Computers in Human Behavior 121 (2021) 106806

Contents lists available at ScienceDirect

Computers in Human Behavior

journal homepage: http://www.elsevier.com/locate/comphumbeh

Exploring the competing influences of privacy concerns and positive beliefs on citizen acceptance of contact tracing mobile applications

Grace Fox [a,*], Trevor Clohessy [b], Lisa van der Werff [a], Pierangelo Rosati [a], Theo Lynn [a]

[a] Irish Institute of Digital Business, Dublin City University Business School, Collins Ave, Dublin 9, Ireland
[b] Department of Enterprise and Technology, Galway Mayo Institute of Technology, Old Dublin Rd, Galway, Ireland

ARTICLE INFO

Keywords:
Privacy calculus
Reciprocity
Government surveillance technology
Privacy
Contact tracing
Proximity tracing
Health surveillance technology
Mobile applications
COVID-19

ABSTRACT

The continued proliferation of information technology in all aspects of our lives fosters benefits but also generates risks to individuals' privacy. In emerging contexts, such as government surveillance technologies, there is a dearth of research investigating the positive and negative drivers of citizens' acceptance. This is an important gap given the importance of citizen acceptance to the success of these technologies and the need to balance potentially wide-reaching benefits with any dilution of citizen privacy. We conduct a longitudinal examination of the competing influences of positive beliefs and privacy concerns on citizens' acceptance of a COVID-19 national contact tracing mobile application among 405 Irish citizens. Combining privacy calculus theory with social exchange theory, we find that citizens' initial acceptance is shaped by their perceptions of health benefits and social influence, with reciprocity exhibiting a sustained influence on acceptance over time and privacy concerns demonstrating a negative, albeit weak influence on willingness to rely on the application. The study offers important empirical and theoretical implications for the privacy literature in the government surveillance, location-based services, and mobile health application contexts, as well as practical implications for governments and developers introducing applications that rely on mass acceptance and reciprocal information disclosure.

1. Introduction

Information technology has become omnipresent in all aspects of our lives. Despite the recent shift in social norms around data collection and analysis, privacy remains a pertinent issue which organizations and governments must consider and address (Dinev, 2014; Pentina, Zhang, Bata, & Chen, 2016). Recent years have seen an increase in the introduction of government surveillance technologies, which enable governments to track citizen transactions and online activity (Reddick, Chatfield, & Jaramillo, 2015). These technologies are largely viewed as invasive due to their impact on individuals' privacy (Bannister, 2005). Indeed, inadequate consideration of citizens' privacy concerns may lead to low acceptance and adoption rates of new government surveillance technologies (Krishen, Raschke, Close, & Kachroo, 2017). While many potential benefits stem from the implementation of different government surveillance technologies, the need to collect data must be balanced with citizens' privacy concerns to achieve citizen acceptance (Trüdinger and Steckermeier, 2017). Despite the growing public awareness and undeniable privacy implications, research in this domain trails other contexts, except for a small number of notable studies (Nam, 2019). Furthermore, extant research focuses largely on citizen acceptance of surveillance programs on a general level (e.g., Thompson, McGill, Bunn, & Alexander, 2020), and the influence of privacy and surveillance concerns on citizens' general online behavior (e.g., Dinev, Bellotto, Hart, Russo, & Serra, 2006; Dinev, Hart, & Mullen, 2008). The contextual nature of privacy and the event-driven nature of surveillance technologies requires consideration in the form of research examining the influence of privacy on citizen acceptance of specific government surveillance technologies (Nam, 2018).

Consequently, this study focuses on the introduction of a national contact tracing mobile application (app) in Ireland. During health crises, such as the current novel coronavirus global pandemic (COVID-19), contact tracing applications aim to reduce and eliminate disease transmission by tracing contacts and isolating exposed individuals (Yasaka, Lehrich, & Sahyouni, 2020). Thus the benefits of these technologies can be extensive and wide-reaching with greater adoption yielding benefits for citizens, health bodies, and governments alike. However, the implementation of such applications by governments as a form of

* Corresponding author.
E-mail addresses: grace.fox@dcu.ie (G. Fox), Trevor.Clohessy@gmit.ie (T. Clohessy), lisa.vanderwerff@dcu.ie (L. van der Werff), pierangelo.rosati@dcu.ie (P. Rosati), theo.lynn@dcu.ie (T. Lynn).

https://doi.org/10.1016/j.chb.2021.106806
Received 18 September 2020; Received in revised form 11 March 2021; Accepted 30 March 2021
Available online 3 April 2021

surveillance technology and clinical intervention also generates understandable privacy concerns (Zastrow, 2020). As the success of these applications is largely dependent on mass citizen acceptance, privacy must be balanced with benefits to achieve this acceptance (Yasaka et al., 2020; Zastrow, 2020). In addition to individuals' perceptions of the privacy and benefits these technologies offer, adoption decisions may be also be influenced by social and relational factors such as the perception of peers, friends and family members towards the technology and the reciprocal benefits of the technology. To examine the interplay between citizens' perceptions of privacy, benefits, and social influence, this study investigates the following research question: *How do privacy, social, and benefit perceptions influence individuals' acceptance of a government contact tracing mobile application?*

To examine this question, we conduct a longitudinal two-stage survey of 405 individuals before and post launch of a national contact tracing application. This study contributes to existing privacy literature in the domain of government surveillance as well as research related to mobile location-based applications (LBS) and mobile health (m-health) applications. First, the paper combines the privacy calculus theory with social exchange theory to extend our focus beyond immediate perceptions of the technology to consider the role of broader social factors in influencing acceptance of government surveillance technologies. Specifically, we consider the role of social influence and perceptions of both perceived health benefits and reciprocal benefits on citizen acceptance of a specific surveillance technology. This contributes to various calls by researchers (e.g., Jozani, Ayaburi, Ko, & Choo, 2020; Trepte, Scharkow, & Dienlin, 2020) to extend and integrate the privacy calculus theory with other diverse theoretical perspectives to develop a more holistic view of cost benefit analyses in technology acceptance. Secondly, the study investigates acceptance as both behavioral intentions and willingness to rely on the application thereby answering calls for empirical investigation of a more diverse set of outcome variables (Benamati, Ozdemir, & Smith, 2017). In particular, the study seeks to understand citizen behavior early in the diffusion process (before and shortly after launch). While prior research has applied common technology acceptance theoretical frameworks, including TAM and UTAUT, to government surveillance, the constructs and disposition used in such frameworks are oriented towards post-launch diffusion and are less applicable to the pre-launch phase. Thirdly and relatedly, the paper examines behavioral intentions before and post launch of the application, thereby answering calls for longitudinal studies in the privacy and technology adoption domains (Dinev et al., 2008; Hoehle, Aloysius, Goodarzi, & Venkatesh, 2019) and considering the potential for early perceptions to have a lasting impact on technology use. Our findings support the combination of the privacy calculus with social exchange theory. They suggest that perceived health benefits, social influence, and reciprocity influence adoption intentions prior to launch, and reciprocal benefits also influence usage intentions over time. However, privacy concerns do not influence acceptance prior to or post launch, and only exhibit a weak influence on willingness to rely on the application. This suggests that reciprocal and health benefits coupled with social influence outweigh concern for privacy in the context of contact tracing applications.

The remainder of the paper is structured as follows; the next section discusses the theoretical underpinnings of our study. Our research model and hypotheses are developed in the third section. The methodology and analysis sections follow. Lastly, the final sections discuss the implications of the study for theory and practice, while acknowledging some limitations and identifying avenues for future research in this important but underexamined context.

2. Theoretical background

The privacy literature can be chronologically organized into three stages. The third stage (3a and 3b) includes all research from 2008, the focus of which has shifted largely to the sharing economy and emerging contexts such as surveillance (Yun, Lee, & Kim, 2019). Due to the differing perspectives and disciplinary lenses from which privacy is studied, there are many competing definitions of privacy, leading to arguments that a general definition of privacy cannot be achieved (Pavlou, 2011). Within the Information Systems (IS) domain, descriptions of privacy largely center around the issue of control and individuals' desire for some level of control. As a result, privacy is often described as individuals' desire to be afforded greater control over the collection and use of their personal information (Bélanger & Crossler, 2011).

Despite the myriad of research conducted in the past three decades, privacy research remains in an early stage of theoretical development as many variables and theories have been studied a small number of times in different contexts (Wirth, 2018; Yun et al., 2019). Existing theories can be categorized based on their emphasis with some theories leveraged to understand the origins of privacy concern, others focused on explaining the individual and organizational factors influencing privacy concerns, theories focused on untangling the trade-offs between privacy and other factors like benefits, and theories focused on the consequences of privacy concern (Li, 2012). Also, theories from other fields such as psychology are frequently adapted to study privacy in different contexts.

The privacy calculus theory (PCT) is categorized as a trade-off theory in that it examines the influence of competing positive and negative beliefs on individuals' willingness to engage with an online organization or technology and is the most commonly used theory within the privacy literature (Wirth, 2018; Yun et al., 2019). PCT has been described as the most useful framework for understanding consumer privacy concerns (Culnan & Bies, 2003). The widespread utilization of the privacy calculus theory may be attributable to its flexibility and the support it has received across a host of contexts and different positive and negative perception based variables (Miltgen & Smith, 2019). PCT provides a solid foundation but often requires a combination of other theories to account for gaps (Sun, Wang, Shen, & Zhang, 2015). As a result, we follow studies within this context (e.g., Dinev et al., 2008) and utilize the privacy calculus theory as our underpinning theory, while also drawing from social exchange theory to develop our calculus model which encompasses a broader set of context specific trade-off variables.

2.1. Government surveillance technology acceptance

Technology adoption represents one of the most developed streams of research within the IS domain comprising a number of theories such as the theory of planned behavior or TPB (Azjen, 1991) and the unified theory of technology acceptance and use or UTAUT (Venkatesh, Morris, Davis, & Davis, 2003). Many of these theories are related and derived from sociology and psychology literature (Venkatesh, Thong, & Xu, 2012). Indeed, Venkatesh et al. (2003) reviewed the eight dominant technology adoption theories to develop UTAUT, a theory examining the influence of factors such as performance expectancy, effort expectancy, subjective norm, and facilitating conditions on individuals' acceptance of new technologies. These theories, predominately UTAUT and the earlier technology acceptance model or TAM (Davis, 1989) have been consistently extended and adapted to examine individuals' adoption of information technology in a number of contexts from consumers' adoption of e-commerce (e.g., Pavlou & Fygenson, 2006) to citizens' acceptance of electronic government technologies (e.g Carter & Bélanger, 2005). More recently, adaptations of UTAUT have been helpful in understanding acceptance of innovations such as health wearable devices (e.g., Wang, Tao, Yu, & Qu, 2020) and blockchain technology (e.g., Queiroz & Wamba, 2019).

Another field which has seen significant investment and development in recent years is that of surveillance technology. Global governments are increasingly implementing sophisticated surveillance technologies facilitating access to real-time data that can be leveraged in efforts to assist with policing, enhancing government to citizen engagement, and assisting with the tracking, mitigation, and eradication

of disease transmission. Surveillance includes "any collection and processing of personal data, whether identifiable or not, for purposes of influencing or managing those whose data have been garnered" (Lyon, 2001, p. 2). Personal data in this context can refer to CCTV images, biometrics, contact information, calls records, and so on. Government surveillance specifically focuses on "the use of sophisticated technology to observe our daily activities (physical surveillance) and to peruse records of those activities (transaction surveillance)" (Slobogin, 2008). Recent research in the area of governmental based surveillance technology has focused on surveillance technologies such as social media and artificial intelligence based-surveillance (Anton, Kus, & Teuteberg, 2021, p. 2121), and visual recognition Internet of Things smart city based surveillance (Kumar et al., 2021). Surveillance technology has been described as a necessary evil (Nam, 2019) and encompassing two sides (Lyon, 2001) where one side is beneficial (e.g., citizen screening, classification) and the other side negative (e.g., security risks, intrusion concerns, privacy risks). The emergence of COVID-19 has resulted in the introduction of governmental top-down surveillance technology initiatives (e.g., tracking applications, CCTV, monitoring sensors/tags) worldwide which are aimed at slowing down the spread of the disease.

