429	38.2
	Master/Diploma	219	19.5
	PhD	37	3.3
	No school qualification	2	0.2
	Other	19	1.7
Current use of COVID-19 app	I am already a user	490	43.6
	I was a user, but not anymore	212	18.9
	I plan to use it sometime in the future	75	6.7
	Not sure whether I will ever use it	273	24.3
	I will never use it	74	6.6

Table 2.
Descriptive statistics

Constructs	Overall mean (SD)	Australia mean (SD)	Germany mean (SD)	UK mean (SD)
Perceived self- benefit	3.67 (1.31)	3.64 (1.35)	3.60 (1.31)	3.76 (1.27)
Perceived public benefit	2.89 (1.25)	2.96 (1.27)	2.74 (1.29)	2.97 (1.19)
Trust in government	4.25 (1.38)	4.23 (1.34)	3.88 (1.39)	4.64 (1.31)
Campaign transparency	3.34 (1.93)	3.29 (1.18)	3.06 (1.10)	3.66 (1.22)
Privacy concerns	3.37 (1.44)	3.02 (1.29)	4.04 (1.50)	3.06 (1.30)
Attitude towards tracking apps	4.16 (1.42)	4.18 (1.41)	4.06 (1.37)	4.24 (1.46)
Intention to use tracking apps	4.08 (1.67)	4.21 (1.68)	4.07 (1.62)	3.97 (1.70)

Table 3.
Construct means

To test convergent validity, the average variance extracted of each latent variable was evaluated (Hair, Risher, Sarstedt, & Ringle, 2019). As all average variance extracted (AVE) values exceed the acceptable threshold of 0.5, the model therefore demonstrated sufficient convergent validity.

To assess discriminant validity between constructs, we used the Fornell–Larcker criterion, based on which the shared variance for all constructs should not exceed their AVEs, which we confirmed (Table 6).

To assess collinearity issues of the inner model, we used the inner variance inflation factor (VIF) (Hair, Hult, Ringle, & Sarstedt, 2016). We applied a full collinearity test (Kock & Lynn, 2012), since the VIF results are also useful to determine common method bias (CMB). Two questions that were irrelevant to the study context were asked to the participants at the end of

the survey to assess potential. All VIF values were lower than 3.3, thus providing no indication of common method bias (Kock, 2015).

6.2 Hypotheses assessment

The results indicate that several factors directly affect individuals' privacy concerns for the current COVID-19 app (Figure 3). Both perceived personal benefits ($\beta = -0.108, p = 0.010$) as well as perceived public benefit ($\beta = -0.089$, $p = 0.038$) have a significant negative relationship with privacy concerns, thus supporting H1 and H2. Trust in the government exhibits the strongest negative relation with privacy concerns ($\beta = -0.302, p < 0.001$), thus supporting H3. The perceived transparency of the COVID-19 app campaign has a dual effect, as it helps reducing privacy concerns ($\beta = -0.190, p < 0.001$), as well as leading to a more positive attitude toward future tracking apps ($\beta = 0.188, p < 0.001$). Given its dual effect on the assessment of the privacy concerns for the current app as well as affecting the attitude towards future tracking app technologies, we obtain support for H4 and H5. We also obtain support for H6 since there is a negative link between privacy concerns and the attitude toward the future tracking apps ($\beta = -0.294, p < 0.001$). The last three hypotheses are related to the intention to use future tracking apps. H7 suggested that attitude has a direct positive effect on intention, which is supported by the results ($\beta = 0.113$, $p < 0.001$). H8 and H9 measured the impacts of our manipulations. We had to reject H8 since we did not see any significant effect of an additional public benefit on intention to use ($\beta = -0.024, p = 0.505$). In contrast, intention to use is higher if governments serve as app providers ($\beta = -0.124$, $p < 0.001$), thus supporting H9.

