6-18-2022

Privacy Vs. Health: The Role of Privacy Trade-offs in the Adoption of Public Health Applications

Amina Egal
University of Lausanne, amina.egal@unil.ch

Dana Naous
University of Lausanne, dana.naous@unil.ch

PRIVACY VS. HEALTH: THE ROLE OF PRIVACY TRADE-OFFS IN THE ADOPTION OF PUBLIC HEALTH APPLICATIONS

Research Paper

Amina Egal, University of Lausanne, Lausanne, Switzerland, amina.egal@unil.ch

Dana Naous, University of Lausanne, Lausanne, Switzerland, dana.naous@unil.ch

Abstract

Innovations in healthcare technology aim to address challenges in health outcomes. COVID-19 contact tracing apps were introduced in various countries as an innovative health solution to stop the spread of the virus. Although aiming for the greater good of the population through maintaining public health, the introduction of these apps was accompanied by controversial debates about their privacy implications leading to low adoption worldwide. In fact, digital contact tracing raised privacy concerns associated to information sharing within the app, which impacts intention to use. However, in the question of health versus privacy several factors come into consideration. We apply a privacy calculus approach to study users' intention to use COVID-19 apps under privacy trade-offs. Based on representative samples from Germany and Switzerland, we find that individual safety outweighs societal safety benefit, trust is crucial for mitigating risk perceptions, and social norm has a great impact on individual's intentions to use.

Keywords: IS Adoption, Privacy Calculus, Tradeoffs, Public Health, COVID-19, Social Norms.

1 Introduction

Healthcare is an integral part of society and is, therefore, interlaced in different segments including the private sector, government, and civil society. The interactions among the different actors in healthcare systems can make communication and information flow complex and expensive. Between 2016 and 2020, several European countries were among the top ranked for healthcare spending per capita (OECD, 2021). The efficient coordination of information across the society can have significant implications on health outcomes by reducing the transmission of disease, particularly during epidemics or pandemics. Innovations in healthcare technology are proliferating to address the challenges around health expenditure and health outcomes. Information technology has facilitated the flow of information in and across healthcare systems and is an important innovative dimension of healthcare delivery models.

Mobile health applications, for example, have been cited as among the five most disruptive types of innovations in healthcare (Sounderajah et al., 2021). Although direct-to-consumer innovations in healthcare systems are not particularly new, and neither are the patient consumer's active involvement and responsibility for self-tracking their health (e.g., weight tracking, drug reactions or menstrual cycles), the choice of data to be digitally shared and analyzed for private and public gain is a growing concept over the past two decades (Harris et al., 2010). It is also one that climaxed during the COVID-19 pandemic. Under normal conditions, innovative ideas should be implemented and introduced to market after several evidence-based research studies and demonstrated safety to patients, providers, and consumers (Palanica and Fossat, 2020). However, the pace of innovation changed radically during COVID-19 in the race to save lives, allowing for the period itself to serve as a testing bed in hindsight. The attributes of an individual's decision-making, what is perceived as a benefit and as a risk, can play

a critical role in the diffusion of novel technologies in the public health sector and can be delved into with the contact tracing application (Harris et al., 2010).

Contact tracing is considered a key control measure for containing infectious diseases. The World Health Organization (WHO) defines contact tracing as "the process of identifying, assessing, and managing people who have been exposed to a disease to prevent onward transmission" (WHO, 2018, p. 2). In the case of the worldwide pandemic of COVID-19, contact tracing is needed to identify individuals who may have been exposed and follows up with them daily for a period of at least 14 days from the last point of exposure (Legendre et al., 2020). The fact that symptoms onset may occur days after infection makes it difficult for traditional approaches to map the network of potential exposure traces. Therefore, advanced techniques that rely on digital technologies are required for effective contact tracing in the COVID-19 context. Contact tracing apps (COVID-19 apps) are mobile applications designed to keep a trace of close contacts through proximity or location tracking (Legendre et al., 2020). These digital solutions alert individuals of the need to self-isolate in case of contact with an infected person depending on the type and severity of the exposure. National apps have been developed in various countries, among them TraceTogether (Singapore), SwissCOVID (Switzerland), TousAntiCOVID (France), and Corona-Warn-App (Germany). However, their introduction has been accompanied by controversial debates about their privacy implications (Cho et al., 2020; Redmiles, 2020) and they did not reach the critical mass adoption desired for their effectiveness (Rowe, 2020).

Although privacy can act as impediment to adoption, Acquisti and Grossklags (2004) explain that users' attitudes can be contradictory with their behaviors, resulting with a privacy paradox phenomenon. Barth and de Jong (2017) discuss that users are willing to compromise their privacy based on their assessment of the cost-benefit trade-offs, in what we call privacy paradox. As such, they are willing to use or disclose information in return of an expected benefit, which can be critical in this situation of COVID-19 apps (as one class of public health apps) for fighting the pandemic. Altmann et al. (2020) found that cybersecurity, privacy, and lack of government trust were main barriers to adoption. However, Guillon and Kergall (2020) found that stressing the individual risk in case of infection and the benefits of quarantine would increase adoption. Also, Trang et al. (2020) found that the societal benefit component helped in COVID-19 app adoption. Von Wyl et al. (2020) emphasize that it is vital to study under what circumstances individuals disclose or withhold their data for increasing the adoption of COVID-19 apps. In that regards, we aim to study the following question: *How do privacy trade-offs and social norm affect the mass adoption of public health apps?*

We build on the large body of research in the information systems (IS) literature that has studied information privacy (Belanger and Crossler, 2011; Smith et al., 2011; Xu et al., 2011) as well as studies on contact tracing apps while using the privacy calculus paradigm (Dinev and Hart, 2006) and introducing collective constructs such as epidemiological insights and social norms. Based on that, we investigate user's intention to use COVID-19 contact tracing apps as trade-off analysis between expected benefits and perceived privacy risks. Our results confirm that risk perceptions are barriers to COVID-19 app use. However, the empirical analysis of data collected from two representative samples in Germany (n = 1,022) and Switzerland (n = 1,006) reveals that individual safety benefits are important in the decision to use the COVID-19 app and that epidemiological insights are drivers for app use. In addition, the results emphasize the role of social norm as collective measure for successful adoption of COVID-19 apps.

The remaining of this paper is structured as follows: First we provide a background on COVID-19 contact tracing apps and the privacy related aspect. Next, we present the research model and hypotheses based on privacy calculus. We then discuss the research settings and results. Finally, we discuss our findings along the tested hypotheses and a hindsight review.