Citizens' acceptance of these surveillance technology initiatives is fundamental to their success and requires a willingness on the part of individual citizens to forego their location based information, contact information and information regarding their close contacts to protect themselves and other citizens. While a small but growing body of recent research has examined governmental based surveillance technologies, there is a dearth of research which has focused on citizens' acceptance of these technologies (Nam, 2019). Studies which have investigated the area have found that: (1) citizens' perceptions of benefits from using governmental surveillance technologies (Nam, 2018), (2) government surveillance technology policy transparency (Thompson et al., 2020), and (3) the presence of privacy (Dinev et al., 2006; Nam, 2019) enhances citizens' trust in surveillance technologies. Ultimately, these considerations are important predictors of citizen surveillance technology acceptance (Thompson et al., 2020).

We build on the emerging body of surveillance acceptance literature to examine the drivers of citizens' acceptance and use of mobile contact tracing applications. As these applications collect health and location data for use at a national level, it is both a surveillance and mobile-health technology and as such is accompanied by a range of potential benefits and privacy risks. In addition to the parallels between the outcome variables in our study and the outcomes popularized in the technology acceptance literature, we argue that social influence is pertinent in this context due to the importance of reciprocal adoption and disclosure among citizens to the success of these applications. However, the early stage of diffusion of these technologies renders many of the factors predicting adoption encompassed in UTAUT and related models such as perceived ease of use inappropriate for inclusion in our study. Indeed, in line with the emergent literature on contact tracing applications (Chan & Saqib, 2021) and the tradition of much of the privacy literature, our focus is not on technology adoption models but on more contextually relevant factors that are known to be of importance to adoption in health and surveillance domains such as privacy (Wu, Wang, & Lin, 2007) and perceived health benefits (Fox, 2020).

2.2. Privacy calculus theory

The primary proposition of the privacy calculus theory is that individuals' behavior is influenced by the careful consideration of the potential negative and positive outcomes associated with the behavior (Laufer & Wolfe, 1977). Privacy calculus theory posits that "personal information provides economic value to trade and explains personal privacy interests as an exchange between information and benefit" (Kim, Park, Park, & Ahn, 2019, p. 274). This perspective provides the foundation for trade-offs between the benefits and perceived risks when individuals encounter information disclosure requests. It is argued that individuals make privacy-related decisions to disclose personal information to a requesting entity through the use of an application or website (e.g., customers purchasing products online, airport Wi-Fi, government online services) after they evaluate the positives and negatives resulting from the decision (Dinev & Hart, 2006). The decision to divulge this personal information is underpinned by a "calculus of behavior" (Culnan & Armstrong, 1999) where individuals assess possible outcomes and weigh up the positives and negatives associated with each result. Individuals are more likely to engage with information technology or disclose personal information in situations where the perceived positives outweigh the perceived negatives (Dinev & Hart, 2006).

Studies have investigated the privacy calculus as an antecedent to behavioral reactions in various domains including personal information disclosure online (Barth & De Jong, 2017; Choi, Wu, Yu, & Land, 2018), willingness to disclose personal information to the Internet of Things (IoT) devices (Kim et al., 2019) and mobile devices or apps (Keith et at., 2013; Morosan & DeFranco, 2015). The flexibility of the privacy calculus is also evidenced in the operationalization of a wide range of negative and positive belief variables (Fox, 2020). Negative beliefs can be broadly termed risk beliefs and may include perceived intrusion (Li, 2012; Xu, Dinev, Smith, & Hart, 2008), situational privacy concerns regarding health information (e.g., Fox, 2020) surveillance (Thompson et al., 2020), and general online privacy concerns (e.g., Dinev et al., 2008; Hallam & Zanella, 2017; Marakhimov & Joo, 2017). Positive beliefs can also be termed confidence beliefs and tend to focus on the utilitarian benefits of specific technologies such as personalized services (e.g., Xu, Teo, Tan, & Agarwal, 2012), IoT services (Kim et al., 2019), health benefits of health technologies (Fox, 2020) or the perceived need for government surveillance (Dinev et al., 2008; Thompson et al., 2020). In summary, the privacy calculus theory proposes two potential paths that may explain acceptance of the technology in this study, one path from negative risk beliefs and the other path from positive confidence beliefs (Keith, Thompson, Hale, Lowry, & Greer, 2013; Sun et al., 2015). In addition to perceptions related to privacy and health benefits, social structures and norms are likely to impact acceptance in the contact tracing application context.

2.2.1. Perceived health benefits

In the context of this study, perceived health benefits refer to the extent that people believe that they will experience health benefits from downloading the COVID-19 mobile contact tracing app. Markus and Keil (1994) describe how technology can be used for "good" reasons which result in positive outcomes but also for "bad" reasons which can result in negative outcomes. According to Bowman, Westerman, and Claus (2012) people rationally engage in behaviors that lead to positive outcomes, especially since most of their goals intend to benefit themselves positively. The primary health benefits (positive outcomes) of using a mobile contact tracing app can be viewed from micro and macro perspectives. At a micro level the mobile app can be used to protect one's personal health and the health of family and community members. Additionally, mobile contract tracing apps are an alternative to strict lockdown measures which have been applied as a result of COVID-19. The blunt measures have been applied to everyone (e.g., those at risk, those who have been infected and those who are deemed healthy). Early evidence suggests that these blanket lockdowns have had collateral effects in terms of negatively impacting individuals' mental health (Holmes et al., 2020) and physical health (Pietrobelli et al., 2020). For example, people are more likely to delay much needed medical treatment in order to adhere to lockdown protocols and out of fear for their health (Holmes et al., 2020). Mobile contact tracing apps, in conjunction with a functional national testing system, can enable people to return to their 'new normal' lives. Parker, Fraser, Abeler-Dörner, and Bonsall (2020) describe mobile contact tracing apps as an "intelligent" means of social distancing in comparison to the "unintelligent" means of social distancing prescribed by national lockdowns. At a macro level, the

mobile contact tracing apps can be used to slow the rate of infection for a specific disease (Parker et al., 2020).

2.3. Social exchange theory

Consistent with the core values of the privacy calculus, social exchange theory (Blau, 1964) seeks to understand human behavior with an emphasis on social structures and norms (Church, Thambusamy, & Nemati, 2017). The theory which embraces modern economics (Shiau & Luo, 2012) was initially developed for studying human behavior (Homans, 1958), and later refined for researching power-dependence relationship behaviors in organizations (Emerson, 1962). More recently, SET has been leveraged to understand how individuals balance social factors with privacy risks to understand interaction with technologies such as social media (Church et al., 2017; Wang & Liu, 2019; Wang & Midha, 2012). The utility of SET in the privacy domain has been demonstrated and SET has been beneficial in advancing our understanding of subjective cost (e.g., privacy concerns) and benefit (improved health) analysis of technological exchanges of personal information (e.g., Acquisti, Brandimarte, & Loewenstein, 2015; Min & Kim, 2015; Posey, Lowry, Roberts, & Ellis, 2010; Shiau & Luo, 2012). As a result, there have been calls issued for the further utilization of theories like SET to better unravel the factors driving individuals' decisions to interact with organizations or technologies and disclose information in these interactions (Wirth, 2018).

SET stipulates that people generally expect reciprocal benefits when being required to adhere to social norms. Core to understanding the behavioral sharing motives of exchanges are the perspectives of egoistic and altruistic (Deci, 1975). Whereas the egoistic perspective is largely influenced by rewards, the altruistic perspective is motivated by a prosocial drive to enhance the welfare of others without expecting personal or economic incentives. With the introduction of contact tracing applications, individuals are required to disclose personal information to reduce transmission of the virus. Indeed, in order for the applications to be successful, others must reciprocate by downloading the application and sharing their information. This study adopts SET to extend our understanding of the costs and benefits of technology use traditionally considered using PCT, by examining the potential for broader social influences and the potential reciprocal benefits to impact technology acceptance. In doing so, we seek to understand the exchange dynamics of several forms of personal information including health data regarding symptoms, personally identifiable information and location data between citizens and a government issued mobile contact tracing application.

2.3.1. Social influence

Researchers have modelled social influence or subjective norm as a predictor of individuals' decisions to adopt new information technologies (e.g., Venkatesh et al., 2003), mobile social networking sites (Zhou & Li, 2014), and sharing location devices (Beldad & Kusumadewi, 2015). Social influence can be described as an individual's perception of social normative pressures or relevant others' beliefs that he or she should or should not perform a behavior such as downloading a new application (Venkatesh et al., 2003). Social influence has also been identified as a factor affecting mobile health and medical applications user behavior (Boulos, Brewer, Karimkhani, Buller, & Dellavalle, 2014; Chang, Lu, Yang, & Luarn, 2016). Mobile health and medical applications enable users to log and track their personal health metrics (e.g., height, weight, blood glucose levels, exercise data, etc) and share their health achievements with other users via social networks and communities (Hamari & Koivisto, 2015). This ability for users to share and connect with a community of people and benchmark their performance reinforces the power of social influence to download mobile health and medical applications (Li et al., 2017; Whelan & Clohessy, 2020, pp. 1–41). It has been demonstrated that the process of compliance/conformance, plays a key component in explaining the impact of social influence on technology adoption (Cialdini & Goldstein, 2004:; Young, 2009). That is, people will download mobile health and medical mobile technologies when other people in a community have already downloaded them. In other words, an individual's perceptions of their peer's attitudes towards contact tracing applications, may influence their acceptance. Additionally, if individuals do not adopt the application, they may believe they are failing to conform to social norms. Given the deleterious health implications of COVID-19, it is important to explore the role of social influence in this context.

2.3.2. Reciprocity

SET dictates that when people exchange resources with other people, they generally expect reciprocal benefits (Blau, 1964). From an IS perspective, reciprocity is defined as the belief that information sharing results in an obligation for a future request for knowledge being obliged (Shiau & Luo, 2012). By adhering to the 'rules of the exchange', SET explains how relationships can evolve into trusting commitments (Emerson, 1976) which ultimately drives and reinforces the process of information and knowledge sharing (Davenport et al., 1998). According to Hamari and Koivisto (2015) reciprocity is a powerful social driver and motivator which emphasizes the returning of a favour or a positive action with another. Reciprocity results in benefits which manifest through the strengthening of shared norms via group interactions. Cialdini (2009) describes how reciprocal benefits, which he refers to as 'weapons of influence', are core to the compliance process. However, reciprocity is inherently flexible and can be exploited by triggering 'unfair exchanges' whereby people will attempt to maximise their benefits while concurrently reducing their risks during an exchange (Cialdini, 2009). Ultimately, a person's level of reciprocal return will be dictated by their cognitive processes (Bandura, 1986). We argue that the nature of contact tracing applications and the requirement to download the application and disclose personal data to achieve the common goal of reducing transmission of the virus renders reciprocal benefits relevant to this study. Reciprocity is important not just in individuals' decisions to download the app but also their willingness to rely on the application for health advice.

3. Hypotheses development

To understand the drivers of individuals' intentions towards a national contact tracing application, this study leverages the privacy calculus to understand the competing influence of negative beliefs (privacy concerns) and positive beliefs (perceived benefits) and integrates SET to unravel the role of social factors (social influence and reciprocal benefits). The descriptions of all constructs and proposed model are illustrated in Table 1 and Fig. 1 respectively.

3.1. Trade-offs and outcomes

Citizen acceptance of government surveillance technologies is crucial to success yet remains understudied (Nam, 2018). While existing literature focuses on the acceptance of surveillance practices in general (e.g., Thomspon et al., 2010; bib_Trüdinger_and_Steckermeier_2017Trüdinger & Steckermeier, 2017), this study focuses on examining the influences of perceptions regarding privacy, benefits, and social factors on acceptance of a national contact tracing application. Technology acceptance in this study is captured with three variables; adoption intention, willingness to rely on the application and future usage intentions. Adoption intentions are measured prior to the implementation of the app at time 1 (T1) and future usage intentions are measured after launch at time 2 (T2). It is important to capture the role of these competing beliefs before and after the introduction of the technology (Hoehle et al., 2019) particularly given the potential for early intentions and attitudes to provide a critical anchor that influences later acceptance (bib_Saadé_and_Otrakji_2007Saadé & Otrakji, 2007). Furthermore, as the success of the application is based not only on

Table 1
Constructs in the model.