7. Discussion and theoretical implications

Both perceived personal and perceived public benefit have demonstrated a significant correlation with privacy concerns, implying that privacy concerns might be alleviated with increasing perceived benefits for the individual. By comparison, the perceived benefit for the individual itself has a stronger correlation with privacy concerns. This directly links to previous findings, which have indicated difficulties to activate awareness of the common good factor in the adoption of tracing apps (Matt, 2022; Trang *et al.*, 2020). We also find that trust in the government as a provider of the COVID-19 contact tracing app in the three targeted countries has the strongest correlation with privacy concerns. This finding is in line with other studies that showed a positive relationship between trust in the government and the willingness to download contact tracing apps (Kostka & Habich-Sobiegalla, 2020; Riemer *et al.*, 2020). The perceived transparency of the COVID-19 contact tracing app campaigns is the second-largest factor that can reduce privacy concerns, which emphasizes the importance of clear, correct and accurate information. In addition, campaign transparency also has a positive association with attitude towards future tracking apps, meaning that the information

Table 4. Results of manipulation checks (1a: Self-benefit – government, 1b: Self and public benefit – government, 2a: Self-benefit – private company, 2b: Self and public benefit – private company)

Manipulation		Treatment groups 1a	1b	2a	2b
App provider	Government	269	282	5	10
	Private company	3	2	261	265
	N/A ("I don't know")	6	4	12	5
	Correct perception	97%	98%	94%	95%
Communicated beneficiary	Self-benefit	198	33	204	35
	Self and public benefit	80	255	74	245
	Correct perception	71%	89%	73%	88%

Constructs	Indicators	Outer loadings	Source
Perceived self-benefit	Using the COVID-19 app is good for my well-being	0.830	Kordzadeh and Warren (2017)
CA = 0.858	There are advantages to me from using the COVID-19 app	0.856	
CR = 0.897	Using the COVID-19 app helps me stay healthy	0.736	
AVE = 0.686	The benefits of using the COVID-19 app outweigh the potential risks	0.884	
Perceived public benefit	Using the COVID-19 app helps society	0.937	Kordzadeh and Warren (2017)
CA = 0.933	Using the COVID-19 app is worthless for society (reverse)	0.848	
CR = 0.952	Using the COVID-19 app is valuable to society	0.924	
AVE = 0.833	Using the COVID-19 app is good for society	0.939	
Trust in government	I know that the government is always honest when it comes to using my personal information	0.892	Hong and Thong (2013), Malhotra *et al.* (2004)
CA = 0.925	I know that the government cares about its citizens	0.822	
CR = 0.943	I know that the government is not opportunistic when using my personal information	0.892	
AVE = 0.769	I know that the government is predictable and consistent with regards to using my personal information	0.852	
	I trust the government keeps my best interests in mind when dealing with my personal information	0.923	
Campaign transparency	The information I receive from the official COVID-19 app campaigns by the government fully encompasses what I need to know	0.846	Schnackenberg *et al.* (2020)
CA = 0.931	The information I receive from the official COVID-19 app campaigns by the government covers all the topics I want to know	0.826	
CR = 0.945	The information I receive from the official COVID-19 app campaigns by the government campaigns is clear	0.874	
AVE = 0.742	The information I receive from the official COVID-19 app campaigns by the government is comprehensible	0.855	
	The information I receive from the official COVID-19 app campaigns by the government appears correct	0.886	
	The information I receive from the official COVID-19 app campaigns by the government appears accurate	0.882	
Privacy concerns	I am concerned that the information I submit on the COVID-19 tracing apps could be misused	0.925	Dinev and Hart (2006)
CA = 0.944	I am concerned that a person can find private information about me on the COVID-19 tracing apps	0.945	
CR = 0.960	I am concerned about submitting information on the COVID-19 tracing apps, because of what others might do with it	0.946	
AVE = 0.857	I am concerned about submitting information on the COVID-19 tracing apps, because it could be used in a way I did not foresee	0.887	
Attitude	Using a tracking app is a good/bad idea	0.915	Venkatesh *et al.* (2003)
CA = 0.911	Using a tracking app is a pleasant/unpleasant idea	0.899	
CR = 0.944	I like/dislike the idea of using a tracking app	0.950	
AVE = 0.849			
Intention	I intend to use the tracking app	0.977	Malhotra *et al.* (2004), Venkatesh *et al.* (2003)
CA = 0.977	I predict I will use the tracking app	0.978	
CR = 0.985	I plan to use the tracking app	0.979	
AVE = 0.956			

Table 5. Measurement items and reliability

provided in a campaign also carries a value on influencing user beliefs towards future tracking app technology. We hereby confirm previous results from Walrave, Waeterloos and Ponnet (2020), who used the health belief model to study COVID-19 tracing apps adoption. In line with various prior studies in other domains (e.g. Anderson & Agarwal, 2011; Dinev *et al.*, 2016), we find that privacy concerns negatively affect users' attitudes towards new tracking