2 Background: COVID-19 Apps and the Privacy Dilemma

Mobile technology enables easier and faster contact tracing versus traditional methods and has evolved into one of the key instruments to fight this worldwide pandemic of COVID-19. In fact, during the first

outbreak, simulations confirmed that if approximately 60% of the population use the requisite country app, governments would have the potential to stop the epidemic and keep countries out of lockdown (University of Oxford, 2020). Similarly, Ferretti et al. (2020) estimated that a 1% increase in app adoption would lead to a case reduction of 0.8% to 2.3%. Therefore, governments and health authorities over the world promoted mobile applications that enable digital contract tracing to continuously track user's proximity and to notify them in the event of possible COVID-19 exposure for self-isolation (Legendre et al., 2020). Common tracing mechanisms rely on smartphone's absolute location (in the case of location-based contact tracing) or relative location (in the case of proximity-based contact tracing) to other smartphones (Legendre et al., 2020). Proximity-based contact tracing was adopted in most countries, it relies on proximity detection via Bluetooth Low Energy (BLE) to infer the relative proximity of smartphones (up to 50m outdoors and 25m in- doors).

COVID19 apps require active information disclosure and sharing of sensitive data. Users might share personal information, health information, contact information and possibly location information on the app, which results in privacy concerns. Sharing contact information can result in identification of users through their social graphs (Legendre et al., 2020). Moreover, sharing location information on the app can result in identification of mobility patterns that can serve as diagnostic representation of sensitive demographic information such as religious or political affiliation (Gambs et al., 2011). As for health information, infected users might be particularly concerned in this case since they share their health status information on the app to facilitate exposure notification. Fears arise around state surveillance acts, similar to South Korea (Klatt, 2020), showing the movement of COVID-19 patients and then used to track the general population at a later stage. For this reason, governments around the world have been continuously evaluating and enhancing the different implementation options of COVID-19 contact tracing apps. The main purpose is to have applications that are privacy-preserving and do not reveal any Personally Identifiable Information (PII) about their users (Ahmed et al., 2020), which can put them at risk of being tracked or under government surveillance. This in turn aims at fostering the adoption of the apps and reaching a critical mass.

Studies addressing the user's perspective on COVID-19 apps adoption (Trang et al., 2020; Walrave et al., 2020; Redmiles, 2020; Rowe, 2020) highlight the existing user privacy concerns associated with using COVID-19 apps and the lack of clear benefit conceptualization. While public health technologies are designed for the good of the general population, it is important to understand individual's motivations and barriers for adopting these technologies. Laufer and Wolfe (1977) were among the first to explore how individual decisions around privacy are formed in everyday life and the multi-dimensional structure of privacy as a societal construct. They highlight three dimensions of the privacy calculus - self, environment and interpersonal. The self dimension refers to the individual (benefits and risks), the environment dimension includes the social arrangements and social norm around privacy in a situation and the interpersonal dimension refers to an individual's concepts of privacy rights and rules as reflected by the environmental dimension. The balancing of normative or societal interests and individual interests is the basis for privacy. The adopted and adapted Privacy Calculus Model in IS literature suggests that self-disclosure intentions are a function of a rational calculus of benefits and costs of privacy behaviors. Individuals choose to "surrender a degree of privacy" for outcomes that are worth the risk of information disclosure (Dinev and Hart, 2006; Jiang et al., 2013).

3 Research Model

The privacy calculus model provides a conceptual framework to analyse the trade-off individuals face in terms of weighing up potentially harmful risks versus expected benefits when deciding whether to withhold or disclose personal information (Dinev and Hart, 2006). It therefore allows explaining the adoption of COVID-19 apps as one category of mobile health application. The privacy calculus has received attention within the healthcare context, in terms of explaining this risk-benefit trade-off process in the intention to adopt and use mobile health technology (Anderson and Agarwal, 2011; Zhang et al., 2018; Rahman, 2019). Applied to COVID-19 apps, the privacy calculus lens allows studying

user's intentions to use as trade-off analysis between perceived risks and benefits taking into consideration other influencing factors including trust, control and social norms (Figure 1).

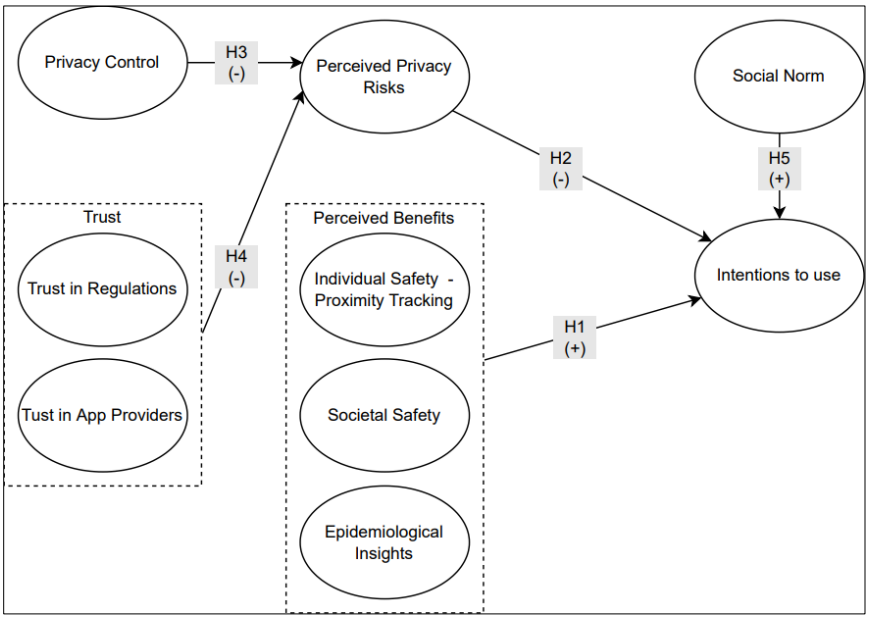

Figure 1. Privacy Calculus Model

3.1 Perceived Benefits

Trang et al. (2020) discuss two types of benefits for COVID-19 apps; related to self and society. We suggest taking a broader public health perspective that integrates a hedonic benefit of epidemiological insights for a country-wide monitoring of COVID-19 cases. Based on three levels characterized mainly by safety considerations, we define our benefit constructs. First, individual safety benefits related to receiving exposure notifications on possible encounters with an infected person through proximity tracking. Second, societal safety benefits whereby the user is able to notify recent contacts in case he or she tests positive for COVID-19, thus protecting family, friends, and general public from infection. Third, the benefit of generating epidemiological insights via the usage of the COVID19 app. This is key in improving the quality of reporting on COVID-19 and performing research on specific patterns in the population that can help in curbing the spread of the virus. For all the perceived benefits, we hypothesize that:

H1: Perceived benefits are positively associated to intentions to use COVID-19 apps.

