Technology in Society 78 (2024) 102616

Contents lists available at ScienceDirect

Technology in Society

journal homepage: www.elsevier.com/locate/techsoc

The privacy calculus in the context of novel health technology for diagnosing and tracking infectious diseases: The role of disease severity and technology's evidence base for effectiveness in adoption and voluntary health data-sharing

M.S. Frangopoulou [a,1], L.N. van der Laan [a,*,1], W. Ebbers [b]

[a] Department of Communication and Cognition, Tilburg University, the Netherlands
[b] Erasmus School of Social and Behavioural Sciences, Erasmus University Rotterdam, the Netherlands

ARTICLE INFO

Keywords:
e-health
Acceptance
Novel technologies
Infectious disease
Privacy calculus

ABSTRACT

In the past decades, accelerated by the recent COVID pandemic, the field of healthcare has faced technological advancements, such as wearables and mobile applications, that collect personal or health data. However, such tools are ineffective if they are not adopted by a large part of the population or if relevant health data, collected by the application, are not (voluntarily) shared. This study assessed the role of disease severity and evidence base for the effectiveness of the technology in the Privacy Calculus risk-benefit trade-off to contribute or hinder technology acceptance and data sharing. A large-scale 2 × 2 × 2 online vignette experiment (n = 822) was carried out, where participants were presented with a hypothetical scenario describing a novel health technology for diagnosing and tracking of infectious diseases. The results indicated that participants' privacy concerns negatively affected their intention to use the technology and willingness to share data, and that a high severity of the disease weakened this relationship. None of the other expected effects on intentions to use, willingness to share data or privacy concerns, were significant. These findings highlight the role of privacy as a barrier to technology acceptance, and suggest disease severity plays a role in the Privacy Calculus risk-benefit trade off by weakening the negative effect of privacy concerns on adoption in contexts where disease severity is high.

1. Introduction

Over the years, an increase in the use of novel technologies in the field of healthcare, and more particularly, infectious diseases, has been observed [1]. Some examples include the use of Artificial Intelligence for surgeries and outbreak tracing [2,3], and light-based technologies to reduce transmission of infections [4,5]. An example of novel technology for combatting infectious diseases implemented in the recent COVID-19 pandemic are contact tracing applications (CTAs), used to notify people when they have been in close proximity with infected individuals, thereby aiming to reduce the spread of the virus [6]. Technologies that enable disease diagnosis and tracking, which play a pivotal role in surveillance, prevention, and curtailing disease transmission, are currently focal points of development within the academic field of health technology, specifically concerning infectious diseases (e.g., Ref. [7,8]). To ensure the exertion of these technologies' health-promoting effects, their acceptance and adoption by the target group, or even the whole population is crucial.

Several of these novel technologies collect and utilize users' personal or health data, e.g., infection status, raising various concerns regarding the data privacy that they provide. In addition, the introduction of these technologies is often accompanied by public debates about privacy, e.g., in the case of CTAs, experts questioned the privacy of such applications in the media, thereby shaping citizen's privacy perceptions about health technologies [9,10]. Past research has consistently shown that privacy concerns negatively influence technology acceptance (e.g., Ref. [11,12]). For a particular service, users or consumers tend to evaluate whether the risks of disclosing personal data outweigh the benefits of using the service [13,14]. This idea of a risk-benefit analysis is proposed in the Privacy Calculus Theory (PCT), introduced by Laufer & Wolfe

* Corresponding author.
E-mail address: l.n.vdlaan@tilburguniversity.edu (L.N. van der Laan).
[1] These authors contributed equally.

https://doi.org/10.1016/j.techsoc.2024.102616
Received 8 September 2023; Received in revised form 28 May 2024; Accepted 28 May 2024
Available online 31 May 2024

[15], and carries a heavy weight with regards to individuals' willingness to share (health) data and thus the use of technologies utilizing this data. There is extensive support for this theory, for instance, in the context of healthcare wearable devices [16] and even regarding CTA adoption [17]. Individuals' perceptions on the risks and benefits of partially giving up their privacy is influenced by several factors, which in turn influence their decision to employ the technology.

There appear to be at least three gaps in our knowledge of the privacy calculus in the domain of novel health technology for diagnosing and tracking of infectious diseases. First, little is known about how contextual, e.g., contemporary disease risk, and technology-specific factors, e.g., the evidence base for the effectiveness of the technology, affect the risk-benefit trade-off. An important characteristic of the COVID-19 pandemic was that infection rates and health damage resulting from an infection fluctuated heavily over the course of the pandemic, depending on other measures taken to reduce the spread and the subtype of the virus roaming around in the population at that moment in time. The perceived potential benefits of using the technology may be higher if the risk of health damage of the infectious disease is high, since using the technology in that context may potentially result in a greater reduction of health damage. Although there are studies on the direct effect of (perceived) disease severity on intention to use health technologies [18], its influence on the risk-benefit trade-off as explained by the PCT is still unknown. It is still unclear whether privacy concerns affect adoption of novel technologies less when disease severity is high, and thus when using the technology may have larger potential benefits.

A distinctive attribute of emerging healthcare technologies aimed at mitigating infectious diseases lies in their pre-emptive introduction, often preceding the establishment of unequivocal efficacy, owing to the urgency of minimizing public health damage. For instance, the adoption of Bluetooth technology for contact tracing during the COVID-19 pandemic represented a novel approach, yet its tangible contributions to virus mitigation remained uncertain at the moment of introduction. Although computer simulations indicated potential efficacy [19], comprehensive empirical studies were lacking. The perceived potential benefits may be perceived as higher or at least surer if the evidence base for effectiveness is more robust – if it has been proven that using the technology actually contributes to the problem it is designed to solve. Although there is evidence for the direct effect of perceived effectiveness (e.g., Performance expectancy, from the Unified Theory of Acceptance and Use of Technology - UTAUT) driving intentions to adopt novel technologies [16], there is a gap in the literature concerning this variable's effect on the risk-benefit trade-off. It is still unclear whether privacy concerns affect adoption of novel technologies less when the potential benefit is more certain.

Considering the apparent connection between concerns about privacy and the willingness to adopt technology, coupled with the absence of comprehensive understanding regarding the factors influencing this connection, the first research question (RQ1) of this study was: *How do privacy concerns affect usage intention of novel technology, and is this relationship moderated by the severity of the disease and/or evidence base for the effectiveness of the technology?*

A second knowledge gap pertains to the motivations underlying the voluntary contribution of data within the healthcare realm. In the contemporary digital health landscape, data holds significant value or is even denoted as 'the new gold' (e.g., Ref. [20]), being sought after by companies for training artificial intelligence models and enhancing health-related applications. Furthermore, government's access to (infection) data is crucial for endeavours such as contact tracing apps to combat viral outbreaks more effectively [19]. In the backdrop of more stringent regulations governing data collection and utilization (e.g., GDPR), the notion of voluntary data donation has emerged as a pivotal subject, constituting a customizable feature within technological interfaces. Several novel health technologies afford users the ability to exert control over their personal and health-related data. A notable illustration is the case of Ireland's CTA Covid Tracker, which granted users full autonomy over their personal information and app usage, without imposing obligatory data disclosure [64]. As posited by the PCT, the decision to share (personal or health) data is influenced by a deliberation of the risks and benefits associated with sharing this information. Though it has been shown that privacy risks negatively impact users' willingness to share data [21], the factors potentially serving as a benefit, remain inadequately explored in relation to voluntary data donation. The current study will investigate how the aforementioned contextual, i.e., contemporary disease risk, and technology-specific factors, i.e., the evidence base for the effectiveness of the technology, affect the willingness to share data. To the researchers' knowledge, no previous study has investigated if individuals are more willing to share their data when disease severity is high. Heightened disease severity might lead users to view data sharing as a requisite for ensuring the effective operation of interventions, thus potentially motivating greater willingness to disclose data. Further, there's a lack of studies investigating how a technology's efficacy affects data donation, though there is some limited evidence that performance expectancy positively affects it [16], suggesting a second research question (RQ2): *How do disease severity and evidence base for effectiveness of a technology influence individuals' willingness to share data?*

A third knowledge gap pertains to the effects of the possibility of voluntary data sharing on privacy concerns. As previously mentioned, an increasing amount of digital health applications implements voluntary data sharing as a customizable feature but the effect of this possibility on privacy concerns is yet to be examined. According to Deci and Ryan's [22] Self Determination Theory (SDT), motivation can either be *autonomous* or *controlled*: while autonomous motivation is self-determined, controlled motivation stems from a feeling of guilt or reward [23]. This suggests that users of a technological device who are given the option to share their personal data, rather than simply be informed of the data collection, may feel a greater sense of autonomy and control over their personal information, which may in turn lower their privacy concerns. Therefore, the third research question (RQ3) was: *How does having the option of voluntarily sharing the data (as compared to mandatory data sharing) affect privacy concerns?*

2. Theoretical framework

2.1. Privacy calculus theory

Privacy concerns play a major role in the acceptance of and intention to use (novel) technologies. Privacy has been defined as a person's right "to decide what information about himself should be communicated to others and under what condition" ([24], p.10). In relation to this, the PCT by Laufer and Wolfe [15] describes individuals' thought processes when required to disclose personal information: when this situation occurs, attempts are made to determine whether the benefit of sharing such information will outweigh the risks of disclosing it [25]. While the risks entail the loss of privacy, benefits concern individuals' expectations of what they might receive in exchange of giving up on their privacy. This reluctance of sharing private data stems from the perceived privacy risk, influenced by, for instance, a high perceived ownership of personal information [26]. Furthermore, the hesitation to use a technology due to its perceived privacy risk being considered greater than the benefit of using it, highlights the important role of privacy concerns on technology acceptance [27]. Other qualitative studies have emphasized the strong effect of privacy concerns on the acceptance of these technologies [11,17].