Construct	Acronym	Description
Social Influence	SI	An individual's perception of relevant others' beliefs that he or she should or should download the new application (Venkatesh et al., 2003)
Reciprocal benefits of the app	REP	An individual's perception of the reciprocal benefits everyone will experience from using the application (Hamari & Koivisto, 2015).
Perceived Health Benefits of the app	BEN	An individual's perception of the health benefits they will experience from using the application (Li, Gupta, Zhang, & Sarathy, 2014).
Privacy Concerns	PC	The extent to which individuals believe they may lose their privacy from interacting with mobile applications (Dinev et al., 2008).
Adoption Intention	INT	An individual's self-assessed likelihood of adopting the application (Venkatesh et al., 2003).
Future Usage Intention	USE	An individual's self-assessed likelihood of adopting/continuing use of the application.
Willingness to rely on the app	RELY	An individual's willingness to provide health advice provided in the application.

downloads but on an individual's willingness to act on health advice within the app (e.g., to self-isolate), we include willingness to rely on the app as another variable representing citizen acceptance. In developing our model, we draw on PCT and SET to consider how individual perceptions of the costs and benefits of the contact tracing app influence our outcome variables. We propose that in the context of health related government surveillance, the impact of perceived health benefits of technology suggested by PCT will be accompanied by a positive impact of broader social benefits related to social influence and reciprocation.

3.2. Social factors (SET)

Social influence is a core predictor of individuals' behavioral intentions and eventual behavior within the technology adoption literature. Generally, if individuals believe that their peers or important referent others would view the behavior in question favorably, they are more likely to engage in the behavior (Venkatesh et al., 2003). The influence of social influence on adoption intentions has been supported in technology adoption studies across a host of contexts from organizational (e.g., Venkatesh et al., 2003) to farming (e.g., Fox, Mooney, Rosati, Paulsson, & Lynn, 2018). Social influence has been adopted in the privacy literature sparingly with mixed support. For example, in one study, social influence was found to positively influence individuals' intentions to use mobile commerce among Chinese citizens but not among US citizens (Dai & Palvi, 2009), and social influence positively influenced information disclosure in online communities among French participants but was not significant among UK participants (Posey et al., 2010). The role of social influence has not been examined in the surveillance literature. Thus, we draw on literature from the related fields of health applications and location-based services. In terms of the former, social influence positively influenced individuals' intentions towards a Taiwanese medical travel app (Chang, Chou, Yeh, & Tseng, 2016). In terms of the latter, Beldad and Kusumadewi (2015) provided support for the positive role of social influence on individuals' willingness to use applications requiring location sharing. In addition, a recent study has found that social influence or subjective norm as it is termed in that study positively influenced intentions to download contact tracing apps in the future (Sharma et al., 2020). In line with these findings, we argue that if individuals believe referent others would view downloading the application as a positive behavior, they will be more likely to download.

H1. Social Influence is positively associated with adoption intentions.

Extant studies leveraging PCT tend to focus on how individuals' willingness to disclose information is determined by utilitarian benefits of a technology or information exchange such as the usefulness of the technology for a given purpose and more recently incorporating hedonic benefits related to enjoyment. There have been calls to examine the

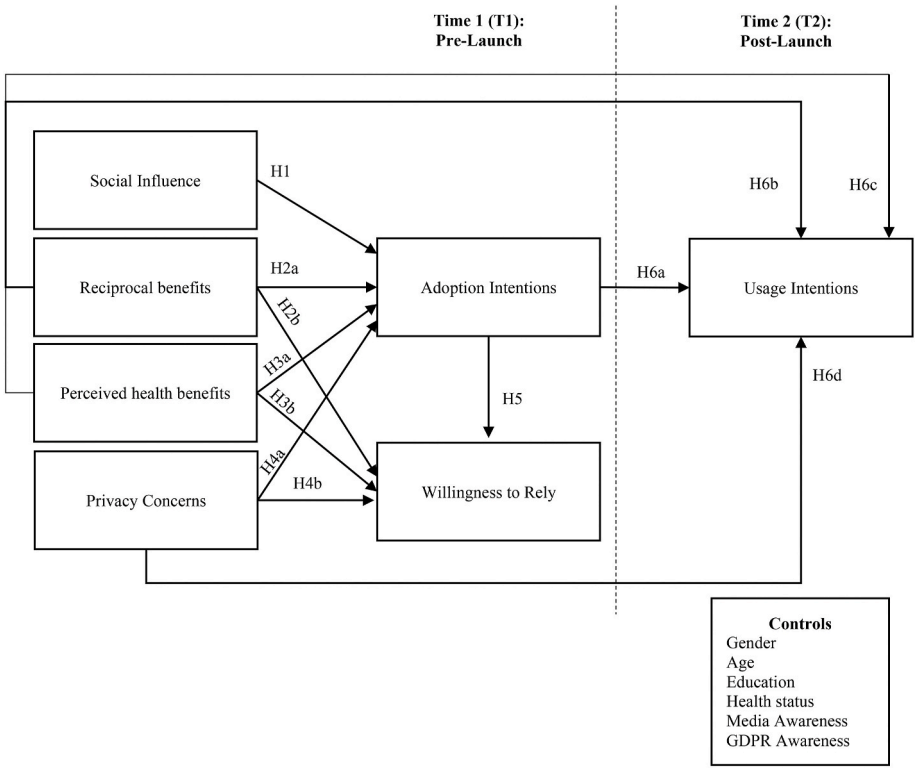

Fig. 1. Proposed research model.

importance of other benefits in different contexts (Sun et al., 2015). Reciprocal benefits refer to individuals' perceptions that downloading the application will generate benefits for themselves and others (Hamari & Koivisto, 2015). Social exchange theory proposes that individuals will be more likely to engage in behaviors they believe align with social norms provided they see reciprocal benefits resulting from these behaviors. In their study of self-disclosure on online communities, Posey et al. (2010) found reciprocity perceptions positively influenced disclosure among French participants but not among UK participants. In their study, Nam (2018) found that perceived public benefits stemming from surveillance measures were positively associated with acceptance of surveillance. In the contact tracing context, benefits in the form of reduced virus transmission are dependent on individuals downloading the application and acting upon advice in the application. In line with Nam (2018), we argue a similar position as if individuals believe the application can benefit the greater good, they are more likely to both adopt the application and rely on the application.

H2a. Reciprocal benefits are positively associated with adoption intentions.

H2b. Reciprocal benefits are positively associated with willingness to rely on the application.

3.3. Perceived benefits (PCT)

Perceived health benefits refer to the personal benefits an individual believes they will experience as a result of using the application. In the health context, health benefits have been positively related to individuals' acceptance of technologies introduced by health organizations such as electronic health record systems (EHRs) (Fox, 2020), and technologies downloaded by individuals themselves such as mobile health applications (Fox, 2020) and wearable tracing devices (Guo, Sun, Wang, Peng, & Yan, 2013; Li, Wu, Gao, & Shi, 2016). Thus, in line with findings in the health context and the proposition within the privacy calculus theory that perceived benefits can represent a positive path to adoption of a technology, we argue that individuals who believe the application will yield benefits for their personal health will express high intentions towards downloading the app and greater willingness to rely on the advice within the app.

H3a. Perceived Health benefits are positively associated with adoption intentions.

H3b. Perceived Health benefits are positively associated with willingness to rely on the application.

3.4. Perceived costs (PCT)

While the variables we consider above represent the potential benefits of using the contact tracing app, both PCT and SET suggest that these benefits will be weighed up against the potential costs of technology use. One of the primary concerns engendered by the use of government surveillance technologies is privacy (Bannister, 2005). As privacy cannot be measured, IS researchers must rely on proxy measures, the most popular of which is privacy concerns (Smith, Dinev, & Xu, 2011). Privacy concerns have been studied within the privacy calculus framework in a number of privacy studies including studies within both the health technology and government surveillance domains. Privacy concerns relate to "the extent which individuals believe they might lose their privacy" (Dinev et al., 2008, p. 218), and can be studied at general levels to capture privacy in a given domain such as the Internet (Dinev & Hart, 2006) or in specific situational contexts such as concerns related to personal health information (Fox & Connolly, 2018) or government intrusion concerns (Nam, 2018). In the health privacy literature, privacy concerns have been negatively associated with acceptance of health technologies such as EHRs (Angst & Agarwal, 2009; Fox & James, 2020; Li & Slee, 2014), willingness to disclose personal information in virtual health communities (Kordzadeh & Warren, 2017) and on health websites (Bansal, Zahedi, & Gefen, 2010), but have had mixed results on individuals' intentions to use mobile health applications with a study focused on older adults supporting the negative association (Fox & Connolly, 2018) and a broader, related study finding an insignificant result (Fox, 2020). In the surveillance context, online privacy concerns negatively impacted general willingness to disclose personal information online (Dinev et al., 2008), and concerns regarding collection negatively impacted individuals' acceptance of surveillance measures (Thompson et al., 2020).

As the COVID-19 tracing application requires personal information, health information and location information, we operationalize privacy concerns at the general mobile application level and describe privacy concerns as the extent to which individuals believe they may lose their privacy from interacting with mobile applications. If individuals believe their use of mobile applications results in a loss of privacy, they are less likely to engage with the application and as a result, may be also less likely to rely on the application for the purpose of health advice as this would require some use and as a result some privacy risk. Further, the link between individuals' intention to download the application and their willingness to rely on it requires examination. Given the premise of the application is to issue health advice and reduce virus transmission, it can be argued that individuals expressing high adoption intentions, that is they believe they will download the application, are also likely to express greater willingness to rely on the application.

H4a. Privacy concerns are negatively associated with adoption intentions.

H4b. Privacy concerns are negatively associated with willingness to rely on the application.

H5. Adoption intentions are positively associated with willingness to rely on the application.

3.5. Adoption intentions over time

There have been calls for research to understand perceptions of a technology pre and post launch (Hoehle et al., 2019). In the context of contact tracing applications, it is important to explore how perceptions of privacy, benefits, and social factors influence individuals' behavioral intentions after launch. Thus, we examine individuals' future usage intentions after launch of the application at time 2 (T2). We are interested in two discrete forms of behavioral intention at T2. First, as some individuals may have already downloaded the app, we focus on the intentions of these individuals to continue use. Second, as some individuals may have not yet downloaded the app, we measure their intentions to adopt the app in the near future. The general technology adoption literature proposes that intentions will lead to behavior (Fishbein & Ajzen, 1975). In other words, it is likely that if individuals expressed positive intentions towards downloading the application prior to launch, they will be likely to also express positive usage intentions after launch. Also, research has shown that the first impressions of a technology influence future use intentions (Saadé & Otrakji, 2007). Thus, we propose that adoption intentions will be positively linked to future intentions to download or continue to use the application.

H6a. Pre-launch adoption intentions (T1) are positively associated with post-launch usage intentions (T2).

There are no government surveillance studies that examine the role of privacy and perceived benefits over time to our knowledge. However, it can be argued that reciprocal benefits representing individuals' beliefs that their use of the application will benefit themselves and others are likely to influence their usage intentions after launch. That is people who believe the application will result in reciprocal benefits are more likely to continue to use or download the application if they have not yet done so. Similarly, individuals' perceptions related to the health benefits

they may experience by using the app are likely to influence their post-launch usage intentions. Privacy risk has been negatively related to intentions to continue use of location-based services in a previous study (Zhou, 2013). However, privacy concerns negatively influenced intentions to continue use of a mobile social networking service (SNS) in a study among university students in China (Zhou & Li, 2014) but had a positive influence on intention to continue use of SNS apps among Korean university students (Choi, 2016). Given the mixed findings, it is important to clarify the influence of privacy concerns on citizens' intentions after the launch of a government surveillance application. Based on the findings and the contextual relevance of the LBS study conducted by Zhou (2013), we posit that privacy concerns regarding mobile applications will persist after the launch of the application and will continue to have a negative impact on future usage intentions.