3.2 Perceived Privacy Risks

An upper barrier to the uptake of COVID-19 apps is due to concerns about the app usage by other citizens and purposes followed by authorities deploying them (Gupta and De Gasperis, 2020). For instance, the Norwegian government and Norwegian app provider Smittestopp had to heed to a temporary ban of the app from the Norwegian Data Protection Authority (NDPA) and have had the app removed due to users' privacy concerns raised. Privacy concerns and perceived privacy risks are generally considered to negatively affect disclosure behavior and are typically used in IS studies to evaluate the cost dimension when employing a privacy calculus model (Dinev and Hart, 2006). Concerns for Information Privacy (CFIP) framework by Smith et al. (1996) focuses on four areas related to online information disclosure: the collection of private data by app providers, unauthorized secondary use of data, improper access, and errors. In the case of COVID-19 apps, users share different information types when using the app, which can be considered a risky behavior. Users' concerns in

that regards revolve around the first two areas corresponding to misuse of the information by app providers and identifying personal aspects as social graphs and mobility patterns (Legendre et al., 2020). Perceived privacy risks are defined as an individual's perception of privacy loss and invasion, whereas privacy concerns (Malhotra et al., 2004) can be described as antecedents to risk beliefs, reflecting users expectation of losses due to information disclosure. These concerns formulate the individual's risk perceptions. We, therefore, base our model on the perceived privacy risk construct as adoption barrier (Krasnova et al., 2010; Naous et al., 2019). We hypothesize that:

H2: Perceived privacy risks are negatively associated to intentions to use COVID-19 apps.

3.3 Perceived Privacy Control

Privacy controls can help mitigate perceived privacy risks if the user has more control over their data sharing (Malhotra et al., 2004). Control on the data sharing on COVID-19 apps concerns both extent (how much personal data is being shared, when and where, and for what period of time) and type of information shared (Ahmed et al., 2020; Trang et al., 2020). In the context of COVID-19 apps implementation, privacy control can be achieved by the application architecture (centralized vs. decentralized) (Legnedre et al., 2020) and the privacy settings implemented within the app. Firstly, it is achieved by the mode of data communication on the app. Anonymous communication of data can guarantee privacy for users, therefore it should be a definite aspect in COVID-19 apps. In addition, permissions, and user consent on sharing any type of information and who can access this information are two important aspects for ensuring control. Hence, we propose the following hypothesis:

H3: Privacy control is negatively associated to perceived privacy risks.

3.4 Perceived Trust

The general population's trust is a central element when population-wide adoption is needed, as is the case with the adoption of COVID-19 apps (Riemer et al., 2020). Trust is key for voluntary utilization, especially in places where it is hard to enforce top-down the use of contact tracing apps (e.g., well-functioning democracies) (Gupta and De Gasperis, 2020). We build on Dinev and Hart's (2006) definition of trust as an individual's belief that a counter-party involved in an interaction has characteristics that prevent them from opportunistic behavior. We study two trust constructs, which relate to the user's perceived risks: trust in app providers based on treatment of data and trust in government based on regulations. Individual risk perceptions are correlated with the user perception of the app provider, typically the national health institutions, on data treatment and the transparency of the underlying intended use of information collected. In line with Krasnova et al. (2010) we argue that user's perception of the app provider's benevolence and integrity affects the choice of disclosure via contact tracing apps. Based on the trustworthiness, honesty and transparency of app providers, users will have lower risk perceptions related to information disclosure on the app.

Legislative and regulatory efforts for implementing objective information practices have an impact on individual disclosure behavior (Yang et al., 2018). The central tenet being that if regulatory systems promote a safe environment in which service providers have limitations and constraints in exploiting users' personal information and against unauthorized use, users can be comfortable in sharing their information. This privacy assurance role implemented through governmental regulation can be viewed as justice perceptions that enable self-disclosure. Applying justice theory, Xu et al. (2009) refer to procedural justice as an explanation for the perceived fairness of procedures regarding the collection and use of data. Their model portrayed government regulations as mitigation to perceived privacy risks by ensuring respectful treatment of personal information. We argue that trust in government regulations reduces risk perceptions for information disclosure on COVID-19 apps that are normally developed by the authorities and should typically follow regulations that protect user privacy. We hypothesize that:

H4: Trust is negatively correlated to the perceived privacy risks.

3.5 Social Norm

Several disciplines have investigated how innovations are adopted through populations of individuals, households, and larger units of analysis. A sociologist's viewpoint is that innovation diffusion or adoption is galvanized by "social contagion", which is when an individual's adoption behavior is a function of their exposure to other actors' knowledge, attitude or behavior towards the innovation (DiMaggio and Powell, 1983). Studies have offered various causal mechanisms of the social influence, including attributions to information transfer and normative pressures. We focus mainly on the social norm that is attributed to normative pressures, where individuals experience dissonance and feel discomfort when their peers have adopted an innovation, but they have not (Davis et al., 1989; DiMaggio and Powell, 1983). This is especially in the context where their participation can save lives of others and contribute to the greater benefits of the population. In the context of IS adoption, social norm corresponds to whether or not an individual is compelled to use an app simply because everybody else seems to be using it (Min and Kim, 2015) and more so than everybody else, people place importance on the individual user including influencers. For COVID-19 apps, collective action is required at the societal level for effective app use (Riemer et al. 2020). Our study item focuses on the normative pressures of peer adoption. We believe that there exists a social influence on the individual for using such apps. Individuals might be willing to use the app if their social circle uses it, and if using the app is well promoted in the society by influential people and companies as a protective measure against COVID-19. Based on these arguments, we hypothesize:

H5: Social norm is positively correlated to intentions to use contact tracing apps.

3.6 Control Variables

In addition to demographic factors that have been used in other studies on information disclosure (Sun et al., 2015; Naous et al., 2019) such as age and gender, we include previous privacy experience as a control variable for privacy consciousness as suggested by Xu et al. (2009). The item examines whether users are aware of past privacy breaches or invasions, and if it affects the perceived personal risks. We also check experience with mobile apps including social networking and location-based services to understand the previous user behavior. Social networking apps, which rely on a user's peers to be used effectively, allowed us to examine user behavior in the context of social norm.