Various studies investigating, for instance, user engagement and anticipated benefits of health technologies, have provided support for the risk-benefit trade-off, as described by the PCT [14,28]. Individuals who feel threated that their privacy is being compromised tend to be more reluctant to adopt a specific technology [11], as they conclude that the risks of using the technology outweigh the benefits. There has been extensive literature on the negative effect of privacy concerns on the

adoption of technologies in the healthcare sector, particularly in the implementation of new technologies [11], on (AI-based) CTAs [17,28], or health wearables [29]. The PCT is particularly relevant in explaining intention to adopt in the context of these novel health technologies, because the usage of the technology assimilates with the decision to disclose data: the main functionality of the technology relies on the data provided by the user. For instance, in teledermatology, (eHealth) apps are used by individuals at home to automatically evaluate photographs of skin lesions and calculate the likelihood of malignant conditions (e.g., skin cancer) (e.g., Young et al., 2020). Pertaining to infectious diseases, many COVID-19 contact tracing apps' main functionality depended on the sharing of Bluetooth codes that enabled the contact tracing (though these codes were anonymised, people perceived the data collected by the app as personal; [10]). Hence, the first hypothesis, replicating these aforementioned studies, reads:

H1. Privacy concerns negatively relate to intention to use the novel health technology.

2.2. Factors affecting the relationship between privacy concerns and intention to use the technology

The above section provided support for a (negative) relationship between privacy concerns and the intention to use the novel technology. In this study, contextual and technology-specific factors that may affect the risk-benefit trade off as coined by PCT, and thus may moderate the relationship between privacy concerns and intention to use the proposed technology are examined.

In the current study the first – contextual – variable focused on regarding this trade-off is disease severity, i.e., whether the infection or disease can cause severe damage to one's health. There is support for the positive effect of perceived severity of a disease on the perceived benefits of using a CTA [28]. Furthermore, a study on COVID-19 revealed that a disease's perceived severity significantly affected the intention to use a CTA to help prevent the spread of the infection [30], though null findings have also arisen [31]. Combining these findings, an increased disease severity could increase the perceived benefits thereby contributing to the benefit-side of the risk-benefit analysis as explained in the PCT, thereby also weakening the relationship between privacy concerns and intention to use.

The second – technology-specific – variable studied in this study was evidence base for effectiveness of the technology. Specifically, whether there is (empirical) support that the technology performs its task successfully. Linking this variable to the UTAUT's PE since a technology with strong support for its effectiveness will most likely meet users' expectations (i.e., yield a high PE), there is support for PE's positive effect on trust of the technology [32,33]. In addition, there is evidence for the negative role of users' trust (in a technology) on perceived privacy risk [13], implying that a trusted technology may be contribute as a potential benefit in individuals' risk-benefit analysis. This suggests that a strong evidence base for the effectiveness of the technology may also contribute as a benefit, thereby influencing the tradeoff and weakening the negative relationship between privacy concerns and intention to use this technology.

In sum, the PCT provides support for the moderating effect of these two variables, as there is potential for their contribution to the risk-benefit tradeoff. A high disease severity could alarm individuals, and a strong evidence base could make users more trusting of the technology, thereby increasing the perceived benefit of the application. As such, the moderating effect of these variables on the effects of privacy concerns on adoption would reflect this specific trade-off, i.e., if benefits are high, the weight of risks is lower for adoption intention than when benefits are low. This is in line with previous PCT conceptualisations involving the benefits' moderating effects of privacy on disclosure-related outcomes; e.g., Ref. [21]). Following this line of reasoning, a high disease severity or a strong evidence base could increase the perceived benefit of using the technology, and thus make privacy concerns weigh less in the risk-benefit tradeoff. Therefore:

H2. The association between privacy concerns and intention to use the novel health technology is weaker when disease severity is high compared to low.

H3. The association between privacy concerns and intention to use the novel health technology is weaker for technology with a strong compared to low evidence base for effectiveness.

2.3. Factors affecting users' willingness to share data

Various factors may contribute to users' willingness to disclose personal information. A prevailing concept in the literature on privacy is the privacy paradox: while individuals may be aware of their personal information being at risk, no measures are taken to protect their privacy, as mentioned by Barth & De Jong [34] in their review article on this concept. This theory strongly relates to Wirth and colleagues' [68] concept of resignation, a study on SNS which revealed that in some situations, individuals tend to "resign" from their privacy concerns, and accept that by disclosing information, they are fully vulnerable to risking their privacy. Furthermore, the PCT should also be addressed, as individuals perform a risk-benefit analysis to evaluate whether they will benefit from sharing their data with the government. Based on these concepts, it is hypothesized that disease severity and evidence base for effectiveness may affect users' protective attitude towards their personal information.

Indeed, these two factors may affect the risk-benefit tradeoff by positively influencing the benefits, in a similar vein as described in the previous section for intention to use the technology. A few studies are relevant specifically regarding the voluntary decision to share data. For disease severity there is evidence from studies on mobile health services that there is a positive effect of perceived benefits (i.e., (health) benefits of using the mobile health application) on users' intention to upload personal data [35,36]. Similar inferences could be made for the evidence base of effectiveness. If there is support for the effectiveness of the novel technology (i.e., high PE), users may be more convinced of its ability to diagnose the disease, and perhaps develop a more positive attitude towards sharing their personal information. There is support for this inference, as PE has been found to have a positive effect on intention to disclose personal information [16]. Another study on digital services located in airports also discovered that perceived benefits are a requirement in order for passengers to be willing to disclose personal information [37]. Even though this study assessed the effect of the benefits of sharing data in a different domain, similar effects may be expected for the health domain. Therefore, based on the theory and the empirical findings described above, the following hypotheses are proposed:

H4. Willingness to share data collected by a novel health technology is higher when the disease severity is high compared to low.

H5. Willingness to share data collected by a novel health technology, is higher when the evidence base of effectiveness is strong compared to weak.

2.4. Voluntary versus mandatory sharing of users' data with the government

A great source of privacy concerns stems from users' lack of knowledge on the handling of their personal information, particularly in terms of how it is collected and who may access it [27]. By providing individuals an option to voluntarily share their data or not, users are given control over their own data which may increase a sense of autonomy. Deci and Ryan's SDT [22], which makes the distinction between *extrinsic* (i.e., driven by reward and punishment) and *intrinsic* motivation (i.e., driven by enjoyment), supports that, in order for

intrinsic motivation to be acquired, three needs must be fulfilled: *autonomy*, *relatedness*, and *competence*. Drawing on this theory, autonomy caused by users' feeling of control and of being capable of performing an action of their own volition could lead to weaker privacy concerns. Furthermore, autonomous individuals may experience a feeling of integrity, as they perceive authenticity in their actions [38]. These positive feelings, caused by autonomy (i.e., in this context, voluntary data disclosure) could perhaps also contribute to a decrease in privacy concerns.

Although the empirical support on mandatory versus voluntary information disclosure is limited, a study involving focus groups revealed that participants expressed concerns regarding unwanted information dissemination [27], emphasizing the user's need for control over their data on privacy concerns. Moreover, a mixed-methods study on health technologies revealed that participants wished to have complete control over the type of data shared with the government, or that at least solely medical information relevant to their care should be collected [39]. As some of these participants voiced their concerns regarding unauthorized use of their data [39], perhaps more control would lower these concerns. Therefore:

H6. Possibility for voluntary data-sharing leads to lower privacy concerns in comparison to mandatory data-sharing.

Based on these hypotheses, the following conceptual framework has been created:

3. Method

3.1. Design

The data used for this manuscript was part of a larger 3x2x2x2 between-subjects experimental study. Data was collected in the context of a collaboration with the Dutch Ministry of Health, Welfare and Sports. The experimental factors of the original study consisted of: **evidence base** for the effectiveness of technology (*strong* versus *weak*), **data-sharing option** (*voluntary* versus *mandatory*), **disease severity** (*high* versus *low*), and **application goal of the technology** (*prediction* versus *tracing* versus *prevention*). Based on these factors, a total of 24 experimental conditions were created and randomly allocated to participants. Random allocation was employed to obtain an even distribution of participants among the conditions.

For this manuscript, only the first three experimental factors were used in the analyses, resulting in a $2 \times 2 \times 2$ between-subjects design, consisting of **evidence base for effectiveness, data sharing option,** and **disease severity**.[2] The manipulation of the experimental factors was performed through fictive, yet realistic scenarios (i.e., vignettes, for more details regarding the vignettes can be found in section 3.1.1, Table 2). A vignette study is regarded as a useful approach in the healthcare domain, as it provides insight on causal relationships between variables [40]. Furthermore, to provide an answer to the RQs, the following variables were measured: **privacy concerns**, **intention to use** the technologyand **willingness to share data** (section 3.5 describes the measurement of these variables).

The study was approved by the Ethical Review Board of the Tilburg School of Humanities and Digital Sciences (Tilburg University) under file number 2022.71.

[2] The fourth factor (i.e., goal of technology), was considered to be out of scope for this particular study, as, it was not expected to relate to the privacy context of this study. To confirm if this variable would affect the reported results, additional analyses were performed (Supplement F). Results for all other variables were unaffected by adding these predictors to the models.

3.2. Participants

A total of 842 participants were recruited via PanelClix, a Dutch panel via which users can participate online in various studies in exchange of rewards. To yield a representative sample of the Dutch population, quota were employed to ensure a sample distribution representative to the Dutch population in terms of gender, age, and educational level (Supplement A). In addition, participants were a) over 16 years of age, and b) Dutch speakers, as the survey was conducted in Dutch. Participants had to indicate their consent and were informed about their right to withdraw from the study at any time or to request their data to be removed. Lastly, participants were rewarded for their time by receiving an amount of the panel's credits based on the study's duration.

Prior to the data processing, respondents who had chosen not to answer at least one of the statements used for this study were removed from the study ($n = 17$), Participants who requested to have their data deleted were also removed ($n = 3$), resulting in a final sample size of 822. The clean dataset revealed a relatively balanced sample in terms of gender, with 50.2 % females ($n = 413$) and 49.8 % males ($n = 409$). Further statistics regarding age and educational level can be found in Table 1.

3.3. Materials

The online experiment was created in Qualtrics, a survey-making interface that ensures that data collection adheres to GDPR, and was subsequently launched on PanelClix.

3.3.1. Vignettes

The experimental manipulations were implemented in fictive scenarios, describing a future situation in which a new virus had appeared. The scenario included a general description of the future (pandemic situation) which was the same for all scenarios, followed by sections explaining the disease severity (varied depending on the condition), a general description of the novel technology and its features (i.e., a toothbrush with sensors), the data-sharing options, (varied depending on the condition), the application goal of the technology (varied depending on the condition), and evidence-base for effectiveness of the technology (varied depending on the condition). Based on the design (i.e., $2 \times 2 \times 2$) employed in this study, a total of 8 scenarios were compared. For each experimental factor different version of particular sections were formulated for the different levels of the factor. Care was taken that all scenario descriptions were of approximately the same length (approximately 170 words). The text used in the study was of Dutch B1 level according to the Common European Framework of Reference (CEFR), and the grammatical structure of the condition description was simple enough to be understood by participants from all demographic categories. Table 2 shows the structure and the specific statements (in English) used for the scenarios. The Dutch versions of the vignettes can be found in the Supplemental materials (Supplement B) and in the project folder on the Open Science Framework (link: https://osf.io/wtkcq/).