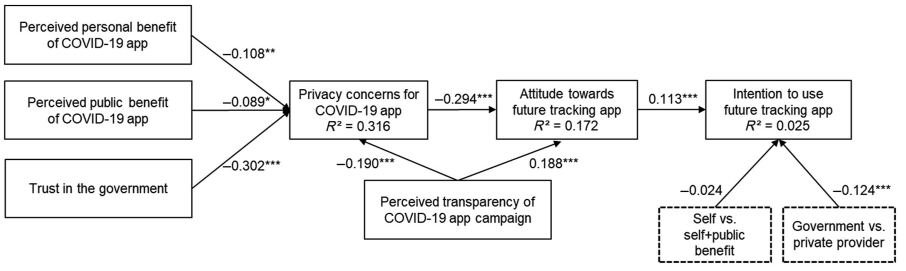
technology. Likewise, numerous studies have confirmed that attitudes are positively associated with behavioral intentions (e.g. Li, 2012; Aloudat *et al.*, 2014; Angst & Agarwal, 2009). Our results also show a positive association of attitude with usage intention of future tracking apps.

Concerning the manipulation variables, we first expected that a benefit for the public in addition to the benefit for the self would lead to a higher intention to use future tracking apps; however, our results did not support this. We know that the nature of benefits that new technologies can have for digitized individuals can be complex and is subject to different roles that individuals take on (Turel, Matt, Trenz, & Cheung, 2020). Trang *et al.* (2020) point out that there are different groups of COVID-19 tracing app users: critics, undecided and advocates. Public benefit appeal appears prominent for the critics and the undecided. It might therefore be due to sample characteristics that we did not find a significant association between perceived public benefit and intention to adopt. Another reason could be the insufficient tangibility of a hypothetical future adoption as it can already be a complex cognitive task to assess the benefits of a new technology for themselves.

Concerning the type of provider of the future tracking app, we know that individuals tend to look for more control over their health data and are more reluctant to disclose when it is used for for-profit research (Anderson & Agarwal, 2011; Willison *et al.*, 2009). In line with this, our results show a positive effect of government involvement, which is in contrast with the findings of Simko *et al.* (2020), who found that participants feel most comfortable when a COVID-19 contact tracing app is provided by Google. However, the same study found participants to be much less comfortable when Apple was the provider. We also like to highlight the possibility that a future tracking app could be provided by a large tech company in combination with a governmental player. However, our results imply that highlighting the government as app provider and emphasizing their privacy-preserving protocols might stimulate use (Fahey & Hino, 2020), although potentially only if the functionality of the app can actually be associated with government tasks.

Constructs	ATT	TRA	INT	PUB	PSB	PC	TRT
Attitude	0.922						
Campaign transp	0.323	0.862					
Intention	0.114	0.016	0.978				
Perc. public benefit	0.388	0.486	0.062	0.913			
Perc. self-benefit	0.422	0.549	0.068	0.790	0.828		
Privacy concerns	−0.380	−0.459	−0.026	−0.386	−0.424	0.926	
Trust in government	0.408	0.551	0.044	0.397	0.468	−0.493	0.877

Table 6.
Discriminant validity



Note(s): *p <= 0.05; **p <= 0.01; ***p <= 0.001

Figure 3.
Structural model

8. Practical implications

Our findings are important for practitioners since they show that trust in governments is an important measure to alleviate privacy concerns for contact tracing apps, and this might not only be relevant for COVID-19 but also for future tracking apps that require users' health and/or location information. Policymakers should consider developing privacy-preserving data usage policies, as well as taking technical precautions that rely on the five main principles: reliability, responsiveness, openness, integrity and fairness (OECD, 2013). Additionally, communication with individuals being clear, consistent, accurate and correct plays a significant role in trust-building. Government officials should therefore keep in mind that privacy perceptions can often be based on beliefs rather than on actual functional-related risks arising from a technology (Becker, Matt, Widjaja, & Hess, 2017).

We have also pointed out the dangers for the future diffusion of a technology that can arise from a government-organized society-wide introduction of a related technology, especially if technology adoption is partially or fully obligatory. Therefore, governments need to take responsibility not only in application design but also in the design of the technology introduction campaigns, as inadequate design may endanger the perception and adoption of the current app and thus, consequently, have a negative effect on the future diffusion or related technologies.