4 Research Approach

4.1 Research Settings

A barrier to the adoption of the COVID-19 app is the data privacy implications it may have. For our study, we selected two countries where citizens place high value on informational privacy: Switzerland and Germany. In fact, Bellman et al. (2004) investigated the effect the Hofstede scale has on informational privacy and found that four Hofstede cultural dimensions - power distance, individivualism, masculinity and uncertainty avoidance - had a positive effect on informational privacy. Germany and Switzerland are in the same category of countries showing similar cultural values under the Hofstede scale, and with higher concerns for privacy. Surprisingly, Germany and Switzerland also had high adoption of the COVID-19 contact tracing apps compared to other countries in Europe with more than 20% adoption rate directly after the release of the first app version. Thus, we investigate our research question in a context of high cultural value on informational privacy.

Germany and Switzerland followed the decentralized approach relying on Google and Apple Exposure Notifications Application Programming Interface (API). The SwissCOVID pioneered the use of decentralized digital privacy-preserving proximity tracing (D3-PT) protocols that store only contact data on the phone, thus protecting the privacy of the user (Legendre et al., 2020). The Corona-warn-app was launched in Germany on June 16, 2020 and was downloaded 6.4 million times on that same day.

In the third quarter of 2020, Germany's Corona-Warn-App had over 21.9 million users (over 25% of the population) (BMG, 2020), and Switzerland's SwissCOVID app reached 1.8 million users (21% of the population) (FOPH, 2020). By mid-June 2021, the SwissCOVID app had been downloaded 3.1 million times corresponding to 36% of the population assuming a single download per person and Switzerland had 983 exposure triggers per 100,000 people. By comparison, the "Corona-Warn-App" was downloaded 28.3 million times corresponding to 34% of the German inhabitants and Germany had 900 exposure triggers per 100,000 inhabitants (Daniore et al., 2021). The number of downloads had steadily reached 25.8 million download on February 25th, 2021 and 43.15 million on February 24th, 2022. On March 6th, 2022, the SwissCOVID app had been downloaded 3.795 million times, however the number of active users was 1.53 million.

To understand users' perceptions on COVID-19 apps, we conducted an online survey with two representative samples from Germany (n = 1,022) and Switzerland (n = 1,006) in June 2020, after the launch of Corona-Warn-App and SwissCOVID app in Germany and Switzerland respectively. During this post-launch period, the adoption has relatively flattened since, we thereby assume that the answers are still representative of the populations' perceptions. Participants were recruited from a commercial online panel via mailings and web advertisements. The respondents were smartphone owners and existing or potential COVID-19 app users. We only included respondents who have at least heard about the country specific app and have a minimum knowledge about its functionalities. Our questionnaire comprised two parts: Part 1 comprised questions pertaining to demographics (age, gender, residence) and questions related to smartphone apps usage. Part 2 involved questions on users' perceptions of benefits and risks associated to contact tracing app use, opinions concerning usage and sharing of information via the app, opinions related to COVID-19 app providers and regulations in country of residence, and questions related to potential misuse of data. All the questions were translated to the local languages, i.e., German (for Germany) and German, French, and Italian (for Switzerland). The study setup was examined by the Ethics Committee within our academic context to guarantee anonymous participation and data confidentiality.

4.2 Measures

To operationalize the model constructs, we mainly relied on pre-tested and valid scales from prior studies where possible and developed scales for new constructs (cf. Appendix B). All items are studied through a seven-point Likert scale ranging from strongly disagree (1) to strongly agree (7). The perceived risk construct was adapted from Xu et al. (2009). For risk antecedents, privacy control items relied on scales from the study of Krasnova et al. (2010) on social networks, as well as the trust in app providers. The second trust construct, i.e., government regulations, was based on items from Xu et al. (2009). In addition, we adapted the social norm construct from the study of Min and Kim (2015) on social networks. The self-developed items aimed to measure user's perceived benefits on specific scenarios of contact tracing as well as the different contexts. We performed a pre-test survey with five users to test content validity of the new items; they resulted with satisfactory inter-item correlations.

4.3 Sample Background

Demographic information about both samples is presented in Table 1. The average age of participants was 46 years for Germany and 44 years for Switzerland, with 49.8% and 50.5% females respectively. In terms of educational background, the majority had vocational training or equivalent (60.4% Germany, 57.2% Switzerland), and around one third held a university degree or equivalent (32.7% Germany, 36.3 % Switzerland). Majority of respondents are employed, 46.9% in Germany and 47.2% in Switzerland had full-time jobs, 28.5% and 22.8% had part-time jobs respectively. The respondents in both samples use a number of context-aware services including navigation apps (67.8% Germany, 71.3% Switzerland) and social networking apps (75.3% Germany, 77.4% Switzerland). In addition, both samples are familiar with mobile apps for health and fitness tracking, with Switzerland having higher adoption (31.6% Germany, 39.1% Switzerland). Regarding their opinion on COVID19 apps, it

is noteworthy that 36.2% from the German population and 37.7% from the Swiss population think that the app should be mandatory, 22.1% and 18.3% are indifferent about that topic respectively. While both the Corona-Warn-App and SwissCOVID are voluntary, this raises questions on whether it should be enforced for taking the necessary measures in fighting COVID-19 with the increased number of cases and the ease of lockdown measures.

Variable	**Level**	**% Germany**	**% Switzerland**
Gender	Male	50.20	49.50
	Female	49.80	50.50
Age	18-25	12.00	12.20
	26-35	17.90	19.60
	36-45	16.20	19.60
	46-55	21.80	21.60
	56-65	18.80	17.60
	66-75	13.30	9.40
Privacy Consciousness	Not informed	44.50	40.90
	Well informed	55.50	59.10

Table 1. Demographic and background information on survey participants

5 Results

To test our research model, we perform a partial least squares (PLS) analysis for structural equation modelling (SEM). PLS analysis is typically used in privacy calculus studies and is well suited for dealing with a mixed model of reflective and formative constructs such as in our model (Naous et al., 2019). It can estimate both measurement and structural models simultaneously and systematically (Hair et al., 2011). To run the simulations, we used SmartPLS3 v3.3.2 as an analysis tool.