H6b. Reciprocal benefits are positively associated with usage intentions (T2).

H6c. Perceived health benefits are positively associated with usage intentions (T2).

H6d. Privacy concerns are negatively associated with usage intentions (T2).

4. Methodology

4.1. Study context

Covid-Tracker Ireland, a national contact tracing mobile application was launched by the government in Ireland on July 6, 2020. The application (shown below in Fig. 2) has three main features; contact tracing, Covid symptom check-in, and updates on the virus in Ireland. The app uses Bluetooth and anonymous IDs to log phones within close contact for over 15 min. The app then downloads the anonymous IDs of people who have tested positive and provides an alert if the user has been in close contact with any of those IDs. Covid check-in allows users to check any symptoms daily and seek health advice, and updates provide an overview of the daily facts and figures in Ireland. Within 48 h of its initial launch, over 1 million people had downloaded the app, and 300,000 people had checked-in, representing almost 50% of the 2.2 million adult smartphone users in Ireland (Brennan, 2020). This is an important achievement as it has been estimated that 60% penetration is required to effectively reduce virus transmission (Zastrow, 2020).

4.2. Instrument development and sampling

Existing scales were used when developing our instrument with minor wording amendments to adapt some items to the context of the contact tracking application. The sources of all variables is outlined in Table 2. At T1, participants' general privacy concerns in the mobile app context were measured as well as situational variables including perceptions of the health benefits and reciprocal benefits associated with the proposed app and social influence. Dependent variables included intention to download the app upon launch and willingness to rely on health advice in the app. At T2, the emphasis was on future behavioral intentions; namely usage of the app. Participants were asked if they had downloaded the app and app users' intentions to continue to use the app were examined and non-users' intentions to download the app in the future were examined. Table 2 details the source and number of items for each construct. The full list of items is provided in the Appendix.

Furthermore, several control variables were included based on the privacy literature. These include demographics which have been found to have mixed impacts on privacy and associated behaviors including gender, age, education level, health status, and experience variables namely awareness of privacy media coverage (1 item from Smith, Milberg, & Burke, 1996) and awareness of the existing privacy regulation the European General Data Protection regulation (GDPR), as knowledge of regulation has been found to influence privacy concern in previous studies (e.g., Miltgen & Smith, 2015). The survey was piloted tested among a small panel of survey design experiments and several wording amendments were made before pilot testing among 10 Irish citizens of varying ages. Respondents were asked to answer demographic and health questions first, followed by general perceptual constructs and control variables, the order of which was randomized. In the third

Table 2
Operationalization of constructs.

Construct	Items	Source
Adoption Intentions (T1 & T2)	3	Venkatesh et al. (2003); Bhattacherjee (2001)
Perceived Health benefits	5	Li et al. (2014)
Reciprocal Benefits	2	Hamari and Koivisto (2015)
Willingness to Rely on App	3	McKnight, Choudhury, and Kacmar (2002)
Social Influence	4	Hamari and Koivisto (2015)
Privacy Concerns	4	Dinev and Hart (2006)

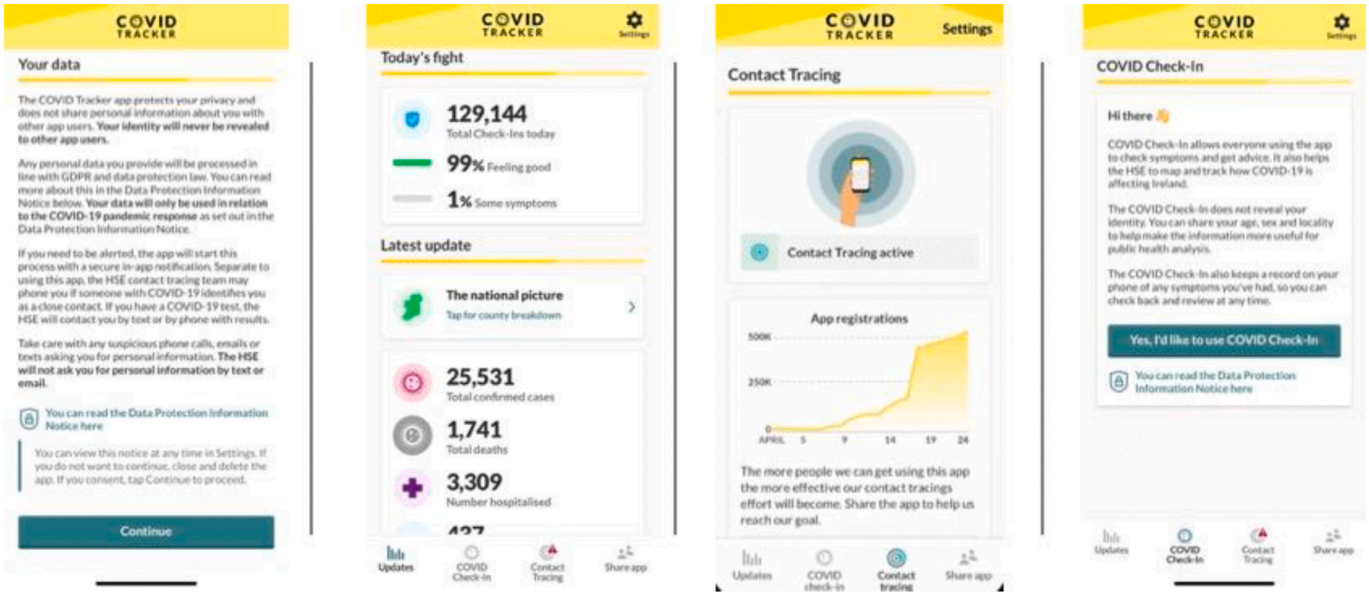

Fig. 2. National contact tracing application.

section, participants were presented with a neutrally framed description of the proposed national contact tracing application at T1 and a description of the launched app was presented at T2. The final section examined perceptions towards the application, and behavioral intentions.

A filter question was included at the start of the survey to ensure participants were aged 18 years and over. Qualtrics was used to host and administer the survey using their panel services. The survey did not collect identifying personal information from respondents, in order to reduce any fears around anonymity and reduce potential common method bias as a result (MacKenzie, Podsakoff, & Podsakoff, 2011). Additional approaches in the survey design to reduce common method bias included informing participants that there were no right or wrong answers. An attention trap was included in the survey to screen out unengaged responses. Due to the focus on the Irish contact tracing application, respondents were restricted to residents in the Republic of Ireland.

4.3. Respondents

A total of 1109 complete responses were received at T1, before the app launch. All of these respondents were recontacted at T2 following the app launch. After two follow-up invitations, a total of 405 responses were received at T2. No responses were removed as all incomplete responses and responses failing the age and attention checks were removed by Qualtrics. The sample demographics are similar to the population characteristics of Ireland as reported in the last census and include respondents from the 26 counties within the country. The gender spilt of the sample was 55.5% female and 44.5% male respectively. Respondents represented various education levels with 38.8% completing high school, and 32.8% holding an Undergraduate degree. In terms of employment status, the majority of respondents indicated they were employed (45.9%), a further 25.7% were retired and the remainder were unemployed (8.9%), studying (2.7%), or unavailable to work (10.4%). To control for health status, respondents were asked if they had any health condition which classified them as vulnerable with regards to COVID-19. The majority indicated no, whereas 18.3% (n = 74) indicated they had a health condition which rendered them more vulnerable to COVID-19. Of the 405 respondents, 202 had downloaded the app and 203 had not yet downloaded the app. The sample characteristics are illustrated below in Table 3.

5. Data analysis and results

Data screening focused on ensuring the data met the thresholds required for multivariate analysis (Hair, Black, Babin, & Anderson, 2010). All items across the seven variables met recommended ± kurtosis and skewness thresholds. To examine multicollinearity, the variance inflation factor (VIF) was calculated for all variables. As all VIF scores were below 10, multicollinearity is not an issue in the data. Data analysis was performed in AMOS v25.0. The proposed factor structure was examined using Confirmatory Factor Analysis (CFA) in AMOS. The seven-factor model indicated good fit across the fit statistics meeting the thresholds outlined by Hair et al. (2010). Three covariances between errors were added to improve fit; two on perceived health benefits, and one on privacy concerns. The model fit statistics were as follows: cmin/df: 2.682, CFI: 0.973, RMSEA: 0.065, SRMR: 0.028. To test for possible common method bias, the common latent factor approach was used based on Gaskin (2019). As there were no significant changes in regression weights after the addition of the common latent factor, common method variance is not considered an issue. Validity and reliability of all constructs was explored. Convergent validity requires all constructs that should converge strongly correlate with each other (Straub et el., 2004) and is assessed by calculating the average variance extracted (AVE). As all variables had AVE scores above 0.50, convergent validity is achieved (Fornell & Larcker, 1981). Discriminant validity requires items on one construct to be sufficiently different from items on other constructs (Straub, Boudreau, & Gefen, 2004). Discriminant validity was tested by comparing the square root of the AVE with the inter-construct correlations (Hair et al., 2010). As the square root of AVE was higher than inter-construct correlations, discriminant validity is achieved, as shown by bold diagonal values in Table 4. Reliability was assessed by calculating the composite reliability (CR) for each construct. With CR scores above 0.70, all constructs were reliable (Raykov, 1997). The data was then imputed for subsequent analysis.

5.1. Hypotheses testing

The proposed causal model was tested using Structural Equation modelling (SEM) in AMOS v25. The model indicated strong fit; cmin/df: 1.850, CFI: 0.999, RMSEA: 0.046, SRMR: 0.0028. Hypothesis 1 proposed a positive relationship between social influence and intention to download the proposed contact tracing application. The data revealed a positive, significant relationship supporting H1 (β 0.168, $p < .001$). H2a and H2b posited that reciprocal benefits would have a positive relationship with intention to download and willingness to rely on the app respectively. Both relationships were strongly supported in the data (H2a: β 0.603, $p < .001$, H2b: β 0.433, $p < .001$). A positive relationship between perceived health benefits and both adoption intentions and willingness to rely on the application were proposed in H3a-b. These relationships were also supported (H3a: β 0.140, $p < .01$, H3b: β 0.303, $p < .001$). In H4a and H4b, it was proposed that privacy concerns would negatively influence individuals' intentions to download the app and rely on the application respectively. Both relationships were negative but insignificant, although with a p value of .052, the relationship proposed in H4b was just above the 0.05 confidence level (H4a: β -.036, $p > .05$, H4b: β -.035, p: >0.05). Lastly, H5 posited that intention to download the application would positively influence willingness to rely on the application. A positive, significant relationship was found in the data, offering strong support for H5 (β 0.253, $p < .001$).

The next set of hypotheses focused on usage intentions at T2. A positive relationship was proposed between adoption intentions at T1 and usage intentions at T2. The data revealed a positive, significant relationship, thus supporting H6a (β 0.483, $p < .001$). It was also posited that reciprocal benefits (H6b) and perceived health benefits (H6c) would positively influence usage intentions at T2. While both relationships were positive, only reciprocal benefits had a significant influence at the 0.05 level thereby supporting H6b but not H6c (H6b: β 0.176, $p < .05$, H6c: β 0.029, $p > .05$). Lastly, a negative association was proposed between privacy concerns and usage intentions at T2. The relationship

Table 3
Sample characteristics.

Gender		Age		Employment		Education	
Male	180	18–24	11	Employed	186	Secondary School	157
Female	225	25–34	51	Self-employed	26	Trade	5
Rather Not Say	0	35–44	73	Unemployed	36	Diploma	32
		45–54	77	Student	11	Bachelor degree	133
		55+	193	Unavailable for work	42	Other Qualification	64
				Retired	104	Doctorate degree	14

Table 4
Validity and reliability statistics.