One critical aspect of such campaigns is the focus on the benefits of adoption that are communicated. We have shown that individuals primarily focus on their personal benefits rather than those for society. Therefore, governments need to question whether they seek to increase the communication of individual benefits to obtain higher adoption rates or whether they seek to make the public benefits more comprehensible. While strengthening the awareness of the public benefit may still have only a relatively minor effect on individuals' adoption decisions, it should also be considered that this might still be an important way to improve societal acceptance of such technologies.

9. Conclusion and limitations

Our main goal was to explore whether the current introduction of COVID-19 tracing apps also affects individuals' intention to use future tracking apps. We identify the perceived transparency of the app introduction campaign as the linking element that affects both perceptions of privacy concerns related to the current tracing app, as well as individuals' attitudes towards future tracking technology and can thus restrict the diffusion of a related technology. Trust in the government has been found to be a key element in reducing privacy concerns, and a governmental app that has trust in the population can profit from higher adoption intention than an app from a private firm.

This study has limitations, some of which provide opportunities for future research. First, we conducted the study in three Western countries, Germany, the United Kingdom and Australia, with varying app structures, privacy policies and app introduction campaigns. Moreover, the perceived risk of catching COVID-19 as well as the perceived severity has differed across these countries and over time, in the same way that other risks (e.g. more frequent natural disasters or gun violence) vary across countries. We aggregated participant responses across the three countries and did not find substantial differences in the model specification between the different countries. However, we cannot establish whether we would find similar results for other countries as well, especially those with substantial differences in culture, regulatory frames and other objective risk factors. Furthermore, most of the survey participants were young and the majority reported having completed higher education. We know from previous research that individuals have different preferences on privacy policies as well as different cognitive abilities to process them (Schöning, Matt, & Hess, 2019). Therefore, our sample participants in these

three countries might deviate in their perceptions and responses from individuals with other characteristics.

Second, our treatment scenario was based on a hypothetical mobile tracking application that uses individuals' location and health data, while the context was a safety service in case of emergencies. Needless to say, the particular design of the proposed functionality, applied data protection regulations and also associated providers might have affected the results and might differ from application with other characteristics. For instance, the type of service might also fit better or less with the responsibilities that individuals associate with governmental or private providers. Also, there are many other types of potential private (e.g. large tech companies vs startups) and governmental providers, such as non-governmental organizations, hospitals or other health entities (Anderson & Agarwal, 2011), and combinations thereof that should be addressed in future studies.

References

Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE Security and Privacy*, *3*, 26–33.

Adu, E. K., Mills, A., & Todorova, N. (2017). The digitization of healthcare: Understanding personal health information disclosure by consumers in developing countries – An extended privacy calculus perspective. *ACIS 2017 Proceedings*.

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*, 179–211.

Alashoor, T., Han, S., & Joseph, R. (2017). Familiarity with big data, privacy concerns, and self-disclosure accuracy in social networking websites: An APCO model. *Communications of the Association for Information Systems*, *41*, 62–96, Article 4.

Aloudat, A., Michael, K., Chen, X., & Al-Debei, M. M. (2014). Social acceptance of location-based mobile government services for emergency management. *Telematics and Informatics*, *31*, 153–171.

Altmann, S., Milsom, L., Zillessen, H., Blasone, R., Gerdon, F., Bach, R., … Abeler, J. (2020). Acceptability of app-based contact tracing for COVID-19: Cross-country survey study. *JMIR mHealth and uHealth*, *8*, e19857.

Amnesty International (2020). Bahrain, Kuwait and Norway contact tracing apps among most dangerous for privacy. Available from: https://www.amnesty.org/en/latest/news/2020/06/bahrain-kuwait-norway-contact-tracing-apps-danger-for-privacy/ (accessed 25 June 2020).

Anderson, C. L., & Agarwal, R. (2011). The digitization of healthcare: Boundary risks, emotion, and consumer willingness to disclose personal health information. *Information Systems Research*, *22*, 469–490.

Angst, C., & Agarwal, R. (2009). Adoption of electronic health records in the presence of privacy concerns: The elaboration likelihood model and individual Persuasion. *MIS Quarterly*, *33*, 339–370.

Bansal, G., Zahedi, F., & Gefen, D. (2008). The moderating influence of privacy concern on the efficacy of privacy assurance mechanisms for building trust: A multiple-context investigation.