5.1 Measrement Model

We measure the first-order perceived constructs reflectively, while the privacy risk construct formatively. Composite Reliability (CR) and average variance extracted (AVE) were used as indicators of construct reliability (Fornell and Larcker, 1981). The CR values for all the constructs were greater than 0.7 and the AVEs greater than 0.4, showing that all our reflective constructs are reliable (cf. Appendix A). Regarding the formative constructs, we check variance inflation factors (VIFs) to assess common method bias. Based on Kock (2015), "if all VIFs resulting from a full collinearity test are equal to or lower than 3.3, the model can be considered free of common method bias". Our results showed VIFs for the formative constructs less than 3.3, thus common method bias is not of concern in our study.

5.2 Hypothesis Testing

Results from our model (Table 2) show positive and significant correlations for individual benefits of proximity tracking in relation to intention to use for both samples. Positive and significant correlations are also shown for the epidemiological benefits and intention to use the respective COVID-19 app. Although the benefits for self and society should be reciprocal, our analysis shows different results. Unexpectedly, we did not find significant correlations between societal safety benefit and intention to use for both samples. This emphasizes the importance of the app for self-protection rather than informing others. In addition, the societal safety benefit requires that users share their health status on the app, which might create concerns for users. Another interesting finding is the significantly positive correlation between epidemiological insights and intention to use. This draws attention to the motivation of users to contribute their data to research to improve our understanding and knowledge about the pandemic and the spread of the virus within the population. Based on that, in terms of

perceived benefits, H1(a) and (c) are supported. Perceived privacy risk negatively correlates to intention to use and is significant, supporting H2. Perceived control negatively correlates to perceived risk and is only significant for Germany, thus supporting H3 for the German population. The relationship between the trust items in both app providers and regulations is significantly negative to perceived privacy risk, supporting H4, with higher significance for Switzerland when it comes to the app providers and Germany for regulations. It seems that trust in the authorities is key for mitigating the risk perception, especially in Switzerland where the authorities had the first initiative for building a decentralized app that preserves users' privacy with the DP-3T framework. Finally, for social norm, we observe significant positive correlations with intention to use, supporting H5 for both countries.

		Germany		**Switzerland**	
	Construct A → Construct B	**Coefficients**	**P-values**	**Coefficients**	**P-values**
H1	(a) Benefit Individual Safety → Intention to Use	0.132	0.000***	0.132	0.000***
	(b) Benefit Societal Safety → Intention to Use	0.049	0.116	0.043	0.197
	(c) Benefit Epidemiological Insights → Intention to Use	0.133	0.000***	0.123	0.001**
H2	Perceived Privacy Risk → Intention to Use	-0.271	0.000***	-0.247	0.000***
H3	Privacy Control → Perceived Privacy Risk	-0.124	0.019*	-0.006	0.901
H4	(a) Trust in App Providers → Perceived Privacy Risk	-0.117	0.016*	-0.201	0.000***
	(b) Trust in Regulation → Perceived Privacy Risk	-0.174	0.001***	-0.131	0.022*
H5	Social Norm → Intention to Use	0.434	0.000***	0.423	0.000***

*Table 2. Hypothesis Testing (Note: *p <0.05, **p <0.01, ***p <0.001)*

6 Discussion

This research aims to understand the adoption of COVID-19 apps through the lens of the privacy calculus, while adding to the benefits structure as well as a construct of social norm. We primarily address Pillar III of Von Wyl et al.'s (2020) research agenda for digital contact tracing apps, on user acceptability. More specifically, our study contributes a micro perspective (i.e., that of the user), providing insights into the users' perceptions of individual benefits and risks of app usage. Understanding users' privacy trade-offs can help in better shaping public health apps for future promotion of healthcare technology and their integration in the society.

In both the Swiss and German context, COVID-19 apps provide a central repository for infections and possible exposures with contextual data that can be further analyzed by researchers to provide epidemiological insights and better understand the spread of the pandemic on the national level. From the analysis, we see that privacy concerns are barriers to using COVID-19 apps. Previous research in the domain of social networks, e-commerce, and location-based services discusses how privacy risk perceptions act as impediments to the disclosure behavior and intentions to use (Xu et al., 2009; Krasnova et al., 2010; Naous et al., 2019). Our results confirm these findings to the category of public health apps, where privacy risk perceptions negatively impact intentions to use. However, our results show a negative relationship between the risk antecedents and the perceived privacy risks. Empirical results from the German population emphasize how the perceived privacy control by users can decrease their perceived privacy risks, which can result in higher intentions to use. This is not the case for Switzerland. In fact, prior research has shown that privacy-control settings might not be seen sufficient by users, due to lack of granularity or their complexity (Krasnova et al., 2010). COVID-19 apps, as developed by governments, have standard functionality and no different privacy options exist in them. This calls for more protective privacy-control settings that guarantee transparent app behavior, which in turn can affect the risk perception, for instance through data logs and dashboards within the app that provide an overview of data collection and processing with control over what data is shared and with who. The effect also radiates to trust.

Trust in innovations literature can be defined as the willingness to accept vulnerability based on having positive expectations about people's intentions and behaviors in risky situations (Clegg et al, 2002). As previously mentioned, the COVID-19 apps were developed and launched in record times when compared to innovative health technologies given the emergency contexts of their development. As highlighted in a study measuring the effect of trust in innovation processes, Clegg et al. (2002) find that trust acts as a main effect on ideas implementation in innovation processes. In this context, given the lack of an inclusive innovation process, building trust would have been a cost to intentions to use the application. Our results support this view, as trust in the app provider is negatively associated with perceived privacy risks. Therefore, it is crucial to have transparent app design and processing of user information for achieving trust in the app capabilities in fighting the pandemic without invasions to privacy. Trust in government regulations for protecting the individual and the trust in the app provider as the authorities are important in diminishing the effect of privacy risks. Reimer et al. (2020) highlight that trust in government and technology are factors that influence collective action at the societal level to guarantee mass adoption. Similarly, our results demonstrate that trust in regulations is negatively associated with perceived privacy risks. Government regulations should be able to protect app users from any mass surveillance acts, which are considered among the most critical aspects in using the app.