A scenario of a virus spreading all over the world that spreads through contact with others or through air was employed in the study because this is a situation highly similar to the coronavirus. It was anticipated that for this reason, it would constitute a credible future scenario for the participants. The particular technology presented in the scenario, i.e., a toothbrush that measures virus particles in saliva and that notifies the user of an infection, was employed because such toothbrushes do not exist yet and could credibly be denoted as a novel technology. Still, its function had a high similarity to the traditional self-tests employed during the corona pandemic which people could use at home to test if they were infected with the corona virus. Therefore, it was anticipated that this functionality would be perceived as plausible. The scenario entailed the collection of health data because health data is

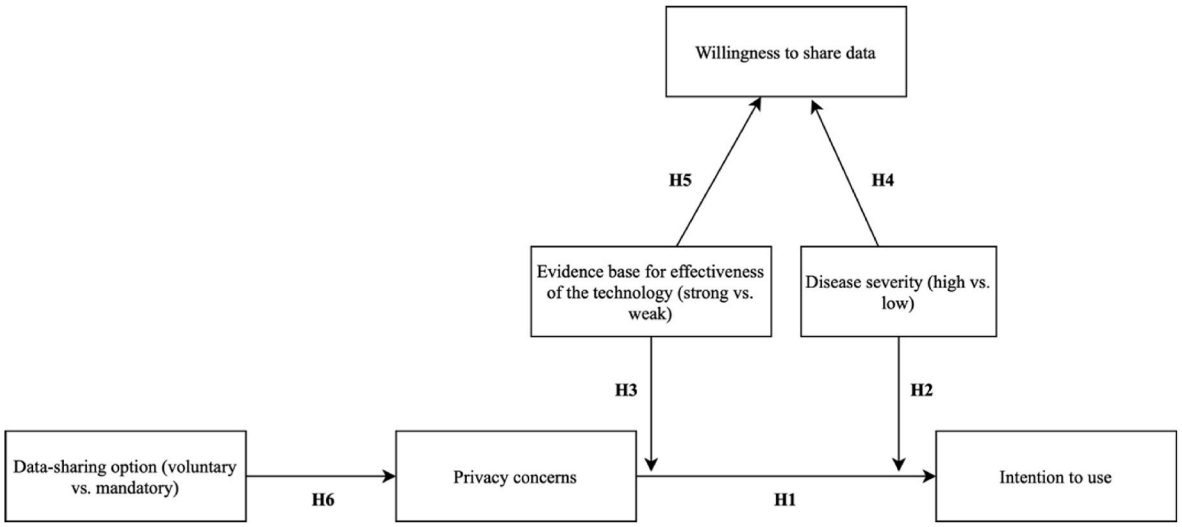

Fig. 1. Figure depicting the conceptual model.

Table 1
Demographic characteristics of the sample.

Variable	Category	Number	Percentage
Gender	Male	409	49.8 %
	Female	413	50.2 %
Age	16–25	85	10.3 %
	26–35	195	23.7 %
	36–45	134	16.3 %
	46–55	126	15.3 %
	56–65	128	15.6 %
	66–75	108	13.1 %
	>76	45	5.5 %
	Prefer not to say	1	0.1 %
Education	Elementary school	28	3.4 %
	Pre-vocational education	188	22.9 %
	Secondary education	89	10.8 %
	Vocational education levels 2-4	224	27.3 %
	Higher professional education	210	25.5 %
	Scientific education or higher	83	10.1 %

a special category of personal data within GDPR, with specific safeguards, and the collection and use of it would be expected to result in significant privacy concerns. Yet, the scenario described that health data would be anonymously collected similar as with CTAs implemented during the corona pandemic, thereby increasing the credibility of the scenario. The credibility of the scenario's employed in the current study was assessed and reported (see results section Randomization and credibility checks).

3.4. Procedure

After logging into PanelClix and selecting the study, participants were redirected to the Qualtrics environment where an information letter was presented to them, and an informed consent form. After providing consent, participants answered questions about demographic demographics (gender, age, educational level). Next, participants were exposed to a randomly allocated fictive scenario, as described in the "Vignettes" section. After this, participants answered questions about technology acceptance, intention to use and other constructs from the Unified Theory of Use and Acceptance of Technology, societal beliefs, reactance, privacy concerns, willingness to share data, constructs from the Health Belief Model, and values related to the implementation of technology. Next, the manipulation checks and credibility were taken, followed by questions about trust in the government and questions relating to the corona virus (conspiracy theories, and coronavirus

Table 2
Overview of sentences employed in the fictive scenario, per experimental factor.

Experimental factor	Statements used in the scenario
None: Introduction of future pandemic situation	*"There is a new virus that is spreading all over the world. The virus can spread through contact with others or through the air."*
Disease severity	**HIGH**: *"The virus can cause a lot of damage to one's health."*
	LOW: *"The virus can cause health damage, but the chance of this is small."*
None: Introduction of novel technology	*"New technologies are available, such as sensors in toothbrushes that can measure whether there are virus particles in the saliva. If the sensor finds the particles, a light on the toothbrush will light up. This means that you may be infected with the virus. The government gives everyone such a toothbrush, but use is voluntary."*
Data-sharing option	**MANDATORY**: *"The toothbrush anonymously collects data about the infection and sends it to the government."*
	VOLUNTARY: *"The toothbrush collects data about the infection anonymously and people can decide for themselves whether to send it to the government"*
None: General statement about data use	*The data provides insight into the current number of infected people, nationally and per region.*
Application goal of the technology	**PREDICTION:** *"In this way, the government can predict how serious the virus outbreak will be in two weeks, both regionally and for the whole of the Netherlands."*
	TRACING: *"If the light on the toothbrush turns on, the government advises you to stay at home and contact the GGD (municipal health service). The GGD can then work with you to find out who you may have infected."*
	PREVENTION: *"For example, the government can respond better to an outbreak by taking measures to prevent further spread of the virus. For example, by setting up a regional lockdown."*
Evidence base for the technology's effectiveness[a]	**STRONG**: *"Many studies have been done on this | predictive | approach | to prevent further spread | to detect infections. The studies show that this approach works."*
	WEAK: *"Hardly any studies have been done on the effectiveness of this | predictive | approach | to prevent further spread | to detect infections. The effectiveness of this approach has not yet been proven."*

Note. This table demonstrates the text used for the scenarios.

[a] For the **Evidence base** phrases, the text was adapted to create a coherent semantic connection with regards to the previous section "Application goal of the technology" (hence the multiple options per sentence).

infection status). Subsequently, manipulation checks were performed, to verify the effect of the experimental manipulations. Upon completion of the study, participants were thanked for their time, and through the provision of a unique identification code, were reminded of the possibility to withdraw their data. Finally, they were routed back to PanelClix to claim their reimbursement.

3.5. Measures

This section describes the variables utilized in this study. Other variables that were measured (as mentioned in section 3.4 Procedures) as part of the larger study, are beyond the scope of the current study and are not detailed here.

The measures below were taken in the online questionnaire. The Dutch version of the items can be found in the Supplemental Materials (Supplement C) and the folder at the Open Science Framework.

3.5.1. Privacy concerns

To measure respondents' privacy concerns regarding the novel technology presented to them in the scenario, the following two statements were used, adapted from Walrave and colleagues' study (2022) on CTAs: (1) *"I am afraid that my privacy is not guaranteed when I use this toothbrush"*, (2) *"I am concerned about how the government uses the data this toothbrush collects about me"*. Items were measured on a 7-point Likert scale (i.e., 1 totally disagree – disagree – somewhat disagree – neutral – somewhat agree – agree – totally agree 7). A high score on these two statements would entail high levels of users' privacy concerns ($M = 4.62$, $SD = 1.71$). The scale was considered reliable ($\alpha = 0.88$).

3.5.2. Intention to use the novel technology

Statements used to measure participants' intention to use the proposed technology were based on the questionnaire employed in Venkatesh and colleagues' study on the UTAUT [67]: (1) *"It is likely that I will start using this toothbrush*", (2) "*I plan to start using this toothbrush*". Participants were asked to imagine that the technology was real. Items were measured on a 7-point Likert scale (i.e., 1 totally disagree – disagree – somewhat disagree – neutral – somewhat agree – agree – totally agree 7). A high score on these two statements would indicate a strong incline towards using the technology ($M = 4.04$, $SD = 1.90$). The scale yielded a reliability score of $\alpha = 0.95$.

3.5.3. Willingness to share personal data

Participants could indicate their willingness to share their data collected from the novel technology with the government, through the following two statements: (1) *"If I had the choice, I would certainly share the data that the toothbrush collects about me with the government"*, (2) *"If I could choose myself, I would not forward the data that the toothbrush collects about me to the government"*. Items were measured on a 7-point Likert scale (i.e., 1 totally disagree – disagree – somewhat disagree – neutral – somewhat agree – agree – totally agree 7). During the data processing, the second statement was reverse-coded. Therefore, scoring higher on this construct would depict a stronger inclination towards sharing data ($M = 3.70$, $SD = 1.68$). A moderately reliable result was observed for the scale ($\alpha = 0.74$).

3.5.4. Manipulation and credibility checks

To assess if participants perceived the manipulations as intended, manipulation checks were performed by including the following scales and statements described in Table 3. Credibility of the scenario was measured with the item: "*How realistic did you think the story was? In other words, how likely do you think it is that this story could become a reality?*" on an answer scale of 1 (very unlikely) to 7 (very likely).

3.6. Data analysis

The data was processed using the statistical software R statistical software/RStudio (v. 2023.03.0 [41,66]). Prior to analysis, the three interval variables (intention to use, privacy concerns, willingness to share data) were converted into z-values by centring and scaling using the R function Scale(). First, regarding RQ1 on the effect of privacy concerns on intention to use, a multiple regression analysis was conducted for privacy concerns (IV) and intention to use the technology (DV) to account for the two moderator variables (i.e., disease severity, evidence base) through interaction effects. To answer RQ2, which focused on the effects of disease severity (IV) and evidence base (IV) on participants' willingness to share data (DV), a two-way analysis of variance (ANOVA) was performed. For RQ3, which focused on the effect of data-sharing options (IV) on privacy concerns (DV), an independent-samples *t*-test was conducted.