Bansal, G., Zahedi, F. M., & Gefen, D. (2010). The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision Support Systems*, *49*, 138–150.

Barth, S., & De Jong, M. D. (2017). The privacy paradox–investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Telematics and Informatics*, *34*, 1038–1058.

Becker, M., Matt, C., Widjaja, T., & Hess, T. (2017). Understanding privacy risk perceptions of consumer health wearables–an empirical taxonomy. *Proceedings of the 38th International Conference on Information Systems (ICIS)*, Seoul.

Chen, H., Beaudoin, C. E., & Hong, T. (2017). Securing online privacy: An empirical test on Internet scam victimization, online privacy concerns, and privacy protection behaviors. *Computers in Human Behavior*, *70*, 291–302.

Cheung, M. F. Y., & To, W. M. (2017). The influence of the propensity to trust on mobile users' attitudes toward in-app advertisements: An extension of the theory of planned behavior. *Computers in Human Behavior*, *76*, 102–111.

Chiu, C.-M., Hsu, M.-H., & Wang, E. T. G. (2006). Understanding knowledge sharing in virtual communities: An integration of social capital and social cognitive theories. *Decision Support Systems*, *42*, 1872–1888.

Cho, H., Ippolito, D., & Yu, Y. (2020). Contact tracing mobile apps for COVID-19: Privacy considerations and related trade-offs. arXiv preprint arXiv:2003.11511, 2020.

Ciucci, M., & Gouardères, F. (2020). *National COVID-19 contact tracing apps*. Luxembourg: European Parliament Think Tank.

Clemons, E. K., & Wilson, J. S. (2015). Family preferences concerning online privacy, data mining, and targeted ads: Regulatory implications. *Journal of Management Information Systems*, *32*, 40–70.

Danquah, L. O., Hasham, N., Macfarlane, M., Conteh, F. E., Momoh, F., Tedesco, A. A., … Weiss, H. A. (2019). Use of a mobile application for Ebola contact tracing and monitoring in northern Sierra Leone: A proof-of-concept study. *BMC Infectious Diseases*, *19*, 810.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, *13*, 319–340.

Dhar, S., & Varshney, U. (2011). Challenges and business models for mobile location-based services and advertising. *Communications of the ACM*, *54*, 121–128.

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, *17*, 61–80.

Dinev, T., Mcconnell, A. R., & Smith, H. J. (2015). Research commentary – Informing privacy research through information systems, psychology, and behavioral economics: Thinking outside the "APCO" box. *Information Systems Research*, *26*, 639–655.

Dinev, T., Albano, V., Xu, H., D'atri, A., & Hart, P. (2016). Individuals' attitudes towards electronic health records: A privacy calculus perspective. *Advances in Healthcare Informatics and Analytics*, Springer, Cham, 19–50.

Dwyer, C. (2011). Privacy in the age of Google and Facebook. *IEEE Technology and Society Magazine*, *30*, 58–63.

Edelman. (2021). Edelman trust barometer. Retrieved from https://www.edelman.de/research/edelman-trust-barometer-2021.

Fahey, R. A., & Hino, A. (2020). COVID-19, digital privacy, and the social limits on data-focused public health responses. *International Journal of Information Management*, *55*, 102181.

Ferretti, L., Wymant, C., Kendall, M., Zhao, L., Nurtay, A., Abeler-Dörner, L., … Fraser, C. (2020). Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing. *Science*, *368*, eabb6936.

Hair, J., Hult, G. T. M., Ringle, C., & Sarstedt, M. (2016). *A primer on partial least squares structural equation modeling*. Bingley: SAGE Publications.

Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. *European Business Review*, *31*, 2–24.

Hinch, R., Probert, W., Nurtay, A., Kendall, M., Wymant, C., Hall, M., … Fraser, C. (2020). Effective configurations of a digital contact tracing app: A report to NHSX.

Holmes, O., Mccurry, J., & Safi, M. (2020, June 18). Coronavirus mass surveillance could be here to stay, experts say. *The Guardian*, p. 18.

Hong, W., & Thong, J. Y. L. (2013). Internet privacy concerns: An integrated conceptualization and four empirical studies. *MIS Quarterly*, *37*, 275–298.

Horvath, L., Banducci, S., & James, O. (2020). Citizens' attitudes to contact tracing apps. *Journal of Experimental Political Science*, *9*(1), 1–13.