Our model shows that individual safety and epidemiological insights have a positive significant relationship with intentions to use COVID-19 apps, while societal safety is less valued by users. Although individual benefits stem from the societal benefit where infected people share their status to notify others, it seems that users value contact tracing apps for their ability to notify them about possible exposure. Contrary to Trang et al. (2020) whose study emphasizes the multi-layered benefit structure for COVID-19 apps in Germany by arguing that individual benefits do not necessarily drive user adoption of the app but its societal impact, our results suggest otherwise. A counter-intuitive aspect of the results is that an association lies in an individual's contribution to epidemiological insights of COVID-19 cases and the intention to use the app, however, sharing data for societal benefit in both Germany and Switzerland is not correlated with the intention to use the app in both country contexts. The results show a difference in perception of the degree to which a user is willing to surrender their data for outcomes (i.e., willing to-share the basic information for use of the app but not willing to disclose health status and trigger exposure for the benefits of the society). It is counter-intuitive because a key success factor of the app and of the COVID-19 prevention approach also depends on triggering the exposure to an infected person's network. The risks in disclosing a positive test result outweigh the benefits. Evidence of how situational settings and the interpersonal dimension of privacy can influence the privacy calculus is limited; however, the results of our study clearly define a change in the perceived risks/benefits based on situation and interpersonal concepts of privacy rights and rules. In a paper on disclosure intentions, Wang et al. (2016) highlight that monetary rewards (cash bonuses, discounts, and coupons) as well as social rewards (pleasure, satisfaction, and relationship development) can offset privacy risks in mobile social networking, with social rewards having more weight than monetary rewards. Follow-up studies could investigate this risk offsetting in health domains.

Our results underline the relatively strong positive impact of social norms on the intention to use, which is a very important point to consider for increasing adoption. Previous research on mobile applications and social networking apps, for instance, has shown that users would be willing to use an app if others are using it, which has been referred to social pressure for integration within a community (Min and Kim, 2015). As highlighted in yet other previous studies, social norm is important but can change in complicated and unexpected ways and respond to various stimuli in lower and higher levels of social organization (Ehrlich and Levin, 2005; Ostrom et al., 2002). Without enough social pressure, the efforts of a few will not have enough impact on existing privacy behaviors. Social pressures can be in the form of policy instruments, which can reinforce and/or influence social norm. Governments can also actively influence the norm through advertising campaigns, information blitzes or appeals to highly respected individuals in society. In addition, social norm can be managed by the provision of information to individuals and households about prevailing behaviors to induce conformity (Kinzig et al., 2013). The COVID-19 app is a health app that promotes the well-being of the society as a whole; therefore, mass-adoption would ideally be promoted through collective action by the different individuals and

influencers as well as higher-level institutions in the society like governments. Moving forward, the effectiveness of the COVID-19 apps could be evaluated on a public dimension and transparently. A proof-of-principle evaluation is available for the SwissCOVID app (Daniore et al., 2021) and evaluations of other country context apps could influence the public's weighting of privacy benefits versus risks.

7 Limitations

There are limitations to this study. Among them is the value placed on epidemiological insights per individual. While we understand that risk perceptions or benefit perceptions do not always correlate with actual risks or benefits, we highlight an individual's willingness to contribute to the epidiomogical insights through the intention to use the COVID-19 contact tracing app. A study on influenza A H1N2, for example, suggested that once media attention for the epidemic and epidiomological insights in five European countries were asynchronic, public risk perceptions and behaviors followed the media logic instead of the epidemiological logic (Reintjes et al., 2016).

In addition, our study has focused on two European samples from Germany and Switzerland with priory model of decentralized contact tracing, however, COVID-19 apps have a national scope and thus may be impacted by the specific national implementation as well as contextual factors. As avenue for future research, we encourage additional studies for understanding users' perceptions on COVID-19 apps in different settings. We also acknowledge a potentional sampling bias. This is due including only participants who have heard of the country-specific app and have limited knowledge of its functionalities. The lack of self-efficacy when it comes to privacy risks could influence the intention to use the app. A follow-up study could differentiate rural populations from urban populations to explore any similarities or differences in areas with high COVID-19 case loads, higher knowledge in the app and its functionalities and areas with lower case loads and knowledge of the app.

8 Conclusion

Applying the privacy calculus, our results provide empirical insights into the benefit and risk perceptions by users. It also highlights how situational context (what is to be shared) and social norm can influence risks and benefits using the case of contact tracing apps adoption in Switzerland and Germany. Our results can be relevant in exploring, what are the degrees of privacy according to social norm and interpersonal privacy rights and rules. From a practical perspective, our results are also relevant to health authorities and service providers of COVID-19 apps and have implications for improving health apps adoption. Our empirical results suggest that establishing a trustworthy relationship with users is a critical aspect. This can be achieved through transparent app design. Understanding users' privacy trade-offs assists developers and providers to address the privacy by design principles through operationalizing features valued and accepted by users and promoting undervalued characteristics. Our results show that an improved understanding of the benefits of COVID-19 apps would augment user intentions to use and therefore their adoption. Having control over the information and visibility on the data processing and treatment by the app provider is needed to minimize risk perceptions. One avenue to explore, in order to augment the app acceptability per Pillar III of Von Wyl et al.'s (2020) research agenda would be to follow participatory design principles or co-creation (user and provider) principles, as it can solidify user's trust through the equalizing of power (Gupta and De Gasperis, 2020). Our findings imply that social norm can act as driver for mass adoption. In the age of social media, influencers can play a decisive role in gaining critical mass and communicating the benefits to users. For instance, in Switzerland, around 30 influencers promote SwissCOVID on Instagram and had 1.4 million views of an advertisement for the app, placed by @swisspublichealth on the Tik Tok platform. Moreover, employers and essential businesses can drive this adoption rate by promoting and recommending the use of app on their premises.

Acknowledgment

This study was funded by the Swiss National Science Foundation (SNSF) under the SINERGIA grant "Development of Personalized Health in Switzerland: Social Sciences Perspectives" (grant no. CRSII5_180350).

References

Acquisti, A. and J. Grossklags (2004). "Privacy attitudes and privacy behavior." *Economics of Information Security*, Springer, Boston, MA, 165-178.

Anderson, C. L. and R. Agarwal (2011). "The digitization of healthcare: boundary risks, emotion, and consumer willingness to disclose personal health information." *Information Systems Research* 22(3), 469–490.

Ahmed, N., Michelin, R. A., Xue, W., Ruj, S., Malaney, R., Kanhere, S. S., Seneviratne, A., Hu, W.,
Janicke, H. and Jha, S. K. (2020). "A survey of covid-19 contact tracing apps." *IEEE Access* 8, 134577–134601.

Altmann, S., Milsom, L., Zillessen, H., Blasone, R., Gerdon, F., Bach, R., Kreuter, F., Nosenzo, D., Toussaert, S. and Abeler, J. (2020). "Acceptability of App-Based Contact Tracing for COVID-19: Cross-Country Survey Study". *JMIR Mhealth Uhealth* 8 (8), e19857

archyde (2020). *StopCovid flop: why tracking apps are more adopted by our neighbors*. URL: https://www.archyde.com/stopcovid-flop-why-tracking-apps-are-more-adopted-by-our-neighbors/ (Visited on 30 September 2021).