Nonsignificant findings were followed up with equivalence tests performed with the R package TOSTER [42,43] and are reported in Supplement G.

Table 3
Overview of the manipulation checks performed for each experimental variable.

Experimental factor	Manipulation check item(s)	Answer scale
Disease severity	*"How likely is it that the virus in the story causes serious health damage?"*	1 – *not probable at all*, 7 – *very probable*
Evidence base for the effectiveness of the technology	*"To what extent had the effectiveness of the toothbrush technology from the story been already proven?"*	1 – *completely unproven*, 7 – *completely proven*
Data sharing option	*"People could decide for themselves whether they would forward the data collected by the toothbrush to the government."*	1 – *certainly not true*, 7 – *certainly true*
	"The data collected by the toothbrush was automatically forwarded to the government."	1 – *certainly not true*, 5 –*certainly true (reverse coded for calculation of construct)*

4. Results

4.1. Randomization and credibility checks

Independence between variables was assessed through a series of chi-square tests of independence on the three experimental variables (i.e., disease severity, evidence base, and data sharing option) for the demographic variables age, gender, and education. The tests revealed that there were no significant relationships between the experimental and demographic variables. An overview of the results can be found in Table 4.

4.2. Manipulation and credibility checks

To ensure the effectiveness of the manipulated experimental variables, manipulation checks were performed for disease severity, evidence base, and the option to share data. First, the 'high' and 'low'

Table 4
Chi-square test results for randomization checks.

	Disease severity	Evidence base of effectiveness	Data sharing option
Age[a]	X^2 (6, $N = 821$) = 3.46, $p = 0.75$	X^2 (6, $N = 821$) = 2.62, p = 0.86	X^2 (6, $N = 821$) = 4.97, $p = 0.55$
Gender	X^2 (1, $N = 822$) = 0.24, $p = 0.62$	X^2 (1, $N = 822$) = 0.95, $p = 0.33$	X^2 (1, $N = 822$) = 0.005, $p = 0.95$
Education	X^2 (5, $N = 822$) = 8.16, $p = 0.15$	X^2 (5, $N = 822$) = 0.95, $p = 0.97$	X^2 (5, $N = 822$) = 8.45, $p = 0.13$

Note. For the analyses with age, the participant that indicated not wanting to disclose their age (n = 1) was removed.

conditions of the disease severity variable were examined; a higher mean for the 'high' condition would suggest that the manipulation was successful. Indeed, the independent samples *t*-test applied to compare mean differences between the 'high' and 'low' severity conditions revealed a significant effect of the manipulation variable ($t(819.5) = 5.69$, $p < 0.001$), with a higher score for the 'high' severity condition ($M = 4.46$, $SD = 1.62$) than for the 'low' condition ($M = 3.80$, $SD = 1.67$), which indicates that the severity was indeed perceived as higher in the high severity condition, thereby rendering the manipulation successful. Second, for evidence base, a higher mean reflects that effectiveness is better proven. Therefore, a higher mean for the 'strong' condition compared to 'weak' would indicate a success of the manipulation. The *t*-test for evidence base was statistically significant ($t(816.54) = 6.10$, $p < 0.001$), with higher means for the 'strong' ($M = 3.83$, $SD = 1.82$) than for the 'weak' condition ($M = 3.08$, $SD = 1.70$), indicating that the manipulation of evidence base was successful. Two items were used to check the manipulation of the data sharing options. The averaged score on these items (higher scores mean more certain of that data sharing is voluntary) of the participants in the conditions where they had the option to voluntarily share the data was significantly higher ($M = 3.58$, $SD = 1.14$) than the score of those in the conditions where it was mandatory to send the data to the government ($M = 2.55$, $SD = 1.06$, $t(818.57) = 13.35$, $p < .001$). It must be noted that the reliability of this manipulation check construct was questionable ($\alpha = 0.61$). Therefore, t-tests were performed on the single items as well: The t-tests of the two separate manipulation check items were also statistically significant, $t(803.5) = 9.17$, $p < 0.001$; $t(807.19) = 12.85$, $p < 0.001$, the first question presented higher means in the 'voluntary' condition ($M = 3.82$, $SD = 1.26$) than in the 'mandatory' ($M = 2.97$, $SD = 1.41$), while the second revealed a higher score for the 'mandatory' condition ($M = 3.87$, $SD = 1.22$), compared to the 'voluntary' ($M = 2.67$, $SD = 1.43$). Therefore, the manipulation of the option to share data also is considered successful.

The credibility assessment involved asking users the extent to which they considered the hypothetical scenarios to be credible. On a scale of 1 (very unlikely) to 7 (very likely), participants rated on average the credibility of the scenario a 3.94 ($SD = 1.89$), suggesting an average score.

4.2Relation between privacy concerns and intention to use

To answer the first RQ and to test H1-H3 on the effect of privacy concerns (IV) on intention to use (DV), and the moderating effects of disease severity and evidence base on this relation, a multiple, moderated linear regression with privacy concerns, disease severity, evidence base, the interaction term between privacy concerns and disease severity, and the interaction term between privacy concerns and evidence base, was performed. The model was evaluated to determine whether assumptions of the linear regression were respected (see Supplement D). The model explained a significant proportion of variance in intention to use the technology, $R^2 = 0.29$, $F(5, 816) = 67.44$ (Table 5).

Privacy concerns significantly predicted intention to use the technology, $\beta = -0.45$, $SE = 0.05$, $t = -9.00$, $p < 0.001$. This can be regarded as a medium effect size [44]. Therefore, it can be concluded that individuals' privacy concerns negatively relate to their intention to use the technology, thus supporting H1 (see Fig. 1).

Table 5
Regression results of model explaining intention to use the novel technology.

Effect	β	*SE*	*t*	*p*
Intercept	0.034	0.051	0.669	0.504
Privacy concerns	−0.451	0.050	−8.996	<0.001
Severity: low	−0.059	0.059	−1.007	0.314
Evidence base: weak	−0.012	0.059	−0.196	0.845
Privacy concerns * Evidence base	0.009	0.059	0.151	0.880
Privacy concerns * Severity	−0.174	0.059	−2.961	0.003

4.3. Moderation effects of disease severity and technology effectiveness on the relation between privacy concerns and intention to use

The second part of RQ1 involved the effect of disease severity and evidence base on the above relationship (H2 and H3). The interaction between privacy concerns and disease severity was found to be statistically significant, $\beta = -0.17$, $SE = 0.06$, $t = -2.96$, $p = 0.003$. This can be regarded as a small effect size [44]. The relationship between privacy concerns and intention to use on the two disease severity levels (i.e., *high* and *low*) was further examined through a simple slope analysis using estimated marginal means. In the high disease severity condition a negative relationship existed between privacy concerns and intention to use, $\beta = -0.45$, $p < 0.001$, $CI = [-0.53, -0.37]$. The same held for the low disease severity condition, $\beta = -0.62$, $p < 0.001$, $CI = [-0.70, -0.54]$. This means that in both conditions a negative relation between privacy concerns and intention to use existed. However, the negative relationship between privacy concerns and intention to use was weaker in the high compared to low disease severity condition. This provides statistical support for the weakening effect of disease severity on the relationship between privacy concerns and intention to use (H2). Fig. 2 displays the regression plots for disease severity as a moderation of the relation between privacy concerns and intention to use the novel technology.

The interaction between privacy concerns and evidence base was not significant, $\beta = 0.01$, $SE = 0.06$, $t = 0.15$, $p = 0.88$, indicating that evidence base did not moderate the relationship between privacy concerns and intention to use the technology, thereby not supporting H3.

4.4. Role of disease severity and evidence base of effectiveness in willingness to share data

The second RQ focused on predictors affecting users' willingness to share data with the government. To answer H4 and H5, a two-way ANOVA was employed to examine the effects of disease severity and evidence base of effectiveness on willingness to share data. Assumption checks and a boxplot displaying the relationships can be found in Supplement E. The main effect for disease severity (H4) yielded an F ratio of $F(1, 819) = 0.06$, $p = 0.82$, while evidence base (H5) yielded an F ratio of $F(1, 819) = 0.31$, $p = 0.58$, meaning that the results do not support H4 and H5.

4.5. Data sharing on privacy concerns

RQ3 concerned the effect of voluntary, compared to mandatory data

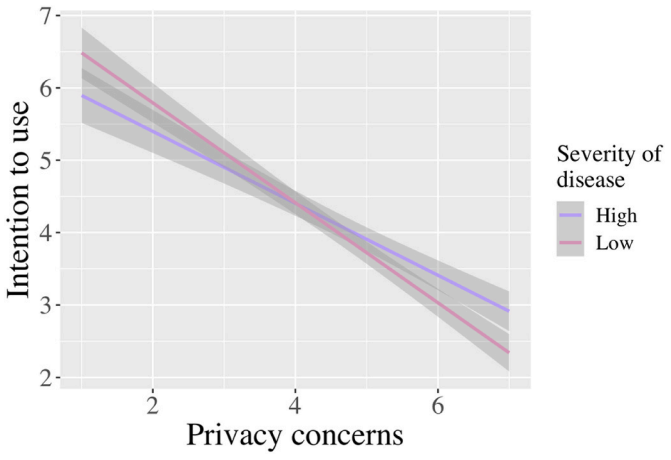

Fig. 2. Regression plot displaying the relationship between privacy concerns and intention to use (7-Point scales: higher values equal stronger intention/privacy concerns), for high and low disease severity. Grey bars depict standard errors.

sharing on individuals' privacy concerns. An independent samples *t*-test was conducted to compare participants in the 'voluntary' data sharing condition and the 'mandatory' condition. Assumption checking and a boxplot illustrating the relationship can be found in Supplement F. There was no significant difference in the scores for the 'voluntary' ($M = 4.60$, $SD = 1.67$) and the 'mandatory' ($M = 4.65$, $SD = 1.76$) conditions, $t(814.63) = 0.36$, $p = 0.72$. The results suggest that the data sharing option did not decrease responders' privacy concerns, thereby not providing support for H6. Fig. 3 depicts an overview of all statistical models.