Hurtz, S. (2020). *Die Corona-App fängt an zu wirken, sobald 15 Prozent mitmachen*. Munich: Süddeutsche Zeitung.

Hvidman, U., & Andersen, S. C. (2016). Perceptions of public and private performance: Evidence from a survey experiment. *Public Administration Review*, *76*, 111–120.

Jafarkarimi, H., Saadatdoost, R., Sim, A. T. H., & Hee, J. M. (2016). Behavioral intention in social networking sites ethical dilemmas: An extended model based on theory of planned behavior. *Computers in Human Behavior*, *62*, 545–561.

Jahari, S. A., Hass, A., Hass, D., & Joseph, M. (2022). Navigating privacy concerns through societal benefits: A case of digital contact tracing applications. *Journal of Consumer Behaviour*, *21*, 625–638.

James, O., & Jilke, S. (2020). Marketization reforms and co-production: Does ownership of service delivery structures and customer language matter? *Public Administration*, *98*, 941–957.

Ketelaar, P. E., & Van Balen, M. (2018). The smartphone as your follower: The role of smartphone literacy in the relation between privacy concerns, attitude and behaviour towards phone-embedded tracking. *Computers in Human Behavior*, *78*, 174–182.

Kock, N. (2015). Common method bias in PLS-SEM: A full collinearity assessment approach. *International Journal of E-Collaboration (IJeC)*, *11*, 1–10.

Kock, N., & Lynn, G. (2012). Lateral collinearity and misleading results in variance-based SEM: An illustration and recommendations. *Journal of the Association of Information Systems*, *13*(7), 546–580.

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour. *Computers and Security*, *64*, 122–134.

Kordzadeh, N., & Warren, J. (2017). Communicating personal health information in virtual health communities: An integration of privacy calculus model and affective commitment. *Journal of the Association for Information Systems*, *18*, 1.

Kostka, G., & Habich-Sobiegalla, S. (2020). In times of crisis: Public perceptions towards COVID-19 contact tracing apps in China, Germany and the US. *New Media & Society*. doi: 10.1177/14614448221083285 (September 16, 2020).

Leins, K., Culnane, C., & Rubinstein, B. I. (2020). Tracking, tracing, trust: Contemplating mitigating the impact of COVID -19 with technological interventions. *Medical Journal of Australia*, *213*, 6.

Li, Y. (2012). Theories in online information privacy research: A critical review and an integrated framework. *Decision Support Systems*, *54*, 471–481.

Li, X., & Chen, X. (2010). Factors affecting privacy disclosure on social network sites: An integrated model. *Proceedings of the 2010 International Conference on Multimedia Information Networking and Security*, 4-6 November 2010. 315–319.

Li, T., Cobb, C., Jackie, Y., Baviskar, S., Agarwal, Y., Li, B., ... Hong, J. (2020). What makes people install a COVID-19 contact-tracing app?. *Understanding the influence of app design and individual difference on contact-tracing app adoption intention*.

Liu, C., Marchewka, J. T., Lu, J., & Yu, C.-S. (2004). Beyond concern: A privacy–trust–behavioral intention model of electronic commerce. *Information and Management*, *42*, 127–142.

Lucivero, F., Hallowell, N., Johnson, S., Prainsack, B., Samuel, G., & Sharon, T. (2020). COVID-19 and contact tracing apps: Ethical challenges for a social experiment on a global scale. *Journal of Bioethical Inquiry*, *17*, 835–839.

Mackenzie, S. B., Podsakoff, P. M., & Podsakoff, N. P. (2011). Construct measurement and validation procedures in MIS and behavioral research: Integrating new and existing techniques. *MIS Quarterly*, *35*, 293–334.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, *15*, 336–355.

Matt, C. (2022). Campaigning for the greater good? – How persuasive messages affect the evaluation of contact tracing apps. *Journal of Decision Systems*, *31*, 189–206.

Meulendijk, M., Meulendijks, E., Jansen, P., Numans, M., & Spruit, M. (2014). What concerns users of medical apps? Exploring non-functional requirements of medical mobile applications. *Proceedings of the 22nd European Conference on Information Systems (ECIS 2014)*, Tel Aviv.

Naous, D., Bonner, M., Humbert, M., & Legner, C. (2022). Learning from the past to improve the future. *Business and Information Systems Engineering*, 1–18.