Bélanger, F. and R. E. Crossler (2011). "Privacy in the digital age: a review of information privacy research in information systems." *MIS quarterly* 35 (4), 1017–1042.

Bellman, S., Johnson, E. J., Kobrin, S. J. and Lohse, G. L. (2004). "International Differences in Information Privacy Concerns: A Global Survey of Consumers." *The Information Society* 20 (5), 313-324.

Cho, H., Ippolito, D. and Yu, Y. W. (2020). "Contact Tracing Mobile Apps for COVID-19: Privacy Considerations and Related Trade-Offs." *arXiv preprint arXiv*:2003.11511v2.

Clegg, C., Unsworth, K., Epitropaki, O. and Parker, G. (2002). "Implicating trust in the innovation process." *Journal of occupational and organizational psychology* 75 (4), 409-422.

Daniore, P., Ballouz, T., Menges, D. and von Wyl, V. (2021). "The SwissCovid Digital Proximity Tracing App after one year: Were expectations fulfilled?." *Swiss Medical Weekly* 151, w30031.

Dinev, T. and P. Hart (2006). "An extended privacy calculus model for e-commerce transactions." *Information Systems Research* 17 (1), 61–80.

Ehrlich, P. R. and S. A. Levin. "The evolution of norms." *PLoS biology* 3 (6), e194.

Ferretti, L., Wymant, C., Kendall, M., Zhao, L., Nurtay, A., Abeler-Dörner, L., Parker, M., Bonsall, D. and Fraser, C., (2020). "Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing." *Science* 368 (6491), eabb6936.

Follis, A. (2020). *ROME - Italian COVID app "Immuni" lacks sufficient users to be effective*.URL: https://www.euractiv.com/section/politics/short_news/rome-italian-covid-app-immuni-lackssufficient-users-to-be-effective/ (Visited on 30 September 2021).

Fornell, C. and D. F. Larcker (1981). "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error." *American Marketing Association* 18 (1), 39–50.

Gambs, S., Heen, O. and Potin, C. 2011. A comparative privacy analysis of geosocial networks. In: *Proceedings of the 4th ACM SIGSPATIAL International Workshop on Security and Privacy in GIS and LBS*, ACM, 33–40.

Guillon M. and P. Kergall (2020). "Attitudes and opinions on quarantine and support for a contact-tracing application in France during the COVID-19 outbreak". *Public Health 188*, 21-31.

Gupta, A. and T. De Gasperis (2020). "Participatory Design to build better contact-and proximitytracing apps." *arXiv preprint arXiv:2006.00432*.

Hair, J. F., Ringle, C. M. and Sarstedt, M. (2011). "PLS-SEM: Indeed a silver bullet." *Journal of Marketing theory and Practice* 19 (2), 139–152.

Klatt, K. (2020). *Opinion | Corona apps: South Korea and the dark side of digital tracking.* URL: https://www.brusselstimes.com/opinion/108594/corona-apps-south-korea-and-the-dark-side-ofdigital-tracking/ (Visited on 30 September 2021).

Kinzig, A.P., Ehrlich, P.R., Alston, L.J., Arrow, K., Barrett, S., Buchman, T.G., Daily, G.C., Levin, B., Levin, S., Oppenheimer, M. and Ostrom, E. (2013). "Social norms and global environmental challenges: the complex interaction of behaviors, values, and policy." *BioScience* 63 (3), 164-175.

Krasnova, H., Spiekermann, S., Koroleva, K., and Hildebrand, T. (2010). "Online social networks: Why we disclose." *Journal of information technology* 25 (2), 109–125.

Laufer, R.S. and M. Wolfe (1977). "Privacy as a concept and a social issue: A multidimensional developmental theory." *Journal of social Issues* 33 (3), 22–42.

Legendre, F., Humbert, M., Mermoud, A., and Lenders, V. (2020). "Contact Tracing: An Overview of Technologies and Cyber Risks." *arXiv preprint arXiv:2007.02806*.

Min, J. and B. Kim (2015). "How are people enticed to disclose personal information despite privacy concerns in social network sites? The calculus between benefit and cost." *Journal of the Association for Information Science and Technology* 66 (4), 839–857.

Naous, D., Kulkarni, V., Legner, C., and Garbinato, B. 2019. Information Disclosure in Location-Based Services: An Extended Privacy Calculus Model. In: *Proceedings of the International Conference on Information systems (ICIS 2019),* Munich, Germany.

Norman, J. (2020). *Deputy CMO urges Australians to use COVIDSafe app following updates*. URL:https://www.abc.net.au/news/2020-08-09/australians-encouraged-to-activate-covidsafecoronvirusapp/12539494 (Visited on 30 September 2020).

OECD (2021). *Health Spending.* URL: https://data.oecd.org/healthres/health-spending.htm (visited on 11 November 2021).

Ostrom, E. E., Dietz, T. E., Dolšak, N. E., Stern, P. C., Stonich, S. E. and Weber, E. U. (2002). "The Drama of the Commons." *National Academies Press.*

Rahman, M. S. 2019. Does Privacy Matters When We are Sick? An Extended Privacy Calculus Model for Healthcare Technology Adoption Behavior. In: *Proceedings of the 10th International Conference on Information and Communication Systems (ICICS 2019)*. IEEE, 41–46.

Redmiles, E. M. (2020). "User Concerns & Tradeoffs in Technology-Facilitated Contact Tracing." *arXiv Preprint arXiv:2004.13219v3.*

Reintjes, R., Das, E., Klemm, C., Richardus, J. H., Keßler, V. and Ahmad, A. (2016). "Pandemic Public Health Paradox: Time Series Analysis of the 2009/10 Influenza A / H1N1 Epidemiology, Media Attention, Risk Perception and Public Reactions in 5 European Countries." *PloS one* 11 (3), e0151258.

Reuters (2020). *Austria invites suggestions to improve coronavirus track and trace app*. URL:https://www.reuters.com/article/healthcoronavirus-austria-apps-idUSL8N2EF1BB (Visited on 30 September 2020).

Riemer, K., Ciriello, R., Peter, S. and 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 (6), 731-745.

Rowe, F. (2020). "Contact Tracing Apps and Values Dilemmas: A Privacy Paradox in a Neo-Liberal World." *International Journal of Information Management* 55, 102178.

Smith, H. J., Dinev, T. and Xu, H. (2011). "Information privacy research: an interdisciplinary review."*MIS quarterly* 35 (4), 989–1016.