4.6. Additional analyses

4.6.1. Direct effect of disease severity on intention to use

Previous studies regarding the direct effect of disease severity on intention to use in the context of infectious diseases have shown no such (or small) direct effects [31,45]. Therefore, we expected that such an effect would be nonsignificant for the current novel technology as well. To test if disease severity had a direct effect on intention to adopt in the current study, we performed a regression analysis of which the results can be found in Table 6. No significant differences in adoption intention were found between the conditions high and low in disease severity.

4.6.2. Relation between privacy concerns and willingness to share data

As previous studies [46] showed robust relations between privacy concerns and willingness to share data, we performed a correlation analysis. Based on these previous studies, we expected a negative relation between privacy concerns and willingness to disclose. In line with this, privacy concerns and Willingness to share data were negatively correlated, $r(820) = -0.67$, $p < 0.001$.

To test the moderating effects of disease severity and evidence base on this relation (i.e., similar as with RQ1 – intention to adopt), a multiple, moderated linear regression with privacy concerns, disease severity, evidence base, the interaction term between privacy concerns and disease severity, and the interaction term between privacy concerns and evidence base, was performed. The model explained a significant proportion of variance in willingness to share data, $R^2 = 0.46$, $F(5, 816) = 139.5$ (Table 7).

The interaction between privacy concerns and disease severity was found to be statistically significant, $\beta = -0.11$, $SE = 0.05$, $t = -2.03$, $p = 0.042$. The relationship between privacy concerns and willingness to share data on the two disease severity levels (i.e., *high* and *low*) was further examined through a simple slope analysis using estimated marginal means. In the high disease severity condition a negative relationship existed between privacy concerns and willingness to share, $\beta = -0.63$, $p < 0.001$, $CI = [-0.70, -0.55]$. The same held for the low disease severity condition, $\beta = -0.73$, $p < 0.001$, $CI = [-0.80, -0.66]$. This means that in both conditions a negative relation between privacy concerns and willingness to share data existed. However, the negative relationship was weaker in the high compared to low disease severity condition. The interaction between privacy concerns and evidence base was not significant, $\beta = -0.03$, $SE = 0.05$, $t = -0.62$, $p = .53$, indicating that evidence base did not moderate the relationship between privacy concerns and willingness to share.

Table 6
Regression results of model explaining intention to use by disease severity.

Effect	β	SE	t	p
Intercept	0.02	0.05	0.43	0.67
Severity: Low	−0.04	0.07	−0.61	0.54

Table 7
Regression results of model explaining the willingness to share data.

Effect	β	*SE*	*t*	*p*
Intercept	0.001	0.045	−0.026	0.979
Privacy concerns	−0.609	0.044	−13.906	<0.001
Severity: low	−0.039	0.051	−0.753	0.452
Evidence base: weak	0.040	0.051	0.773	0.440
Privacy concerns * Evidence base	−0.032	0.051	−0.622	0.534
Privacy concerns * Severity	−0.105	0.051	−2.034	0.042

4.6.3. Effect of the option to voluntarily share data on intention to adopt and willingness to share data

To explore the effects of the option to voluntarily share data on intention to adopt and willingness to share data, two additional analyses were performed. The model described for RQ1 was extended with the experimental factor Data sharing option, and an interaction term of

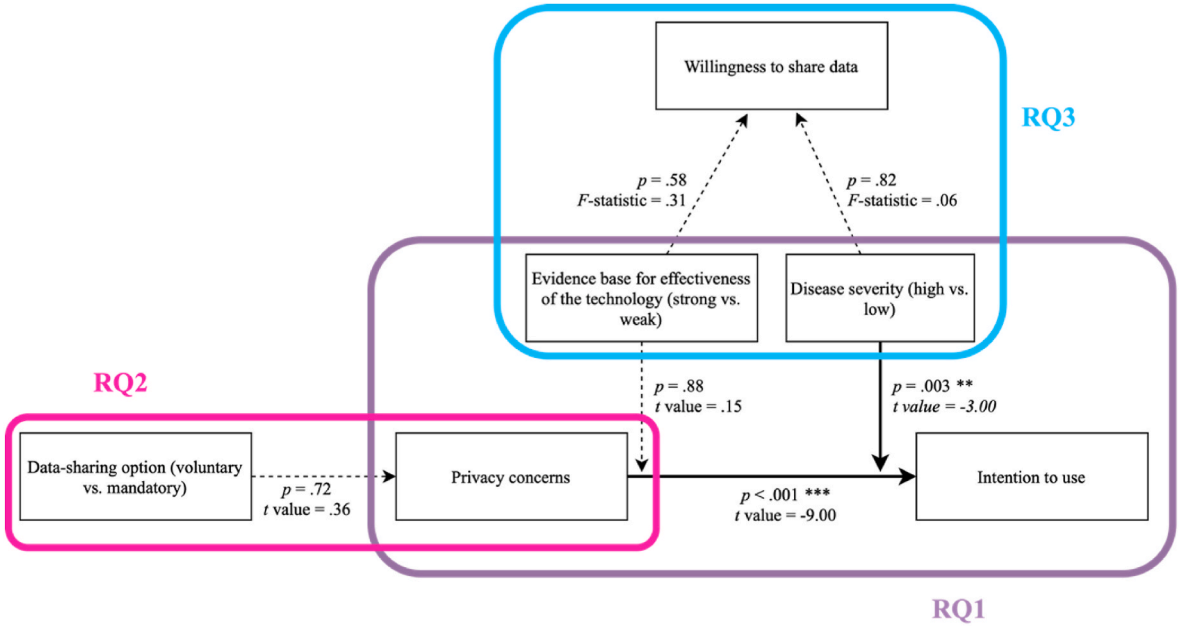

Fig. 3. Overview of the results of all analyses.
Note. *p* values marked with (**) indicate a statistical significance level above 0.01; *p* values marked with (***) indicate a significance level above 0.001.

privacy concerns by Data sharing option was added. The results can be found in Table 8. Adding the Data sharing option to the model did not affect the effects previously reported for RQ1. No main effect of Data sharing option was found ($\beta = 0.02$, $SE = 0.06$, $t = 0.39$, $p = 0.70$) but the interaction between privacy concerns and the Data sharing option was found to be statistically significant, $\beta = 0.17$, $SE = 0.06$, $t = 2.82$, $p = 0.005$. The relationship between privacy concerns and intention to use on the two Data sharing options (i.e., *voluntary* and *mandatory*) was further examined through a simple slope analysis using estimated marginal means. In the Voluntary Data sharing condition a negative relationship existed between privacy concerns and intention to adopt, $\beta = -0.45$, $p < 0.001$, $CI = [-0.53, -0.37]$. The same held for the Mandatory Data sharing condition, $\beta = -0.61$, $p < 0.001$, $CI = [-0.69, -0.53]$. This means that in both conditions a negative relation between privacy concerns and intention to adopt existed. However, the negative relationship was weaker in the Voluntary compared to the Mandatory Data sharing condition.

To assess the role of the Data sharing option in willingness to share data, the model described for RQ2 was extended with the experimental factor Data sharing option. Adding the Data sharing option to the model did not affect the effects previously reported for RQ2. The main effect for Data sharing option yielded an F ratio of $F(1, 818) = 0.41$, $p = 0.52$, meaning that there was no direct effect of Data sharing option on willingness to share data.

5. Discussion

This study investigated the privacy calculus in the context of adoption and data-sharing of novel health technology for diagnosing and tracking infectious diseases, and how contextual, i.e., disease severity, and technology-specific, i.e., the evidence base for the effectiveness of the technology, factors affected the privacy calculus. Answering the first RQ, it was found that individuals with stronger privacy concerns had a lower intention to use the proposed technology but this relationship was weaker when the disease severity was high, suggesting that disease severity affects the privacy calculus for adoption. Answering the second research question, neither the disease severity, nor the evidence base of effectiveness influenced users' willingness to voluntarily share personal data collected from the technology, suggesting that the decision to share data was not directly affected by these contextual and technology-specific factors, though the effects of privacy concerns on willingness to share was again lower in the high severity disease context. Furthermore, regarding the last RQ, giving users the option to decide whether they would voluntarily share their data with the government did not affect their privacy concerns.

5.1. Privacy concerns and intention to use the technology

Confirming the first hypothesis, the current study revealed that after reading the scenario of a future pandemic situation, participants with higher privacy concerns were less likely to use the novel toothbrush, as depicted by the relation between privacy concerns an intention to use, thereby conceptually replicating and confirming findings from the existing literature [11,17,28,29,47].

Slow diffusion and low adoption rates of new technologies caused by privacy concerns are not exceptional. In the context of e-health technologies, when the topic of privacy emerges, individuals tend to have certain demands regarding the secure use and containment of their data, and have also voiced the desire to have control over it [48]. Indeed, there is increased awareness of people's digital footprints, particularly among the younger generation [49]. When CTAs were first launched during the COVID-19 pandemic, privacy concerns about these technologies dominated the public debate. Even though many of these applications (e.g., the German and Dutch CTAs; Harborth et al., 2023; [10]), have been designed in a decentralized and privacy friendly manner, they continued to raise privacy concerns. In addition, misperceptions about the type of data that was collected were highly prevalent and persistent. For instance, for the Dutch CTA, almost half of the population thought that personal information was collected, while this was not the case [10]. Privacy concerns may also stem from a lack of governmental trust, thus hindering CTA acceptance [50].Given that the current and previous studies consistently attribute an important role to privacy concerns in the acceptance, this highlights that in the design and implementation of e-health technologies, privacy concerns cannot be neglected, as they are an important barrier to adoption of (novel) technology. To summarize, by confirming the results found in previous studies, this study solidifies the knowledge on the relationship between privacy concerns and intention to use novel health technologies for diagnosing and tracking of diseases.

Based on the assumption that a higher disease severity increases the perceived benefit of using the application and thus affecting the risk-benefit trade-off, disease severity was evaluated as a moderator on the relationship between privacy concerns and intention to use the toothbrush. Given the fairly recent COVID-19 outbreak caused by rapid and severe infection rates [51], it was expected that participants informed of the great potential damage inflicted upon their health (i.e., high severity) would see greater benefits of using the application. In line with H2, it was found that the relation between privacy concerns and intention to use the technology was weaker in a scenario where the disease is highly severe compared to a context where the damage caused by the virus is relatively mild. The effect of a high disease severity is rather expected; participants in this condition may have felt the high severity level alarming, thus wanting to take action regardless of their privacy being at risk.