	CR	AVE	1	2	3	4	5	6	7
1.Health Benefits	.952	.800	**.894**						
2.Social Influence	.927	.762	.770***	**.873**					
3.Adoption Intention (T1)	.990	.970	.759***	.752***	**.985**				
4.Willingness to Rely	.963	.898	.836***	.777***	.851***	**.947**			
5. Reciprocal Benefits	.976	.952	.808***	.784***	.851***	.888***	**.976**		
6. Privacy Concerns	.927	.761	-.061	-.087	-.132*	-.147**	-.135*	**.873**	
7. Usage Intention (T2)	.991	.973	.532***	.517***	.657***	.610***	.610***	-.140**	**.986**

***p < .001, **p < .01, *p < .05.

was negative but not significant at the 0.05 level (β -.063, p > .05).

In terms of control variables, most relationships were insignificant. However, gender had a significant influence on willingness to rely on the application with women less likely to rely on the app and GDPR awareness had a positive influence on usage intention at T2. The model demonstrates respectable variance explained across the three acceptance variables with 76.9% of the variance in individuals'intentions to download the application at T1 explained and 88.3% of the variance explained in willingness to rely on the application as well as 46.8% of variance in usage intentions at T2. Reciprocal benefits was the strongest predictor of both intentions to download the application and willingness to rely on the application, whereas adoption intention was the strongest predictor of T2 usage intentions. Bootstrapping was conducted using 2000 samples and a confidence level of 90% to explore indirect effects. Reciprocal benefits had a significant indirect influence on behavioral intentions at T2 (β 0.291, p < .01) and perceived health benefits had a positive significant indirect influence (β 0.069, p < .05), whereas privacy concern had a negative indirect effect on behavioral intentions (β -.017, p > .05), but this effect was not significant at the 0.05 level. The results are summarized in Table 5 and Fig. 3 below.

Table 5
Summary of results.

Hypothesis	Support?	Standardized regression weight	p-value
H1: Social Influence → Adoption Intention (T1)	Yes	.168	<0.001
H2a: Reciprocal Benefits → Adoption Intention (T1)	Yes	.603	<0.001
H2b: Reciprocal Benefits → Willingness to Rely (T1)	Yes	.433	<0.001
H3a: Perceived Health Benefits → Adoption Intention (T1)	Yes	.140	0.003
H3b: Perceived Health Benefits → Willingness to Rely (T1)	Yes	.303	<0.001
H4a: Privacy concern → Adoption Intention (T1)	No	-.036	>0.05
H4b: Privacy concern → Willingness to Rely (T1)	Weak	-.035	0.052
H5: Adoption Intention (T1)→ Willingness to Rely (T1)	Yes	.253	<0.001
H6a: Adoption Intention (T1)→ Usage Intention (T2)	Yes	.483	<0.001
H6b: Reciprocal Benefits → Usage Intention (T2)	Yes	.176	0.038
H6c: Perceived Health Benefits → Usage Intention (T2)	No	.029	>0.05
H6d: Privacy concern → Usage Intention (T2)	No	-.063	0.098
Controls			
Gender → Adoption Intention (T1)		−0.011	0.648
Gender → Willingness to rely (T1)		−0.035	0.044
Gender → Usage Intention (T2)		0.049	0.184
Education → Adoption Intention (T1)		0.025	0.304
Education → Willingness to rely (T1)		−0.001	0.963
Education → Usage Intention (T2)		0.054	0.146
Age → Adoption Intention (T1)		0.013	0.608
Age → Willingness to rely (T1)		0.012	0.515
Age → Usage Intention (T2)		−0.027	0.485
GDPR Awareness → Adoption Intention (T1)		0.001	0.974
GDPR Awareness → Willingness to rely (T1)		−0.017	0.358
GDPR Awareness → Usage Intention (T2)		0.087	0.024
Media Awareness → Adoption Intention (T1)		0.040	0.122
Media Awareness → Willingness to rely (T1)		−0.026	0.158
Media Awareness → Usage Intention (T2)		0.043	0.283
Health status → Adoption Intention (T1)		0.004	0.887
Health status → Willingness to rely (T1)		−0.005	0.777
Health status → Usage Intention (T2)		0.013	0.737

6. Discussion

Contact tracing applications require individuals to disclose personal health information related to symptoms, identifiable information such as name and contact information, and their location information to improve tracing and reduce transmission. While there are obvious benefits to the reduction of transmission, the types of data required render privacy an important issue which requires consideration. This study combines the privacy calculus theory with social exchange theory to examine the competing influences of individuals' benefits,privacy beliefs and social factors on their acceptance of the national contact tracing application in Ireland. The study contributes to the body of literature arguing the theoretical and practical importance of understanding how privacy influences individuals' acceptance of new technologies with acceptance represented by many variables including willingness to accept specific government surveillance technologies (Nam, 2018), willingness to disclose location data to applications (Jozani et al., 2020; Sun et al., 2015) and willingness to adopt and disclose information to health technologies (Fox, 2020). In this study, citizen acceptance was represented by three variables, two of which are measured before the app launch and one measured after launch. First, the analysis reveals that individuals' intention to download the application was shaped only by positively framed beliefs namely social influence, reciprocal benefits and perceived health benefits, whereas risk or negative beliefs related to privacy concern did not have a significant influence. Willingness to rely on the application is a core function of acceptance in this context. Our findings show that both individuals' perceptions of reciprocal and health benefits associated with the app positively influence willingness to rely, and privacy concern has a negative but weak influence. Individuals' future intentions regarding the application were influenced by their prior adoption intentions and reciprocal benefits, with privacy concern found to have a negative influence at the .10 level.

The significant role of social influence on initial adoption intentions supports the technology adoption literature and the influence of referent others on individuals' willingness to use a technology (Venkatesh et al.,

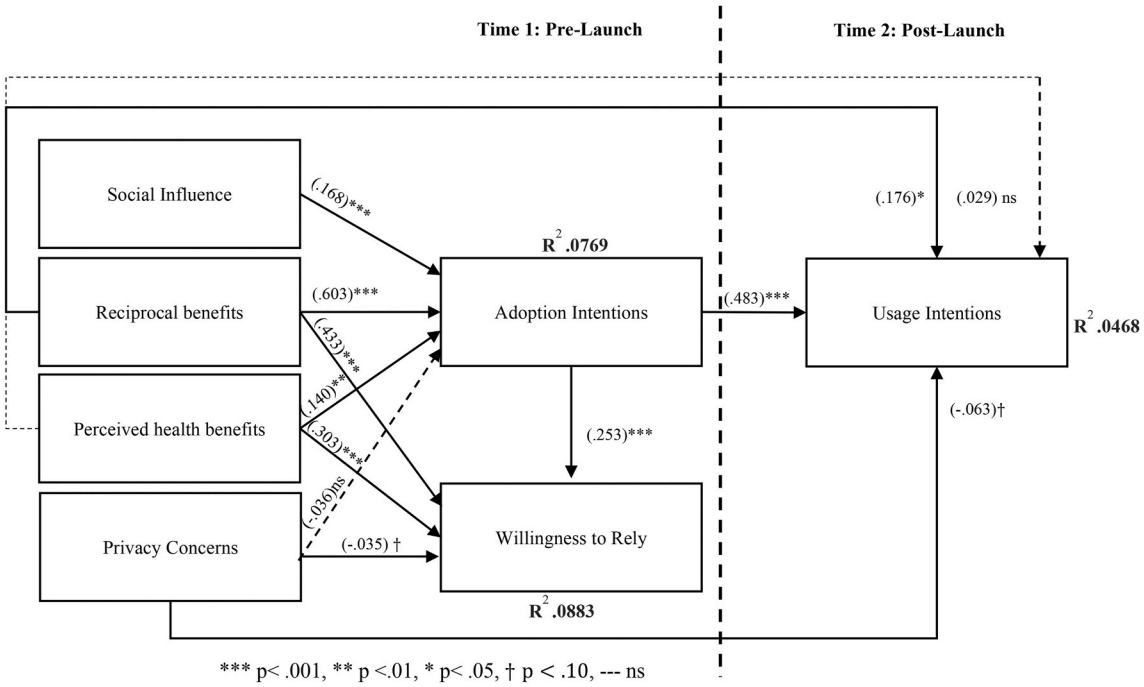

Fig. 3. Structural model results.

2003). Surprisingly, social influence has been largely ignored in studies focused on privacy or technology acceptance that involves some level of information disclosure except for some recent studies such as Posey et al. (2010) who found mixed support for its role in shaping information disclosure on social networking sites and more recently in Sharma et al. (2020), who found support for the positive role of subjective norm in shaping intentions to download contact tracing apps in the future. We argue that social influence is particularly pertinent in contexts which require mass acceptance of new technology in order to achieve success such as government surveillance technologies as examined in this study. If individuals believe referent others such as peers, friends, and family members would view their decision to download the contact tracing application favorably, they are more likely to download the app. Strongly aligned to the issue of social influence is the role of reciprocity, which is a form of social influence.

Perceived reciprocity can signal to individuals that others also accept some vulnerability by adopting the application and disclosing their information, thus positively impacting the individual's assessment of the behavior and increasing their own willingness to be vulnerable by engaging in the behavior in question (Posey et al., 2010). In our study, perceptions of reciprocal benefits positively influenced all three acceptance variables; intentions to adopt, willingness to rely, and future usage intentions. Thus, we extend support for social exchange theory to the privacy context in relation to a contact tracing application. The findings suggest that even when an application requires disclosure of sensitive location and health information, if individuals believe the application can benefit themselves and the wider community, they are more likely to accept and rely on the application, signalling a commitment to the application and the information it presents. The inclusion of reciprocal benefits in our studies answers calls to consider additional benefits beyond utilitarian benefits and hedonic benefits (Sun et al., 2015). Moreover, our study shows that in the current context, individuals' perceptions of the health benefits they may experience from using the application are also important determinants of acceptance of the application prior to launch. Interestingly, this perception did not significantly influence future intentions after launch, but this may be partly explained by the significant indirect effect revealed in post-hoc bootstrapping analysis.

The mixed findings on the role of privacy concern further obfuscates our understanding of privacy across situational contexts. Some related studies in the health technology domain have found significant negative relationships between privacy concerns and intentions towards new technologies including EHRs (Fox & James, 2020), but not mobile health technologies (Fox, 2020). Studies in the government surveillance context have not yet examined the PC-acceptance relationship among specific technologies but have offered support for the negative influence of privacy concern at a more general level including on individuals' willingness to disclose personal information online (Dinev et al., 2008), and broad acceptance of surveillance measures (Thompson et al., 2020). Looking at the broader privacy literature, a number of recent studies have found an insignificant influence across different conceptualizations of privacy and acceptance including privacy risk on intentions towards IoT services (Kim et al., 2019), privacy concerns on app usage (Pentina et al., 2016), and privacy concerns on intentions towards different online activities (Crossler & Posey, 2017). These disparities are also evident in studies conducted after the implementation of a new technology or amongst existing users of a technology. For example, privacy concerns negatively influenced continuance intentions among social networking users in one Chinese study (Zhou & Li, 2014) but did not significantly influence LBS usage intentions among existing users and non-users in another study (Xu & Gupta, 2009).

Some of these discrepancies may be attributed to the different proxy variables used to measure privacy including privacy risk, privacy concern, and perceived privacy (Smith et al., 2011), the different measurement scales leveraged, as well as the level of conceptualization of both privacy and acceptance variables. Indeed, Davazdahemami, Hammer, Kalgotra, and Luse (2020) attribute the inconsistencies between privacy and outcome variables to the three levels in which existing studies conceptualize privacy concerns and outcomes namely; the general level i.e. general privacy concerns or willingness to disclose personal information generally, the contextual level such as mobile applications or social networking services and the situational level i.e. concerns or acceptance within a given context. The mixed findings for privacy concern in this study and others can also be discussed using the privacy calculus lens. It may be that the role of positive beliefs in this study including powerful social influences, potential health benefits and

reciprocal benefits outweighed individuals' considerations of the privacy implications of such technologies. It may also relate to the possible temporal influence of privacy as recently discussed by Hallam and Zanella (2017), who found that online privacy concerns did not influence self-reported information disclosure online, but negatively influenced near-future information disclosure intentions and negatively influenced far-future intentions to engage in privacy-protective behaviors such as withholding information, whereas social rewards influenced near-future intentions to disclose and self-reported online disclosure behaviors. In addition, a recent mixed methods study found that perceived health benefits positively influenced individuals' adoption intentions towards EHRs and mobile health technologies, whereas privacy concerns only influenced intentions towards EHRs, but privacy concerns were more influential in determining post-usage behaviors such as discontinuance or privacy protective behaviors (Fox, 2020). Our findings offer some support for this temporality effect with privacy concerns exhibiting a significant, albeit weak influence on app usage intentions after launch, but not prior to launch. Individuals may not effectively consider the risk or privacy aspects of adoption prior to the launch (Barth & De Jong, 2017) or they might be willing to download the application but may not be fully committed. This is suggested by the negative influence on willingness to rely, as individuals' privacy concerns negatively impacts this willingness which may be seen as a lack of complete acceptance of the application. After launch, when individuals have a greater understanding of the application and the information disclosure it requires, their consideration of privacy may be more conscious.