Smith, H. J., Milberg, S. J. and Burke, S. J. (1996). "Information Privacy: Measuring Individuals Concerns about Organizational Practices." *MIS Quarterly* 20 (2), 167–196.

Sun, Y., Wang, N., Shen, X. L. and Zhang, J. X. (2015). "Location information disclosure in locationbased social network services: Privacy calculus, benefit structure, and gender differences." *Computers in Human Behavior* 52, 278–292.

Trang, S., Trenz, M., Weiger, W. H., Tarafdar, M., and Cheung, C. M. (2020). "One app to trace them all? Examining app specifications for mass acceptance of contact-tracing apps." *European Journal of Information Systems* 29 (4), 1–14.

University of Oxford (2020). *Digital contact tracing can slow or even stop coronavirus transmission and ease us out of lockdown*. URL: https://www.research.ox.ac.uk/Article/2020-04-16-digitalcontact-tracing-can-slow-or-even-stop-coronavirus-transmission-and-ease-us-out-of-lockdown (Visited on 30 September 2021).

Walrave, M., Waeterloos, C., and Ponnet, K. (2020). "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." *Cyberpsychology, Behavior, and Social Networking* 24 (6), 377-383.

WHO, C. (2018). "Emergencies preparedness, response." *Chikungunya*, p.2.

Von Wyl, V., Bonhoeffer, S., Bugnion, E., Puhan, M. A., Salathé, M., Stadler, T., Troncoso, C., Vayena, E. and Low, N.(2020). "A research agenda for digital proximity tracing apps." *Swiss Medical Weekly* 150 (29-30), w20324.

Xu, H., Teo, H.-H., Tan, B. C., and Agarwal, R. (2009). "The role of push-pull technology in privacy calculus: the case of location-based services." *Journal of management information systems* 26 (3), 135–174.

Xu, H., Dinev, T., Smith, J., and Hart, P. (2011). "Information privacy concerns: Linking individual perceptions with institutional privacy assurances." *Journal of the Association for Information Systems* 12 (12), 1.

Yang, S.-K., Kwon, Y.-J. and Lee, S.-Y. T. (2018). "The Impact of Information Sharing Legislation on Cybersecurity Industry." *Industrial Management & Data Systems* 120 (9), 1777-1794.

Zhang, X., Liu, S., Chen, X., Wang, L., Gao, B. and Zhu, Q. (2018). "Health information privacy concerns, antecedents, and information disclosure intention in online health communities." *Information & Management* 55 (4), 482–493.

Zimmermann, B. M., Fiske, A., Prainsack, B., Hangel, N., McLennan, S. and 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 (2), e25525.

Appendix A: Constructs Reliability

Construct	Germany				Switzerland			
	Cronbach's Alpha	**rho_A**	**CR**	**AVE**	**Cronbach's Alpha**	**rho_A**	**CR**	**AVE**
Intention to Use	0.966	0.967	0.978	0.937	0.956	0.956	0.971	0.919
Benefit Proximity Tracking	0.906	0.906	0.941	0.841	0.890	0.890	0.932	0.819
Benefit Societal Safety	0.873	0.878	0.922	0.798	0.837	0.875	0.900	0.751
Benefit Epidemiological Insights	0.900	0.901	0.938	0.834	0.864	0.866	0.917	0.787
Privacy Control	0.917	0.925	0.947	0.857	0.904	0.913	0.940	0.838
Trust in App Providers	0.937	0.939	0.960	0.888	0.950	0.952	0.968	0.909
Trust in Regulation	0.957	0.957	0.972	0.921	0.966	0.966	0.978	0.936
Social Norm	0.867	0.886	0.917	0.787	0.855	0.868	0.911	0.774

Appendix B: Constructs and Measures

Construct		Adapted	Measures
Perceived Privacy Risk (prk)	prk1	Xu et al. 2009	I feel that using the COVID-19 app would involve many unexpected problems.
	prk2		Overall, I see no real threat to my privacy when using the COVID-19 app.*(inverted)
	prk3		I feel that using the COVID-19 app is risky.
Benefit: Individual Safety - Proximity Tracking	bis1	Self-developed	I trust that the COVID-19 app reliably identifies actual contact with an infected person.
	bis2		I trust that the COVID-19 app notifies me on exposure to the virus.
	bis3		I trust that the COVID-19 app detects possible encouter with a person infected with COVID-19.
Benefit: Societal Safety	bss1	Self-developed	With the COVID-19 app, I am able to share my status with people I have been in contact with if I had COVID-19.
	bss2		With the COVID-19 app, I am able to notify my recent contacts in case of infection with COVID-19.
	bss3		With the COVID-19 app, I am able to protect my family and friends through notifying them in case of infection.
Benefit: Epidemiological Insights	bei1	Self-developed	I trust that, with the COVID-19 app, authorities are able to better monitor the spread of COVID-19.
	bei2		I trust that the COVID-19 app improves the statistics on the spread of the virus.
	bei3		I trust that the COVID-19 app provides relevant information for deciding on measures to reduce the spread of the virus.
Intentions to use	i1	Xu et al. 2009	I am likely to use the COVID-19 app authorized by public health authorities.
	i2		I am willing to use the COVID-19 app authorized by public health authorities.
	i3		It is probable that I use the COVID-19 app authorized by public health authorities.
Social Norm	sn1	Min and Kim 2015	I feel that I should use the COVID-19 app because everybody else seems to be using it.
	sn2		I feel that most people who are important to me think I should use the COVID-19 app.
	sn3		I feel that people who influence my behavior think that I should use the COVID-19 app.
Perceived Control	ctl1	Krasnova et al. 2010	I feel in control over my data if the COVID-19 app uses anonymous communication (through anonymized user IDs).
	ctl2		Privacy-preserving settings present in COVID-19 apps allow me to have full control over the data I provide.
	ctl3		I feel in control of who can view my data if the COVID-19 app uses informed consent.
Trust: Regulations	trg1	Xu et al. 2009	Government regulations protect my information provided on the COVID-19 app.
	trg2		Government regulations protect me from any misuse of my information on the COVID-19 app.
	trg3		Government regulations protect me from unauthorized use of my information disclosed on the COVID-19 app.
Trust: App Providers	tsp1	Krasnova et al. 2010	I trust that COVID-19 app providers are trustworthy and will not misuse any of my information.
	tsp2		I trust that COVID-19 app providers are honest in their dealings with me and my data.
	tsp3		I trust that COVID-19 app providers are interested in the well being of individuals.