There is limited other empirical support of the moderating role of disease severity on the relationship between privacy concerns and intention to use the technology. To our knowledge, one study on CTAs employed during COVID-19 revealed that perceived privacy risk affected behavioural intention, and that the relationship was moderated by self-reported perceived disease threat [52]. Jointly, the current study and Chopdar's suggest that disease severity contributes to individuals' risk-benefit analysis, in that disease severity influences the benefits of giving up on their privacy to make use of the toothbrush, thereby providing support for the PCT. The current study is thereby the first experimental study to show that the impact of privacy concerns on intention to use is weaker in a situation where the disease is severe, thereby extending our knowledge on how contextual factors influence the privacy calculus.

The evidence base for effectiveness as a factor influencing the relationship between privacy concerns and intention to use was investigated as well. The level of empirical support for the efficacy of the technology in battling the new virus did not seem to influence the relationship between privacy concerns and intention to use, thereby not providing support for H3. There is limited empirical research on the effect of evidence base as a moderator of this relationship, particularly in the field of healthcare. Though some several studies found a direct relation between performance expectancy and perceived privacy risk [53], no earlier study had investigated evidence base as a moderator. Though the absence of an effect in the current study suggests that evidence base of a

Table 8
Regression results of model explaining intention to use the novel technology, extended with experimental factor Data sharing option.

Effect	β	*SE*	*t*	*p*
Intercept	0.020	0.059	0.355	0.722
Privacy concerns	−0.534	0.058	−9.223	<0.001
Severity: low	−0.058	0.059	−0.997	0.319
Evidence base: weak	−0.007	0.059	−0.123	0.902
Data sharing option: voluntary	0.023	0.059	0.390	0.696
Privacy concerns * Evidence base	0.017	0.059	0.291	0.771
Privacy concerns * Severity	−0.177	0.059	−3.017	0.003
Privacy concerns * Data sharing option	0.166	0.059	2.819	0.005

novel technology's effectiveness does not contribute to individuals' risk-benefit analysis as posited in the PCT, the results should be replicated to confirm the absence of this effect.

5.2. Disease severity and technology effectiveness on users' willingness to share data

For many novel (health) technologies, it holds that solely adopting the proposed technology is not sufficient to be optimally effective or to limit the spread of a virus. The more data is shared with the company behind the eHealth app or the government, the quicker actions can be taken to engage in containment methods. In this study, it was found that the disease severity did not influence participants' willingness to share their data with the government. This finding contrasts the fourth hypothesis as it was expected that a higher disease severity would lead to increased willingness to share data. The finding is also not in line with a previous study on information disclosure in restaurants during the COVID-19 pandemic which revealed that the perceived severity of the disease had a positive effect on the perceived benefit of disclosing personal information, which in turn affected information disclosure behaviour [54]. One other study had shown a positive effect of perceived severity on perceived benefits of CTAs [28]. Combining the findings of these studies with this research, it seems that disease severity may increase the perceived benefit of disclosing information but not to such an extent that it directly affects the decision to share data. It should be noted that in the additional analysis, in which we tested if disease severity moderated the relation between privacy concerns and willingness to share data, a significant effect was found. In both high and low disease severity contexts, a negative relation between privacy concerns and willingness to share data existed. However, the negative relationship was weaker in the high compared to low disease severity condition. Finding no direct effect of this potential benefit but, instead, a moderating effect of disease severity on the relationship between privacy concerns and willingness to share, has theoretical implications regarding the PCT. The findings are in line with previous notions (e.g., Ref. [21]) regarding the calculus perspective, namely that it primarily drives joint effects (and not separate effects) of risk and benefits: if the perceived benefit outweighs the risk, users with high privacy concerns would share more information.

Linking this with the PCT, although the findings regarding adoption for H2 suggested that disease severity affects the privacy calculus trade-off in relation to adoption of data-collecting technology (where data is required for the main functionality of the technology, e.g., diagnosis), this may not be the case for the explicit decision to share data (e.g., with the government). That is, a high disease severity may stimulate individuals to disregard their privacy for as far needed to use the application but may not push individuals to share more information than strictly required to use the intervention for their own benefits.

In contrast to H5, no effect of evidence base for effectiveness on the willingness to share data was found. Also in the additional analysis, in which the moderating effect of evidence base on the relation between privacy concerns and willingness to share data, no significant effect was found. This is also in contrast to findings of slightly related studies showing an effect of performance expectancy on an individuals' intention to disclose information [16]. The current study extends previous findings by showing that evidence base for effectiveness may not have contributed to individuals' privacy risk assessment in so far as needed to share data.

An important difference between the previous studies supporting the link between disease severity and/or evidence base of effectiveness with willingness to share data, and the current one is that in this study, the severity and evidence base were experimentally manipulated, while the previous studies used self-reports of severity and constructs such as performance expectancy. It could be that the relations in previous studies with self-reports were biased by individuals who generally rate the severity of the disease situation lower or have less trust in technology solving it are also generally less willing to share their data via these technologies, thereby creating spurious relationships between these variables. Therefore, this study extends the existing knowledge by providing insights into the causal relationships between these variables.

5.3. The role of control in data disclosure (mandatory versus voluntary data sharing)

The third RQ focused on users' handling of their anonymous infection status, and how different data-sharing options affected privacy concerns. According to the SDT, the freedom to make choices triggers a feeling of autonomy in individuals. Indeed, people tend to demand control over their data, particularly with new technologies [39,55]. Drawing on this theory, it was expected (H6) that having the option to voluntary share data with the government would result in decreased privacy concerns. However, the findings of this study revealed that being given the option to decide whether the data should be shared with the government did not have any significant effects on participants' privacy concerns. These finding contrasts previous studies in the health domain. For instance, a study of Xu et al. [56], showed that a stronger sense of control over their personal information on a health website led to lower privacy concerns. Another study on online banking services' provided support for a positive effect of perceived control on perceived privacy [57]. Furthermore, a study on (mobile) health technologies indicated through qualitative analysis that a greater control over users' data would lower their privacy concerns, and that data collection without their consent would generate strong privacy concerns [39]. Such findings are not surprising; having control over the type of data being shared stems from the concept of autonomy, which is often perceived as a requirement when users are asked about their preferences on the handling of their data.

Again, an important difference between the previous studies and the current one is that in the latter, the option to share data was experimentally manipulated, while the previous studies used self-reports of perceived control. It could be that the relations in previous studies were biased by individuals who generally are more concerned about their privacy also perceiving to generally have a lower level of control over their data, thereby creating spurious relationships between these variables.

It should be noted that our additional analysis, in which we explored the role of voluntary data sharing in technology adoption, showed that the negative relationship between privacy concerns and intention to adopt was weaker in the Voluntary compared to the Mandatory Data sharing condition. This suggests that, if they are provided with the option to voluntarily share their data (or not), privacy concerns are less influential for their decision to use this data-collecting technology. This study extends the existing knowledge by showing that the effect of having the option to share your data on privacy concerns, may be smaller than was expected from the previous studies using self-reports. At the same time, having the option to share data does weigh in the privacy calculus by decreasing the effect of privacy concerns on the intention to adopt technology.

5.4. Strengths and limitations and implications for future research

An important asset of the current study is that an experimental approach was employed. Although many observational cross-sectional studies have observed the adoption patterns of novel technologies in the field (e.g., van der Waals et al., 2021; [58]), at different moments (with varying contemporary infection rates) in a real pandemic, they are unable to provide information about causality. Through this experiment using manipulations of disease severity, evidence base, and data-sharing options within realistic vignettes, it was possible to discover relationships among different variables in order to obtain an accurate picture of the factors causally affecting technology acceptance. A drawback of employing hypothetical vignettes is that this allows measuring

intentions (to adopt or share data) rather than actual behaviours. Even though the predictors of intentions and behaviours overlap to a considerable extent for adoption decisions (e.g., in the case of Contact tracing apps: [31,45,59]), it is important to note that there is a gap between intentions and actual behaviours (e.g., see the Privacy Paradox, Barth & De Jong, 2017), which stresses the importance of replicating these findings in a relevant field setting.

Although textual vignettes have been recognized as a valuable approach in the healthcare field, an increasing amount of governmental communication, especially regarding technology, nowadays takes place via animations or videos. Therefore, future studies could present the vignettes as videos explaining the novel technology. A study revealed that the combination of animation and spoken text can be a more effective method of communication for health-related topics in terms of recall, compared to written messages, regardless of participants' health literacy levels [60]. Even though the text of the vignette was written in a level understandable by the majority of the Dutch population, future studies in this field should consider adding more visual information, rather than simple text.

In the current study, the future scenario entailed a technology that was distributed by the government. The reason why the scenario was designed as such was because these technologies have been distributed by governments or governmental health associations in the past (COVID-19 pandemic) as well (e.g., Dutch and German CTAs were introduced by the government, UKs CTA was introduced by the National Health Services) and would therefore would constitute a realistic scenario. Though the mean levels of intentions ($M = 4.04$) and willingness to share (3.70) are above the midpoint of the (7-Point) scale, it is important to note that the experiences during the recent pandemic may have affected (over all conditions) intention or willingness to share data within a governmentally-distributed technology. In several countries, (e.g., The Netherlands), the support for governmental corona measures dropped over the course of the pandemic. For instance, the evaluation of the Dutch CTA showed that initially trust in the governmental approach to battling the virus, and the perceived contribution of the contact tracing app to reducing the spread of the virus, was beneficial but this dropped slightly throughout the pandemic [10,61]. Previous research has shown that the source of health policy (e.g., scientists versus governments) and the trust in this source affects acceptance [62,65]. A suggestion for future research is therefore to explore how the source of the technology may affect how the benefits affect the risk-benefit trade-off as proposed in the Privacy Calculus Theory.

Though the PCT has been shown to explain privacy-related decisions, it should be noted that there is more to disclosure decisions than only the (rational) risk-benefit as proposed in the PCT; they are also influenced by less rational factors, such as heuristics (e.g., Knijnenberg et al., [63]). By carefully matching the different conditions, we can rule out that alternative accounts of disclosure decisions have confounded our results pertaining to the risk-benefit tradeoff. However, given the importance of heuristics in disclosure, future research in this field should disentangle the relative contributions of these rational and non-rational factors.