In summary, these findings support the privacy calculus theory and social exchange theory in this situational context, highlighting the strong influences of all positive beliefs prior to launch and the sustained importance of reciprocity after launch. Privacy concerns exhibit some negative influence on willingness to rely on the application and usage intentions after use. This suggests that the cost-benefit analysis individuals conduct may be more weighted towards the positive outcomes prior to launch, but privacy remains important particularly after launch.

6.1. Implications for research

This study makes two core theoretical contributions. First, this study adopts a broader conceptualization of citizen acceptance to consider both adoption and usage intentions over time and willingness to rely on the application. Most privacy studies are cross-sectional in nature, as highlighted in a recent literature review which identified 13 longitudinal studies compared to 191 cross-sectional studies (Wirth, 2018). This is an important void within the privacy and technology adoption literature that this study addresses. In the privacy literature, the *privacy paradox*, or the mismatch between individuals' privacy concerns and their disclosure and technology usage behaviors has led to researchers issuing cautions around assumptions that intended behaviors will result in actual behaviors (Bélanger & Crossler, 2011). Additionally, the e-government branch of the technology adoption literature has called for longitudinal studies (Venkatesh, Thong, Chan, & Hu, 2016). The longitudinal nature of this study enables the examination of the privacy calculus over time.

Second, the study extends the privacy calculus theory to integrate social exchange theory considering the role of social influence and reciprocal benefits on citizen acceptance of a specific government surveillance technology. Prior studies have employed the privacy calculus theory across various perspectives (e.g., Gutierrez, O'Leary, Rana, Dwivedi, & Calle, 2019; Kim et al., 2019). However, the majority of these studies have either only used privacy calculus as the sole theoretical perspective or have only used a narrow set of trade-off variables (Miltgen & Smith, 2019) which has ultimately led to calls for more divergent theoretical perspectives (Jozani et al., 2020; Trepte et al., 2020). Privacy in the context of government surveillance technologies is extremely complex because there are often demonstratable benefits of these technologies but their use often leads to clear invasions of individuals' privacy. Using the privacy calculus as the foundational theory in conjunction with social exchange theory, this study develops a theoretical model encompassing a broader set of trade-offs and contributes to understanding the competing influences related to benefits and risks on citizen acceptance of a specific emerging technology.

6.2. Implications for practice

Our study has practical implications for governments and developers of contact tracing applications and similar technologies that require citizen adoption and sensitive information disclosure to function. Many governments introduce new technologies without considering citizens' concerns, which may lead to low take up rates and ultimate failure (Krishen et al., 2017). COVID-19 is a highly contagious pathogenic viral disease. Its sudden and rapid transmission worldwide left policymakers with little time in which to make robust decisions regarding non-pharmaceutical interventions such as social isolation and the implementation of contact tracing programmes, in the absence of strain-specific control options. This is not an apologia for governments in their delays in rolling out robust programmes of digital contact tracing and associated promotion and communication plans in response to COVID-19. Member states of the World Health Organization (WHO) are obligated to develop citizen health surveillance systems and processes in the event of global pandemics (WHO, 2005). Failure to impose such systems can hamper a government's public and clinical health response to the pandemic. Consequently, it is important for governments to implement an effective digital contact tracing strategy with the highest level of population coverage possible. In the case of mobile contact tracing applications, a network effect occurs as the number of users increases, which consequently increases the mobile application's value and usefulness (Gu, Xu, Xu, Zhang, & Ling, 2017). Achieving a sufficiently high penetration of a population is not an insignificant challenge. For example, COVID-19 contact tracing apps have a target 60% penetration rate to achieve their aim of reducing virus transmission (Zastrow, 2020). This being the case and given both the challenges of initial adoption and building and maintaining trust in digital contact tracing programmes, policymakers should consider whether there are long term public health benefits, beyond COVID-19, in normalizing the use of digital contact tracing apps. Indeed, recent research suggests that contact tracing apps might be better adopted outside of or before pandemics when disease concerns are low (Chan & Saqib, 2021). In the case of COVID-19 contact tracing apps, this requires careful consideration as the public has only permitted for their data to be captured and used in the specific context of COVID-19. Any future update of the contact tracing app for more general health surveillance would require an additional opt-in by the user, potentially to the detriment of take-up and trust in the app and/or government. Given the delicate balance between public health, privacy, civil liberties inherent in digital contact tracing, governments need to consult and liaise with all stakeholders, including the public, data protection authorities, and civil liberties advocates as early and transparently as possible, and that suitable governance mechanisms are put in place to provide oversight on digital contact tracing programs.

While our study found that privacy concerns did not play a significant role, this finding does not suggest that privacy is unimportant. As per PCT, it may be that perceived benefits outweighed privacy concerns in this context. However, communication efforts from governments introducing surveillance technologies such as contact tracing applications should seek to address privacy concerns by stressing the privacy protections and the reasons behind requests for information disclosure. Specifically, governments should justify their design and functional decisions in a transparent manner. Policymakers need to justify and be transparent about their technical choices and the implications for citizens clearly linking the functional decisions to health benefits. Whether rightly or wrongly, in the context of the COVID-19 contact tracing apps,

the privacy debate has been framed around decisions to pursue one of two approaches to contact tracing - (i) decentralized contact tracing where data remains distributed on individual devices, or (ii) centralized contact tracing where data is aggregated on a central server (Sweeney, 2020). While the former supports privacy by design and personal privacy rights, the latter provides greater data to health authorities faster and arguably contributes to greater understanding and decision-making related to disease transmission. Such decisions may be further complicated by where to centralize such data (e.g., federal, national, or supernational) and with whom such data will be shared. In this respect, The WHO has proposed 17 ethical and appropriate use principles for digital proximity tracing technologies (WHO, 2020). For example, these tracing applications should consider transparency and explainability. That is information relating to the data collection, data use and data storing processes should clear and unambiguous. Meaningful information should also be provided relating to instances of auto-decision-making algorithms and the probability and types of errors that may occur.

In line with SET and PCT, our findings confirm that social influence, perceived health benefits, reciprocity are important considerations. Governments must effectively communicate both the health and public benefits of using digital contact tracing applications prior to and after their launch. It is important to note that the use of digital contact tracing applications is only one method in a broader set of interventions used by governments to combat the transmission of disease. Consequently, to harness trust, governments are advised to show citizens how the cumulative impact of their mix of interventions interacts together to combat the spread of COVID-19 (WHO, 2020). Post-launch communication campaigns should continue to highlight the health and reciprocal benefits of the long-term use of the tracing application. The Irish application also contains an embedded social sharing tool which enables users to share the tracing application to their contacts across a myriad of social media communication platforms (e.g., Viber, WhatsApp, Facebook) thus enabling the harnessing of reciprocity and social influence. Governments are advised to review their tracing applications over time.

For developers of contact tracing applications and associated technologies, in addition to the considerations discussed above, there are salient ethical considerations and technical considerations that should be considered beyond compliance with data privacy regulations. For example, from a privacy perspective, it is imperative that designers should inform governments of potential privacy concerns that may manifest. Apple's and Google's deployment of open source code enabled governments to create COVID-19 tracing applications which did not need the disclosure of GPS location data was initially heralded as a breakthrough for privacy advocates. However, it has since emerged in certain jurisdictions that have used the open source code to develop their contact tracing apps (e.g., Denmark and Ireland) that in order for individual users to use the tracing application their GPS location must be turned on (Singer, 2020). This raises fundamental security and privacy concerns and has seen governments enter into dialogues with Google to determine why this data may be needed. Similarly, there may be technical considerations that Governments may need to be made aware of. For example, while the Irish contact tracing application has achieved strong performance to date, over 10% of users have deleted the application (Brennan, 2020). As well as privacy concerns, the public cited application performance issues as reasons for abandoning the tracing application e.g., the application was found to be draining mobile battery life (O'Brien, 2020a, 2020b). To both increase adoption and reduce abandonment, policymakers need to promote the adoption and use of contact tracing apps and communicate the benefits of continued use even where functionality and privacy concerns exist. In addition, when use is abandoned, specific intervention programmes need to be designed to reactivate former users, again emphasizing the benefits of participation. To be transparent with the public themselves, policymakers need to insist that the third parties that they rely upon for digital contact tracing are also transparent. Digital contact tracing is a complex chain of data and trust between governments, citizens, and technology providers. As well as privacy-preserving technologies, public education, and communication, the implementation of a transparent and integrated multi-stakeholder framework for assurance and accountability may provide a much needed series of controls to build trust between all stakeholders involved in digital contact tracing and repair trust in the event of a violation.

7. Limitations and future research directions

As with any study, there are several limitations which must be acknowledged. First, while this study assessed pre-adoption and post-adoption attitudes over a short time frame, it would be interesting to conduct follow up research to determine factors relating to discontinuance and re-engagement with COVID-19 mobile tracing technologies. In recent years, researchers have acknowledged the fact that initial adoption of a technology may not lead to ongoing continued usage (Bhattacherjee, 2001). This has resulted in a shift in focus towards understanding individuals' behaviors after the initial adoption of a new technology, often with an emphasis on understanding why individuals discontinue use (Polites & Karahanna, 2012; Recker, 2016). Second, this study focused solely on a COVID-19 mobile tracing decentralized application which was introduced by the Irish government voluntarily. There are also centralized mobile tracing technologies which are being introduced in countries such as France. While both instances of tracing technology use Bluetooth technology to log when contacts are close to each other, there are fundamental differences in the manner in which data is processed and stored. With the decentralized model, data is kept on users' phones, while the data in a centralized model is uploaded to a remote cloud server and used to identify other contacts should COVID-19 symptoms start to manifest. Future research could use this study as a theoretical base to examine citizens' privacy and benefit perceptions relating to centralized applications. There is emerging anecdotal evidence to suggest that centralized architectures are impeding adoption rates amongst citizens due to privacy and data management concerns (O'Brien, 2020a, 2020b). Thirdly, citizens' attitudes relating to the acceptance of COVID-19 tracing technologies in Ireland could be different from other countries. Future research could examine cross-country differences with regards to COVID-19 mobile tracing applications. Finally, given the breadth of variables considered within the privacy literature, it would not be possible to consider all potentially influential positive and negative beliefs and social factors within this context. Due to the focus on the trade-offs between positive and negative beliefs over time, the study does not consider potential antecedents to privacy concerns such as perceived sensitivity or the array of additional outcomes such as privacy-protective behaviors upon adoption. Such factors may further clarify the role of privacy in the contact tracing context as well as the broader government surveillance and mobile application contexts.

8. Conclusion

Research on citizens' acceptance of government surveillance technologies and the influence of privacy on this acceptance remains nascent, despite the continued growth in government investment in such technologies and the tendency to introduce these technologies during or following a crisis. The current study leverages the privacy calculus theory as an underlying theory and incorporates social exchange theory to determine how individuals' privacy concerns and their perceptions of benefits, reciprocity and social influence shape their acceptance of a government contact tracing application over time. The study highlights the important role of social influence and reciprocity in influencing acceptance of technologies which require mass acceptance and reciprocal information disclosure to be successful. The study also points to the temporal influence of privacy concerns highlighting the importance of addressing privacy both prior to and post introduction of new

technology to ensure citizen acceptance and reliance is achieved. The model can be extended to other contexts particularly the context of government surveillance technologies and location based and mobile health applications.