Newton, K. (2020). Government communications, political trust and compliant social behaviour: The politics of covid-19 in Britain. *The Political Quarterly*, *91*, 502–513.

OECD (2013). Trust in government, policy effectiveness and the governance agenda. Government at a Glance.

O'neill, P. H., Ryan-Mosley, T., & Johnson, B. (2020). A flood of coronavirus apps are tracking us. Now it's time to keep track of them. *MIT Technology Review*.

Palanisamy, R. (2014). The impact of privacy concerns on trust, attitude and intention of using a search engine: An empirical analysis. *International Journal of Electronic Business*, *11*, 274–296.

Paul, C., Scheibe, K., & Nilakanta, S. (2020). Privacy concerns regarding wearable IoT devices: How it is influenced by GDPR?. *Proceedings of the 53rd Hawaii International Conference on System Sciences*, Maui, HI.

Raskar, R., Nadeau, G., Werner, J., Barbar, R., Mehra, A., Harp, G., … Louisy, K. (2020). COVID-19 contact-tracing mobile apps: Evaluation and assessment for decision makers. arXiv preprint arXiv:2006.05812.

Redmiles, E. M. (2021). User concerns 8 tradeoffs in technology-facilitated COVID-19 response. *Digital Government: Research and Practice*, *2*, 1–12.

Reith, R., Buck, C., Lis, B., & Eymann, T. (2020). Tracking fitness or sickness -combining technology acceptance and privacy research to investigate the actual adoption of fitness trackers. *Proceedings of the 53rd Hawaii International Conference on System Science 2020, University of Hawaii* (pp. 3538–3547).

Reith, R., Buck, C., Walther, D., Lis, B., & Eymann, T. (2019). How privacy affects the acceptance of mobile payment solutions. *Proceedings of the Twenty-Seventh European Conference on Information Systems (ECIS2019)*, Stockholm and Uppsala.

Riemer, K., Ciriello, R., Peter, S., & Schlagwein, D. (2020). Digital contact-tracing adoption in the COVID-19 pandemic: IT governance for collective action at the societal level. *European Journal of Information Systems*, *29*, 731–745.

Rowe, F., Ngwenyama, O., & Richet, J.-L. (2020). Contact-tracing apps and alienation in the age of COVID-19. *European Journal of Information Systems*, *29*, 545–562.

Sacco, M., Christou, T., & Bana, A. (2020). Digital contact tracing for the COVID-19 epidemic: A business and human rights perspective. *SSRN Electronic Journal*.

Schnackenberg, A. K., Tomlinson, E., & Coen, C. (2020). The dimensional structure of transparency: A construct validation of transparency as disclosure, clarity, and accuracy in organizations. *Human Relations*, *74*(10). doi: 10.1177/0018726720933317.

Schöning, C., Matt, C., & Hess, T. (2019). Personalised nudging for more data disclosure? On the adaption of data usage policies format to cognitive styles. *Proceedings of the 52nd Hawaii International Conference on System Sciences (HICSS)*, Maui. 4395–4404.

Sharma, S., Singh, G., Sharma, R., Jones, P., Kraus, S., & Dwivedi, Y. K. (2020). Digital health innovation: Exploring adoption of COVID-19 digital contact tracing apps. *IEEE Transactions on Engineering Management*, 1–17.

Simko, L., Calo, R., Roesner, F., & Kohno, T. (2020). COVID-19 contact tracing and privacy: Studying opinion and preferences. arXiv preprint arXiv:2005.06056.

Smith, H., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly*, *35*, 989–1015.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly*, *20*, 167–196.

Tavakol, M., & Dennick, R. (2011). Making sense of Cronbach's alpha. *International Journal of Medical Education*, *2*, 53–55.

The Bogota Post (2020). Tracking coronavirus: Should you install the CoronApp? Available from: https://thebogotapost.com/tracking-coronavirus-coronapp/46864/ (accessed 27 June 2020).

Trang, S., Trenz, M., Weiger, W., Tarafdar, M., & Cheung, C. (2020). One app to trace them all? Examining app specifications for mass acceptance of contact-tracing apps. *European Journal of Information Systems*, *29*(4), 415–428.

Turel, O., Matt, C., Trenz, M., & Cheung, C. M. K. (2020). An intertwined perspective on technology and digitised individuals: Linkages, needs and outcomes. *Information Systems Journal*, *30*, 929–939.