5.5. Societal implications

This study's practical relevance lies in the identification of variables that should be considered in the development of novel technologies directed to monitor individuals' health, and specifically the conditions that call for the creation of such diagnostic tools. The study also revealed that contextual factors, such as the contemporary disease severity, are important with regards to the introduction of novel health technologies. The study provides insight into the optimal context for the introduction of novel health technologies, as it was shown that the negative relationship between privacy concerns and intention to use is weaker when the disease severity is high. Furthermore, as evidence base did not yield any significant effects, communication campaigns could rather focus on other perceived benefits of the technology. Knowing that having the option to share data voluntarily might not affect privacy concerns, designers could focus on other ways to reduce privacy concerns. Therefore, in the event of a future pandemic, technology companies working closely with the government for the creation of health tools could take into consideration this study's findings to assess the characteristics of the technologies, and thus ensure high adoption rates.

6. Conclusion

Infectious diseases, such as the recent COVID-19 outbreak, have been the source for major concerns regarding their spread and potential health damage. To limit their spread, several technologies were developed, with some resulting in greater adoption levels than others. In this experiment with realistic scenarios of a novel diagnosis technology, the role of privacy concerns affecting the intention to use of and the extent to which people would be willing to share their health data with the government was investigated. Privacy concerns hindered intention to use and willingness to share data less when the contemporary disease severity was high, suggesting that disease severity affects the cost-benefit trade-off as posited in the PCT. No such relieving effect of evidence base of the technology was found for intention to adopt or on willingness to share data. Research on technology acceptance in the field of healthcare seeking to examinate further the PCT should take into consideration this study's contribution to the literature on health technologies.

Funding

The panel costs were funded by the Dutch Ministry of Health, Welfare and Sports.

Availability of data and materials

The materials, the data, and the analysis script can be found on the Open Science Framework (link: https://osf.io/wtkcq/).

CRediT authorship contribution statement

M.S. Frangopoulou: Writing – original draft, Methodology, Formal analysis, Conceptualization. **L.N. van der Laan:** Writing – review & editing, Writing – original draft, Methodology, Data curation, Conceptualization. **W. Ebbers:** Writing – review & editing, Methodology, Investigation, Conceptualization.

Declaration of competing interest

The authors declare no competing interests.

Data availability

The data and code are available on the open science framework website : https://osf.io/wtkcq

Appendix A. Supplementary data

Supplementary data to this article can be found online at https://doi.org/10.1016/j.techsoc.2024.102616.

References

[1] O. Ali, & A. AlAhmad, H. Kahtan, A review of advanced technologies available to improve the healthcare performance during COVID-19 pandemic, Procedia Comput. Sci. 217 (2023) 205–216, https://doi.org/10.1016/j.procs.2022.12.216.

[2] I.-H.A. Chen, A. Ghazi, A. Sridhar, D. Stoyanov, M. Slack, J.D. Kelly, J.W. Collins, Evolving robotic surgery training and improving patient safety, with the integration of novel technologies, World J. Urol. 39 (8) (2021) 2883–2893, https://doi.org/10.1007/s00345-020-03467-7.

[3] F. Fitzpatrick, A. Doherty, G. Lacey, Using artificial intelligence in infection prevention, Curr. Treat. Options Infect. Dis. 12 (2) (2020) 135–144, https://doi.org/10.1007/s40506-020-00216-7.

[4] M.S. Nogueira, Ultraviolet-based biophotonic technologies for control and prevention of COVID-19, SARS and related disorders, Photodiagnosis Photodyn. Ther. 31 (2020) 101890, https://doi.org/10.1016/j.pdpdt.2020.101890.

[5] C.P. Sabino, A.R. Ball, M.S. Baptista, T. Dai, M.R. Hamblin, M.S. Ribeiro, A. L. Santos, F.P. Sellera, G.P. Tegos, M. Wainwright, Light-based technologies for management of COVID-19 pandemic crisis, J. Photochem. Photobiol. B Biol. 212 (2020) 111999, https://doi.org/10.1016/j.jphotobiol.2020.111999.

[6] R. Jalabneh, H.Z. Syed, S. Pillai, E.H. Apu, M.R. Hussein, R. Kabir, S.M.Y. Arafat, Md A.A. Majumder, S.K. Saxena, Use of mobile phone apps for contact tracing to control the COVID-19 pandemic: a literature review, in: S. Nandan Mohanty, S. K. Saxena, S. Satpathy, J.M. Chatterjee (Eds.), Applications of Artificial Intelligence in COVID-19, Springer, Singapore, 2021, pp. 389–404, https://doi.org/10.1007/978-981-15-7317-0_19.

[7] E. Christaki, New technologies in predicting, preventing and controlling emerging infectious diseases, Virulence 6 (6) (2015) 558–565, https://doi.org/10.1080/21505594.2015.1040975.

[8] A.D. Hossain, J. Jarolimova, A. Elnaiem, C.X. Huang, A. Richterman, L.C. Ivers, Effectiveness of contact tracing in the control of infectious diseases: a systematic review, Lancet Public Health 7 (3) (2022) e259–e273, https://doi.org/10.1016/S2468-2667(22)00001-9.

[9] D. Harborth, S. Pape, L.T. McKenzie, Why individuals do (not) use contact tracing apps: a health belief model perspective on the German corona-warn-app, Healthcare (Basel) 11 (4) (2023) 583, 10.3390%2Fhealthcare11040583.

[10] L.N. Van der Laan, J.M.S. De Wit, N.E. Van der Waal, Endreport coronamelder evaluation - survey liss panel wave 6, Retrieved from, https://research.tilburguniversity.edu/en/publications/eindrapportage-coronamelder-evaluatie-survey-liss-panel-wave-6, 2022, May 16.

[11] D. Dhagarra, M. Goswami, G. Kumar, Impact of trust and privacy concerns on technology acceptance in healthcare: an Indian perspective, Int. J. Med. Inf. 141 (2020) 104164, https://doi.org/10.1016/j.ijmedinf.2020.104164.

[12] E.-M. Schomakers, C. Lidynia, M. Ziefle, The role of privacy in the acceptance of smart technologies: applying the privacy calculus to technology acceptance, Int. J. Hum. Comput. Interact. 38 (13) (2022) 1276–1289, https://doi.org/10.1080/10447318.2021.1994211.

[13] S.X. Duan, H. Deng, Exploring privacy paradox in contact tracing apps adoption, Internet Res. 32 (5) (2022) 1725–1750, https://doi.org/10.1108/INTR-03-2021-0160.

[14] M. Jozani, E. Ayaburi, M. Ko, K.-K.R. Choo, Privacy concerns and benefits of engagement with social media-enabled apps: a privacy calculus perspective, Comput. Hum. Behav. 107 (2020) 106260, https://doi.org/10.1016/j.chb.2020.106260.

[15] R.S. Laufer, M. Wolfe, Privacy as a concept and a social issue: a multidimensional developmental theory, J. Soc. Issues 33 (3) (1977) 22–42, https://doi.org/10.1111/j.1540-4560.1977.tb01880.x.

[16] T. Jernejcic, O. El-Gayar, The role of the privacy calculus and the privacy paradox in the acceptance of wearables for health and wellbeing, AIS Trans. Hum.-Comput. Interact. 14 (4) (2022) 490–522, https://doi.org/10.17705/1thci.00177.

[17] S.J. Hong, H. Cho, Privacy management and health information sharing via contact tracing during the COVID-19 pandemic: a hypothetical study on AI-based technologies, Health Commun. 38 (5) (2023) 913–924, https://doi.org/10.1080/10410236.2021.1981565.

[18] Y. Gao, H. Li, Y. Luo, An empirical study of wearable technology acceptance in healthcare, Ind. Manag. Data Syst. 115 (9) (2015) 1704–1723, https://doi.org/10.1108/IMDS-03-2015-0087.

[19] M.E. Kretzschmar, G. Rozhnova, M.C.J. Bootsma, M. Van Boven, J.H.H.M. Van de Wijgers, M.J.M. Bonten, Impact of delays on effectiveness of contact tracing strategies for COVID-19: a modelling study, Lancet 5 (8) (2020) E42–E459.

[20] S. Shubladze, How to make use of the new gold: data, Forbes (2023, March 27). https://www.forbes.com/sites/forbestechcouncil/2023/03/27/how-to-make-use-of-the-new-gold-data/?sh=29883d7d2bbf.

[21] C.-L. Hsu, Y.-C. Liao, C.-W. Lee, L.K. Chan, Privacy concerns and information sharing: the perspective of the U-shaped curve, Front. Psychol. 13 (2022) 771278, https://doi.org/10.3389/fpsyg.2022.771278.

[22] E.L. Deci, R.M. Ryan, Intrinsic Motivation and Self-Determination in Human Behavior, Springer US, 1985, 10.1007/978-1-4899-2271-7.

[23] M.S. Hagger, S.J. Hardcastle, A. Chater, C. Mallett, S. Pal, N.L.D. Chatzisarantis, Autonomous and controlled motivational regulations for multiple health-related behaviors: between- and within-participants analyses, Health Psychol. Behav. Med. 2 (1) (2014) 565–601, https://doi.org/10.1080/21642850.2014.912945.

[24] A.F. Westin, Privacy and freedom, Wash. Lee Law Rev. 25 (1) (1968) 166.

[25] H. Xu, H.-H. Teo, B.C.Y. Tan, R. Agarwal, The role of push-pull technology in privacy calculus: the case of location-based services, J. Manag. Inf. Syst. 26 (3) (2009) 135–174, https://doi.org/10.2753/MIS0742-1222260305.

[26] S. Sharma, R. Crossler, Disclosing too much? Situational factors affecting information disclosure in social commerce environment, Electron. Commer. Res. Appl. 13 (5) (2014) 305–319, https://doi.org/10.1016/j.elerap.2014.06.007.

[27] E.-M. Schomakers, M. Ziefle, Privacy concerns and the acceptance of technologies for aging in place, in: J. Zhou, G. Salvendy (Eds.), Human Aspects of IT for the Aged Population. Design for the Elderly and Technology Acceptance, vol. 11592, Springer International Publishing, 2019, pp. 313–331, https://doi.org/10.1007/978-3-030-22012-9_23.