Credit author statement

Grace Fox: Conceptualization, Methodology, Formal analysis, Writing – draft and revised manuscript. Trevor Clohessy: Writing – draft and revised manuscript. Lisa van der Werff; Conceptualization, Writing – draft and revised manuscript, Pierangelo Rosati: Data curation, Writing – draft and revised manuscript, Theo Lynn; Data curation, Writing – draft and revised manuscript.

Acknowledgements

This work is funded by the Irish Institute for Digital Business.

Appendix A. All items

Construct	Item		Std. rwg	Mean	Std. Dev
Perceived Benefits (7 point agreement scale adapted from Li et al., 2014)	PerBen1	Using the COVID app would improve my access to my health information.	.888	4.27	1.75
	PerBen2	Using the COVID app would help me become more informed.	.896	4.57	1.73
	PerBen3	Using the COVID app would improve my ability to manage my health.	.939	4.17	1.75
	PerBen4	Using the COVID app would improve the quality of healthcare.	.877	4.21	1.79
	PerBen5	I would manage my health more effectively using the COVID app.	.917	3.93	1.75
Reciprocal Benefits (7 point agreement scale adapted from Hamari & Koivisto, 2015)	RecBen1	I believe that downloading the COVID app could be mutually helpful to myself and other people.	.964	5.02	1.74
	RecBen2	I believe my participation in the COVID app could be advantageous to me and other people.	.964	4.98	1.77
Social Influence (7 point agreement scale adapted from Venkatesh et al., 2003; Hamari & Koivisto, 2015)	SoInf1	People who influence my attitudes would recommend the COVID app.	.783	3.90	1.60
	SoInf2	People who are important to me would think positively of me using the COVID app.	.938	4.35	1.64
	SoInf3	People who I appreciate would encourage me to use the COVID app.	.947	4.30	1.65
	SoInf4	My friends would think using the COVID app is a good idea.	.866	4.41	1.61
Internet Privacy Concerns (7 point agreement scale adapted from Dinev & Hart, 2006)	PC1	I am concerned that the information I submit on mobile apps could be misused.	.785	5.43	1.23
	PC2	I am concerned that a person can find private information about me from mobile apps.	.812	5.38	1.34
	PC3	I am concerned about submitting information on mobile apps, because of what others might do with it.	.921	5.36	1.32
	PC4	I am concerned about submitting information on mobile apps, because it could be used in a way I did not foresee.	.912	5.49	1.26
Intention to adopt (7 point agreement scale adapted from Venkatesh et al., 2003)	Int1	I intend to download the COVID app when it becomes available.	.986	4.53	1.95
	Int2	I plan to download the COVID app when it becomes available.	.995	4.51	1.95
	Int3	I predict I will download the COVID app when it becomes available.	.972	4.53	1.97
Willingness to rely on app (7 point agreement scale based on Gillespie, 2003; McKnight et al., 2002)	Rely1	I would be willing to rely on the information and advice provided by the COVID app to keep me safe.	.940	4.53	1.81
	Rely2	I would be willing to rely on the COVID app to keep me informed.	.953	4.68	1.79
	Rely3	I feel I could count on the accuracy of the information and advice provided by the COVID app.	.909	4.40	1.76
Usage Intentions (T2) (7 point agreement scale based on Bhattacherjee, 2001 and Venkatesh et al., 2003)	Use1	I intend to download/keep using the app in the future.	.991	4.62	2.11
	Use2	I plan to download/keep using the app in the future.	.978	4.63	2.13
	Use3	I predict I will download/keep using the app in the future.	.989	4.63	2.14

References

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science, 347*(6221), 509–514.

Angst, C. M., & Agarwal, R. (2009). Adoption of electronic health records in the presence of privacy concerns: The elaboration likelihood model and individual persuasion. *MIS Quarterly, 33*(2), 339–370.

Anton, E., Kus, K., & Teuteberg, F. (2021). January). Is ethics really such a big deal? The influence of perceived usefulness of AI-based surveillance technology on ethical decision-making in scenarios of public surveillance. *Proceedings of the 54th Hawaii International conference on system sciences*.

Bandura, A. (1986). *Social foundations of thought and action: A social cognitive theory*. Englewood Cliffs, NJ, US: Prentice-Hall.

Bannister, F. (2005). The panoptic state: Privacy, surveillance and the balance of risk. *Information Polity, 10*(1), 65–78.

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*(2), 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*(7), 1038–1058.

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly*, 1017–1041.

Beldad, A., & Kusumadewi, M. C. (2015). Here's my location, for your information: The impact of trust, benefits, and social influence on location sharing application use among Indonesian university students. *Computers in Human Behavior, 49*, 102–110.

Benamati, J. H., Ozdemir, Z. D., & Smith, H. J. (2017). An empirical test of an antecedents–privacy concerns–outcomes model. *Journal of Information Science, 43*(5), 583–600.

Bhattacherjee, A. (2001). Understanding information systems continuance: An expectation-confirmation model. *MIS Quarterly*, 351–370.

Blau, P. M. (1964). *Exchange and power in social life*. Transaction Publishers.

Boulos, M. N. K., Brewer, A. C., Karimkhani, C., Buller, D. B., & Dellavalle, R. P. (2014). Mobile medical and health apps: State of the art, concerns, regulatory control and certification. *Online journal of public health informatics, 5*(3), 229.

Bowman, N. D., Westerman, D. K., & Claus, C. J. (2012). How demanding is social media: Understanding social media diets as a function of perceived costs and benefits–A rational actor perspective. *Computers in Human Behavior, 28*(6), 2298–2305.

Brennan, C. (2020). HSE's COVID-19 tracing app passes 1m downloads. Available: https://www.irishexaminer.com/news/arid-31010089.html.

Carter, L., & Bélanger, F. (2005). The utilization of e-government services: Citizen trust, innovation and acceptance factors. *Information Systems Journal, 15*(1), 5–25.

Chang, I. C., Chou, P. C., Yeh, R. K. J., & Tseng, H. T. (2016). Factors influencing Chinese tourists' intentions to use the taiwan medical travel app. *Telematics and Informatics, 33*(2), 401–409.

Chang, R. C. S., Lu, H. P., Yang, P., & Luarn, P. (2016). Reciprocal reinforcement between wearable activity trackers and social network services in influencing physical activity behaviors. *JMIR mHealth and uHealth, 4*(3), e84.
Chan, E. Y., & Saqib, N. U. (2021). Privacy concerns can explain unwillingness to download and use contact tracing apps when COVID-19 concerns are high. *Computers in Human Behavior*, 106718.
Choi, S. (2016). The flipside of ubiquitous connectivity enabled by smartphone-based social networking service: Social presence and privacy concern. *Computers in Human Behavior, 65*, 325–333.
Choi, B., Wu, Y., Yu, J., & Land, L. (2018). Love at first sight: The interplay between privacy dispositions and privacy calculus in online social connectivity management. *Journal of the Association for Information Systems, 19*(3), 124–151.
Church, E. M., Thambusamy, R., & Nemati, H. (2017). Privacy and pleasure: A paradox of the hedonic use of computer-mediated social networks. *Computers in Human Behavior, 77*, 121–131.
Cialdini, R. B. (2009). *Influence: Science and practice* (Vol. 4). Boston, MA: Pearson education.
Cialdini, R. B., & Goldstein, N. J. (2004). Social influence: Compliance and conformity. *Annual Review of Psychology, 55*, 591–621.
Crossler, R., & Posey, C. (2017). Robbing Peter to pay Paul: Surrendering privacy for security's sake in an identity ecosystem. *Journal of the Association for Information Systems, 18*(7), 2.
Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science, 10*(1), 104–115.
Culnan, M. J., & Bies, J. R. (2003). Consumer privacy: Balancing economic and justice considerations. *Journal of Social Issues, 59*(2), 323–342.
Dai, H., & Palvi, P. C. (2009). Mobile commerce adoption in China and the United States: A cross-cultural study. *ACM SIGMIS - Data Base: The DATABASE for Advances in Information Systems, 40*(4), 43–61.
Davazdahemami, B., Hammer, B., Kalgotra, P., & Luse, A. (2020). *From general to situational privacy concerns: A new mechanism to explain information disclosure in social networks*. Communications of the Association for Information Systems (in press), (in press).
Davenport, T., Prusak, L., Wills, G., Alani, H., Ashri, R., Crowder, R., et al. (1998). *Working knowledge*. Harvard Business School Press.
Deci, E. L. (1975). *Intrinsic motivation*. New York, NY: Plenum Press.
Dinev, T. (2014). Why should we care about privacy? *European Journal of Information Systems, 23*, 97–102.
Dinev, T., Bellotto, M., Hart, P., Russo, V., & Serra, I. (2006). Internet users' privacy concerns and beliefs about government surveillance: An exploratory study of differences between Italy and the United States. *Journal of Global Information Management, 14*(4), 57–93.
Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research, 17*(1), 61–80.
Dinev, T., Hart, P., & Mullen, M. R. (2008). Internet privacy concerns and beliefs about government surveillance–An empirical investigation. *The Journal of Strategic Information Systems, 17*(3), 214–233.
Emerson, R. M. (1962). Power-dependence relations. *American Sociological Review, 27*(1), 31–41.
Emerson, R. M. (1976). Social exchange theory. *Annual Review of Sociology, 2*(1), 335–362.
Fishbein, M., & Ajzen, I. (1975). *Intention and Behavior: An introduction to theory and research*. MA, USA: Addison-Wesley.
Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*(1), 39–50.
Fox, G. (2020). "To protect my health or to protect my health privacy?" A mixed-methods investigation of the privacy paradox. *Journal of the Association for Information Science and Technology*, 1–15.
Fox, G., & Connolly, R. (2018). Mobile health technology adoption across generations: Narrowing the digital divide. *Information Systems Journal, 28*(6), 995–1019.
Fox, G., & James, T. L. (2020). Toward an understanding of the antecedents to health information privacy concern: A mixed methods study. *Information Systems Frontiers*, 1–26.
Fox, G., Mooney, J., Rosati, P., Paulsson, V., & Lynn, T. (2018). *Towards an understanding of farmers' mobile technology adoption: A comparison of adoption and continuance intentions*. AMCIS.
Gaskin, J. (2019). *Data screening*. Date accessed: June 2, 2020, retrieved from http://statwiki.kolobkreations.com/index.php?title=Data_screening.
Gillespie, N. (2003). *'Measuring trust in working relationships: The behavioral trust inventory', paper presented at the academy of management conference* (Seattle, WA).
Guo, X., Sun, Y., Wang, N., Peng, Z., & Yan, Z. (2013). The dark side of elderly acceptance of preventive mobile health services in China. *Electronic Markets, 23*(1), 49–61.
Gutierrez, A., O'Leary, S., Rana, N. P., Dwivedi, Y. K., & Calle, T. (2019). Using privacy calculus theory to explore entrepreneurial directions in mobile location-based advertising: Identifying intrusiveness as the critical risk factor. *Computers in Human Behavior, 95*, 295–306.
Gu, J., Xu, Y. C., Xu, H., Zhang, C., & Ling, H. (2017). Privacy concerns for mobile app download: An elaboration likelihood model perspective. *Decision Support Systems, 94*, 19–28.
Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2010). *Multivariate data analysis, A global perspective*. New Jersey: Pearson Education.
Hallam, C., & Zanella, G. (2017). Online self-disclosure: The privacy paradox explained as a temporally discounted balance between concerns and rewards. *Computers in Human Behavior, 68*(1), 217–227.
Hamari, J., & Koivisto, J. (2015). Working out for likes: An empirical study on social influence in exercise gamification. *Computers in Human Behavior, 50*, 333–347.
Hoehle, H., Aloysius, J. A., Goodarzi, S., & Venkatesh, V. (2019). A nomological network of customers' privacy perceptions: Linking artifact design to shopping efficiency. *European Journal of Information Systems, 28*(1), 91–113.
Holmes, E. A., O'Connor, R. C., Perry, V. H., Tracey, I., Wessely, S., Arseneault, L., & Ford, T. (2020). Multidisciplinary research priorities for the COVID-19 pandemic: A call for action for mental health science. *The Lancet Psychiatry, 7*(6), 547–560.
Homans, G. (1958). Social behavior as exchange. *American Journal of Sociology, 63*(6), 597–606.
Jozani, M., Ayaburi, E., Ko, M., & Choo, K. K. R. (2020). Privacy concerns and benefits of engagement with social media-enabled apps: A privacy calculus perspective. *Computers in Human Behavior, 107*, 106260.
Keith, M. J., Thompson, S. C., Hale, J., Lowry, P. B., & Greer, C. (2013). Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior. *International Journal of Human-Computer Studies, 71*(12), 1163–1173.
Kim, D., Park, K., Park, Y., & Ahn, J. H. (2019). Willingness to provide personal information: Perspective of privacy calculus in IoT services. *Computers in Human Behavior, 92*, 273–281.
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), 45–81.
Krishen, A. S., Raschke, R. L., Close, A. G., & Kachroo, P. (2017). A power-responsibility equilibrium framework for fairness: Understanding consumers' implicit privacy concerns for location-based services. *Journal of Business Research, 73*, 20–29.
Kumar, M., Raju, K. S., Kumar, D., Goyal, N., Verma, S., & Singh, A. (2021). An efficient framework using visual recognition for IoT based smart city surveillance. *Multimedia Tools and Applications*, 1–19.
Laufer, R. S., & Wolfe, M. (1977). Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of Social Issues, 33*(3), 22–42.
Li, Y. (2012). Theories in online information privacy research: A critical review and an integrated framework. *Decision Support Systems, 54*(1), 471–481.
Li, H., Gupta, A., Zhang, J., & Sarathy, R. (2014). Examining the decision to use standalone personal health record systems as a trust-enabled fair social contract. *Decision Support Systems, 57*, 376–386.
Li, J., Sellis, T., Culpepper, J. S., He, Z., Liu, C., & Wang, J. (2017). Geo-social influence spanning maximization. *IEEE Transactions on Knowledge and Data Engineering, 29*(8), 1653–1666.
Li, T., & Slee, T. (2014). The effects of information privacy concerns on digitizing personal health records. *Journal of the Association for Information Science and Technology, 65*(8), 1541–1554.
Li, H., Wu, J., Gao, Y., & Shi, Y. (2016). Examining individuals' adoption of healthcare wearable devices: An empirical study from privacy calculus perspective. *International Journal of Medical Informatics, 88*, 8–17.
Lyon, D. (2001). *Surveillance society: Monitoring everyday life*. UK): McGraw-Hill Education.
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*(2), 293–334.
Marakhimov, A., & Joo, J. (2017). Consumer adaptation and infusion of wearable devices for healthcare. *Computers in Human Behavior, 76*, 135–148.
Markus, M. L., & Keil, M. (1994). If we build it, they will come: Designing information systems that people want to use. *MIT Sloan Management Review, 35*(4), 11.
McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information Systems Research, 13*(3), 334–359.
Miltgen, C. L., & Smith, H. J. (2015). Exploring information privacy regulation, risks, trust, and behavior. *Information & Management, 52*(6), 741–759.
Miltgen, C. L., & Smith, H. J. (2019). Falsifying and withholding: Exploring individuals' contextual privacy-related decision-making. *Information Management, 56*(5), 696–717.
Min, J., & Kim, B. (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.
Morosan, C., & DeFranco, A. (2015). Disclosing personal information via hotel apps: A privacy calculus perspective. *International Journal of Hospitality Management, 47*, 120–130.
Nam, T. (2018). Untangling the relationship between surveillance concerns and acceptability. *International Journal of Information Management, 38*(1), 262–269.
Nam, T. (2019). What determines the acceptance of government surveillance? Examining the influence of information privacy correlates. *The Social Science Journal, 56*(4), 530–544. https://doi.org/10.1016/j.soscij.2018.10.001
O'Brien, C. (2020). *Google to roll out software fix to remedy issue with Covid app*. Retrieved from https://www.irishtimes.com/business/technology/google-to-roll-out-software-fix-to-remedy-issue-with-Covid-app-1.4325981.
O'Brien, C. (2020). *France offers a case study in the battle between privacy and coronavirus tracing apps*. Retrieved from https://venturebeat.com/2020/05/18/france-offers-a-case-study-in-the-battle-between-privacy-and-coronavirus-tracing-apps/.
Parker, M. J., Fraser, C., Abeler-Dörner, L., & Bonsall, D. (2020). Ethics of instantaneous contact tracing using mobile phone apps in the control of the COVID-19 pandemic. *Journal of Medical Ethics*, 1–5.
Pavlou, P. A. (2011). State of the information privacy literature: Where are we now and where should we go? *MIS Quarterly*, 977–988.