Udesky, J. O., Boronow, K. E., Brown, P., Perovich, L. J., & Brody, J. G. (2020). Perceived risks, benefits, and interest in participating in environmental health studies that share personal exposure data: A U.S. survey of prospective participants. *Journal of Empirical Research on Human Research Ethics*, *15*, 425–442.

Urbaczewski, A., & Lee, Y. J. (2020). Information technology and the pandemic: A preliminary multinational analysis of the impact of mobile tracking technology on the COVID-19 contagion control. *European Journal of Information Systems*, *29*, 405–414.

Van Dorp, K. J. (2002). Tracking and tracing: A structure for development and contemporary practices. *Logistics Information Management*, *15*(1), 24–33.

Venkatesh, V., Morris, M., Davis, G., & Davis, F. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, *27*, 425–478.

Venkatesh, V., Thong, J. Y. L., & Xu, X. (2012). Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology. *MIS Quarterly*, *36*, 157–178.

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

Willison, D. J., Steeves, V., Charles, C., Schwartz, L., Ranford, J., Agarwal, G., … Thabane, L. (2009). Consent for use of personal information for health research: Do people with potentially stigmatizing health conditions and the general public differ in their opinions? *BMC Medical Ethics*, *10*, 10.

Wilson, D., & Valacich, J. S. (2012). Unpacking the privacy paradox: Irrational decision-making within the privacy calculus. *Proceedings of the 33rd International Conference on Information Systems 2012*, Orlando, FL.

Xu, Z. (2019). An empirical study of patients' privacy concerns for health informatics as a service. *Technological Forecasting and Social Change*, *143*, 297–306.

Xu, H., Teo, H.-H., Tan, B. C. Y., & Agarwal, R. (2009). The role of push-pull technology in privacy calculus: The case of location-based services. *Journal of Management Information Systems*, *26*, 135–174.

Xu, H., Gupta, S., Rosson, M. B., & Carroll, J. M. (2012). Measuring mobile users' concerns for information privacy. *Proceedings of the 2012 International Conference on Information Systems*, Orlando, FL.

Yun, H., Lee, G., & Kim, D. J. (2019). A chronological review of empirical research on personal information privacy concerns: An analysis of contexts and research constructs. *Information and Management*, *56*, 570–601.

Zhang, X., Liu, S., Chen, X., Wang, L., Gao, B., & Zhu, Q. (2018). Health information privacy concerns, antecedents, and information disclosure intention in online health communities. *Information and Management*, *55*, 482–493.

Zhong, R. (2020, May 26). China's virus apps may outlast the outbreak, stirring privacy fears. *The New York Times*, p. 26.

Zimmermann, B. M., Fiske, A., Prainsack, B., Hangel, N., Mclennan, S., & Buyx, A. (2021). Early perceptions of COVID-19 contact tracing apps in German-speaking countries: Comparative mixed methods study. *Journal of Medical Internet Research*, *23*, e25525.

About the authors

Christian Matt is a Professor and Co-director of the Institute of Information Systems at the University of Bern, Switzerland. He holds a PhD in Management from Ludwig-Maximilians-Universität (LMU), Munich, Germany, and was a visiting scholar at the National University of Singapore and the Wharton School of the University of Pennsylvania, among others. His current research focuses on digital transformation and value creation, hybrid intelligence and data-based services. His research has been published in the *European Journal of Information Systems, Journal of Management Information Systems, Information Systems Journal, Electronic Markets, Business and Information Systems Engineering, MIS Quarterly Executive*, and several others. Christian Matt is the corresponding author and can be contacted at: christian.matt@iwi.unibe.ch

Mena Teebken is a PhD candidate and research assistant at the Institute for Digital Management and New Media at LMU Munich. Her doctoral thesis addresses privacy perceptions in digital workplaces from an individual and organizational perspective. Before joining LMU Munich, she received her Master of Science degree from the University of Mannheim. Her research has been published in Proceedings of the Americas Conference on Information Systems and the Hawaii International Conference on System Sciences, amongst others.

Beril Özcan works as a "Voice of the Customer" Specialist for a large software company, where she focuses on customer experience management. Earlier she was a student researcher at the Institute for Digital Management and New Media at LMU Munich, where she received her Master of Science degree.