[28] T.T. Nguyen, M.T. Tran Hoang, M.T. Phung, "To our health!" Perceived benefits offset privacy concerns in using national contact-tracing apps, Libr. Hi Technol. 41 (1) (2023) 174–191, https://doi.org/10.1108/LHT-12-2021-0461.

[29] E.-M. Schomakers, C. Lidynia, M. Ziefle, Listen to my heart? How privacy concerns shape users' acceptance of e-health technologies, in: 2019 International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), 2019, pp. 306–311, https://doi.org/10.1109/WiMOB.2019.8923448.

[30] S. Geber, T. Friemel, Tracing-technology adoption during the COVID-19 pandemic: the multifaceted role of social norms, Int. J. Commun. 16 (2022) 247–266.

[31] N.E. Van Der Waal, J. De Wit, N. Bol, W. Ebbers, L. Hooft, E. Metting, L.N. Van Der Laan, Predictors of contact tracing app adoption: integrating the UTAUT, HBM and contextual factors, Technol. Soc. 71 (2022) 102101, https://doi.org/10.1016/j.techsoc.2022.102101.

[32] A. Choudhury, O. Asan, J.E. Medow, Effect of risk, expectancy, and trust on clinicians' intent to use an artificial intelligence system—blood Utilization Calculator, Appl. Ergon. 101 (2022) 103708, https://doi.org/10.1016/j.apergo.2022.103708.

[33] Z. Gu, F. Xu, J. Wei, An empirical study on factors influencing consumer's initial trust in wearable commerce, J. Comput. Inf. Syst. 56 (1) (2015) 79–85, https://doi.org/10.1080/08874417.2015.11645804.

[34] S. Barth, M.D.T. De Jong, The privacy paradox – investigating discrepancies between expressed privacy concerns and actual online behavior – a systematic literature review, Telematics Inf. 34 (7) (2017) 1038–1058, https://doi.org/10.1016/j.tele.2017.04.013.

[35] H.-M. Hsu, Does privacy threat matter in mobile health service? From health belief model perspective, in: PACIS 2016 Proceedings, 65, 2016. http://aisel.aisnet.org/pacis2016/65.

[36] T. Wang, T.D. Duong, C.C. Chen, Intention to disclose personal information via mobile applications: a privacy calculus perspective, Int. J. Inf. Manag. 36 (4) (2016) 531–542, https://doi.org/10.1016/j.ijinfomgt.2016.03.003.

[37] D. Mwesiumo, N. Halpern, S. Bråthen, T. Budd, P. Suau-Sanchez, Perceived benefits as a driver and necessary condition for the willingness of air passengers to provide personal data for non-mandatory digital services at airports, Transport. Res. Pol. Pract. 171 (2023) 103659, https://doi.org/10.1016/j.tra.2023.103659.

[38] M. Vansteenkiste, R.M. Ryan, B. Soenens, Basic psychological need theory: advancements, critical themes, and future directions, Motiv. Emot. 44 (1) (2020) 1–31, https://doi.org/10.1007/s11031-019-09818-1.

[39] G. Fox, "To protect my health or to protect my health privacy?" A mixed-methods investigation of the privacy paradox, J. Assoc. Inf. Sci. Technol. 71 (9) (2020) 1015–1029, https://doi.org/10.1002/asi.24369.

[40] J. Sheringham, I. Kuhn, J. Burt, The use of experimental vignette studies to identify drivers of variations in the delivery of health care: a scoping review, BMC Med. Res. Methodol. 21 (1) (2021) 81, https://doi.org/10.1186/s12874-021-01247-4.

[41] R Core Team, R: A Language and Environment for Statistical Computing, R Foundation for Statistical Computing, Vienna, Austria, 2021. URL, https://www.R-project.org/.

[42] A.R. Caldwell, Exploring equivalence testing with the updated TOSTER R package, PsyArXiv (2022), https://doi.org/10.31234/osf.io/ty8de.

[43] D. Lakens, Equivalence tests: a practical primer for t-tests, correlations, and meta-analyses, Soc. Psychol. Personal. Sci. 1 (2017) 1–8, https://doi.org/10.1177/1948550617697177.

[44] J. Cohen, Statistical Power Analysis for the Behavioral Sciences, second ed., Erlbaum, Hillsdale, MI, USA, 1988, 1988; ISBN 0-8058-0283-5.

[45] M. Walrave, C. Waeterloos, K. Ponnet, Tracing the COVID-19 virus: a health belief model approach to the adoption of a contact tracing app, JMIR Publ. Health Surveill. 6 (3) (2020) e20572, https://doi.org/10.2196/20572.

[46] I.M. Al-Jabri, M.I. Eid, A. Abed, The willingness to disclose personal information: trade-off between privacy concerns and benefit, Inf. Comput. Secur. 28 (2) (2020) 161–181.

[47] M. Trkman, P. Popovic, P. Trkman, The roles of privacy concerns and trust in voluntary use of governmental proximity tracing applications, Govern. Inf. Q. 40 (1) (2023) 101787, https://doi.org/10.1016/j.giq.2022.101787.

[48] C. Cheung, M. Bietz, K. Patrick, Privacy attitudes among early adopters of emerging health technologies, PLoS One 11 (11) (2016) e0166389, https://doi.org/10.1371/journal.pone.0166389.

[49] S. Karabatak, M. Karabatak, Z generation students and their digital footprints, in: 2020 8th International Symposium on Digital Forensics and Security (ISDFS), 2020, pp. 1–5, https://doi.org/10.1109/ISDFS49300.2020.9116455.

[50] G. Kostka, S. Habich-Sobiegalla, In Times of Crisis: Public Perceptions toward COVID-19 Contact Tracing Apps in China, Germany, and the United States, New Media and Society, 2022, https://doi.org/10.1177/14614448221083285 epub ahead of print.

[51] H.H. Khachfe, M. Chahrour, J. Sammouri, H.A. Salhab, B.E. Makki, M.Y. Fares, An epidemiological study on COVID-19: a rapidly spreading disease, Cureus 12 (3) (2020) e7313, https://doi.org/10.7759/cureus.7313.

[52] P.K. Chopdar, Adoption of Covid-19 contact tracing app by extending UTAUT theory: perceived disease threat as moderator, Health Pol. Technol. 11 (3) (2022) 100651, https://doi.org/10.1016/j.hlpt.2022.100651.

[53] D. Yoon Kin Tong, A study of e-recruitment technology adoption in Malaysia, Ind. Manag. Data Syst. 109 (2) (2009) 281–300, https://doi.org/10.1108/02635570910930145.

[54] E. Lee, J. Kim, J. Kim, C. Koo, Information privacy behaviors during the COVID-19 pandemic: focusing on the restaurant context, Inf. Syst. Front (2022), https://doi.org/10.1007/s10796-022-10321-1.

[55] C. Vigurs, C. Maidment, M. Fell, D. Shipworth, Customer privacy concerns as a barrier to sharing data about energy use in smart local energy systems: a rapid realist review, Energies 14 (5) (2021) 1285, https://doi.org/10.3390/en14051285.
[56] H. Xu, T. Dinev, J. Smith, P. Hart, Information privacy concerns: linking individual perceptions with institutional privacy assurances, J. Assoc. Inf. Syst. Online 12 (12) (2011) 798–824, https://doi.org/10.17705/1jais.00281.
[57] Y. Chang, S.F. Wong, C.F. Libaque-Saenz, H. Lee, The role of privacy policy on consumers' perceived privacy, Govern. Inf. Q. 35 (3) (2018) 445–459, https://doi.org/10.1016/j.giq.2018.04.002.
[58] M. Walrave, C. Waeterloos, K. Ponnet, Reasons for nonuse, discontinuation of use, and acceptance of additional functionalities of a COVID-19 contact tracing app: cross-sectional survey study, JMIR Publ. Health and Surveill. 8 (1) (2022) e22113, https://doi.org/10.2196/22113.
[59] M. Walrave, C. Waeterloos, K. Ponnet, Ready or not for contact tracing? Investigating the adoption intention of COVID-19 contact-tracing technology using an extended unified theory of acceptance and use of technology model, Cyberpsychol., Behav. Soc. Netw. 24 (6) (2021), https://doi.org/10.1089/cyber.2020.0483 (2021), 377-38.
[60] C.S. Meppelink, J.C. Van Weert, C.J. Haven, E.G. Smit, The effectiveness of health animations in audiences with different health literacy levels: an experimental study, J. Med. Internet Res. 17 (1) (2015) e11, https://doi.org/10.2196/jmir.3979.
[61] L.N. Van der Laan, J.M.S. De Wit, N.E. Van der Waal, Endreport CoronaMelder Evaluation - Survey LISS Panel Wave 1, 2020, December 9. Retrieved from, https://research.tilburguniversity.edu/files/50756058/Rapportage_Evaluatie_CoronaMelder_TilburgUniversity_LISSpanel_Wave1_v1_4.pdf.
[62] C. Evers, D.R. Marchiori, A.F. Junghans, J. Cremers, D.T.D. De Ridder, Citizen approval of nudging interventions promoting healthy eating: the role of intrusiveness and trustworthiness, BMC Publ. Health 18 (1) (2018) 1182, 10.3389%2Ffpubh.2023.1079992.
[63] B. Knijnenberg, E. Raybourn, D. Cherry, D. Wilkinson, S. Sivakumar, H. Sloan, Death to the privacy calculus, SSRN Electron. J. (2017), https://doi.org/10.2139/SSRN.2923806.
[64] HSE. (n.d.). Privacy and how we use your data. (n.d.). https://www2.hse.ie/conditions/coronavirus/covid-tracker-app/privacy-and-how-we-use-your-data.html.
[65] M. Osman, N. Fenton, T. Pilditch, D. Lagnado, M. Neil, Whom do we trust on social policy interventions? Basic and Appl. Psychol. 40 (5) (2017) 249–268, https://doi.org/10.1080/01973533.2018.1469986.
[66] R Studio Team, RStudio, Integrated Development for R. RStudio, PBC, Boston, MA, 2020. URL, http://www.rstudio.com/.
[67] Morris Venkatesh, Davis, Davis, User acceptance of information technology: toward a unified view, MIS Q. 27 (3) (2003) 425, https://doi.org/10.2307/30036540.
[68] J. Wirth, C. Maier, S. Laumer, The influence of resignation on the privacy calculus in the context of social networking sites: an empirical analysis, Res. Pap. 161 (2018). https://aisel.aisnet.org/ecis2018_rp/161.