Pavlou, P. A., & Fygenson, M. (2006). Understanding and predicting electronic commerce adoption: An extension of the theory of planned behavior. *MIS Quarterly*, 115–143.
Pentina, I., Zhang, L., Bata, H., & Chen, Y. (2016). Exploring privacy paradox in information-sensitive mobile app adoption: A cross-cultural comparison. *Computers in Human Behavior, 65*, 409–419.
Pietrobelli, A., Pecoraro, L., Ferruzzi, A., Heo, M., Faith, M., Zoller, T., & Heymsfield, S. B. (2020). *Effects of COVID-19 lockdown on lifestyle behaviors in children with obesity living in Verona, Italy: A longitudinal study*. Obesity.
Polites, G. L., & Karahanna, E. (2012). Shackled to the status quo: The inhibiting effects of incumbent system habit, switching costs, and inertia on new system acceptance. *MIS Quarterly, 36*(1), 21–42.
Posey, C., Lowry, P. B., Roberts, T. L., & Ellis, T. S. (2010). Proposing the online community self-disclosure model: The case of working professionals in France and the UK who use online communities. *European Journal of Information Systems, 19*(2), 181–195.
Queiroz, M. M., & Wamba, S. F. (2019). Blockchain adoption challenges in supply chain: An empirical investigation of the main drivers in India and the USA. *International Journal of Information Management, 46*, 70–82.
Raykov, T. (1997). Estimation of composite reliability for congeneric measures. *Applied Psychological Measurement, 21*(2), 173–184.
Recker, J. C. (2016). Reasoning about discontinuance of information system use. *Journal of Information Technology Theory and Application, 17*(1), 41–66.
Reddick, C. G., Chatfield, A. T., & Jaramillo, P. A. (2015). Public opinion on national security agency surveillance programs: A multi-method approach. *Government Information Quarterly, 32*(2), 129–141.
Saadé, R. G., & Otrakji, C. A. (2007). First impressions last a lifetime: Effect of interface type on disorientation and cognitive load. *Computers in Human Behavior, 23*(1), 525–535.
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. https://doi.org/10.1109/TEM.2020.3019033. In press.
Shiau, W. L., & Luo, M. M. (2012). Factors affecting online group buying intention and satisfaction: A social exchange theory perspective. *Computers in Human Behavior, 28*(6), 2431–2444.
Singer, N. (2020). *Google promises privacy with virus app but can still collect location data*. Retrieved from https://www.nytimes.com/2020/07/20/technology/google-covid-tracker-app.html.
Slobogin, C. (2008). *Privacy at risk: The new government surveillance and the Fourth Amendment*. University of Chicago Press.
Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly*, 989–1015.
Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly*, 167–196.
Straub, D., Boudreau, M.-C., & Gefen, D. (2004). Validation guidelines for IS positivist research. *Communications of the Association for Information Systems, 13*(1), 24.
Sun, Y., Wang, N., Shen, X. L., & Zhang, J. X. (2015). Location information disclosure in location-based social network services: Privacy calculus, benefit structure, and gender differences. *Computers in Human Behavior, 52*, 278–292.
Sweeney, Y. (2020). Tracking the debate on COVID-19 surveillance tools. *Nature Machine Intelligence, 2*(6), 301–304.
Thompson, N., McGill, T., Bunn, A., & Alexander, R. (2020). Cultural factors and the role of privacy concerns in acceptance of government surveillance. *Journal of the Association for Information Science and Technology, 71*(9), 1129–1142.
Trepte, S., Scharkow, M., & Dienlin, T. (2020). The privacy calculus contextualized: The influence of affordances. *Computers in Human Behavior, 104*, 106115.
Trüdinger, E. M., & Steckermeier, L. C. (2017). Trusting and controlling? Political trust, information and acceptance of surveillance policies: The case of Germany. *Government Information Quarterly, 34*(3), 421–433.
Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly, 27*(3), 425–478.
Venkatesh, V., Thong, J. Y., Chan, F. K., & Hu, P. J. (2016). Managing citizens' uncertainty in e-government services: The mediating and moderating roles of transparency and trust. *Information Systems Research, 27*(1), 87–111.
Venkatesh, V., Thong, J. Y., & Xu, X. (2012). Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology. *MIS Quarterly*, 157–178.
Wang, X., & Liu, Z. (2019). Online engagement in social media: A cross-cultural comparison. *Computers in Human Behavior, 97*, 137–150.
Wang, Y., & Midha, V. (2012). *User self-disclosure on health social networks: A social exchange perspective*. ICIS 2012 Proceedings.
Wang, H., Tao, D., Yu, N., & Qu, X. (2020). Understanding consumer acceptance of healthcare wearable devices: An integrated model of UTAUT and TTF. *International Journal of Medical Informatics, 139*, 104–156.
Whelan, E., & Clohessy, T. (2020). *How the social dimension of fitness apps can enhance and undermine wellbeing*. Information Technology & People.
Wirth, J. (2018). January. Dependent variables in the privacy-related field: A descriptive literature review. In *Proceedings of the 51st Hawaii International Conference on system sciences*.
World Health Organization. (2005). *International health regulations* (2nd ed.) Geneva; Retrieved from https://www.who.int/ihr/publications/9789241580496/en/.
World Health Organization. (2020). *Ethical considerations to guide the use of digital proximity tracing technologies for COVID-19 contact tracing*. Retrieved from https://www.who.int/publications/i/item/WHO-2019-nCoV-Ethics_Contact_tracing_apps-2020.1.
Wu, J. H., Wang, S. C., & Lin, L. M. (2007). Mobile computing acceptance factors in the healthcare industry: A structural equation model. *International Journal of Medical Informatics, 76*(1), 66–77.
Xu, H., Dinev, T., Smith, H. J., & Hart, P. (2008). Examining the formation of individual's privacy concerns: Toward an integrative view. *ICIS 2008 proceedings*, 6.
Xu, H., & Gupta, S. (2009). The effects of privacy concerns and personal innovativeness on potential and experienced customers' adoption of location-based services. *Electronic Markets, 19*(2–3), 137–149.
Xu, H., Teo, H. H., Tan, B. C., & Agarwal, R. (2012). Research note—effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: A study of location-based services. *Information Systems Research, 23*(4), 1342–1363.
Yasaka, T. M., Lehrich, B. M., & Sahyouni, R. (2020). Peer-to-Peer contact tracing: A privacy-preserving smartphone application. *Journal of Medical Internet Research, 8*(4). https://doi.org/10.2196/18936
Young, H. P. (2009). Innovation diffusion in heterogeneous populations: Contagion, social influence, and social learning. *The American Economic Review, 99*(5), 1899–1924.
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 & Management, 56*(4), 570–601.
Zastrow, M. (2020). Coronavirus contact-tracing apps: Can they slow the spread of COVID-19? *Nature*. https://doi.org/10.1038/d41586-020-01514-2. Available: https://www.nature.com/articles/d41586-020-01514-2. In press.
Zhou, T. (2013). Examining continuous usage of location-based services from the perspective of perceived justice. *Information Systems Frontiers, 15*(1), 141–150.
Zhou, T., & Li, H. (2014). Understanding mobile SNS continuance usage in China from the perspectives of social influence and privacy concern. *Computers in Human Behavior, 37*, 283–289.