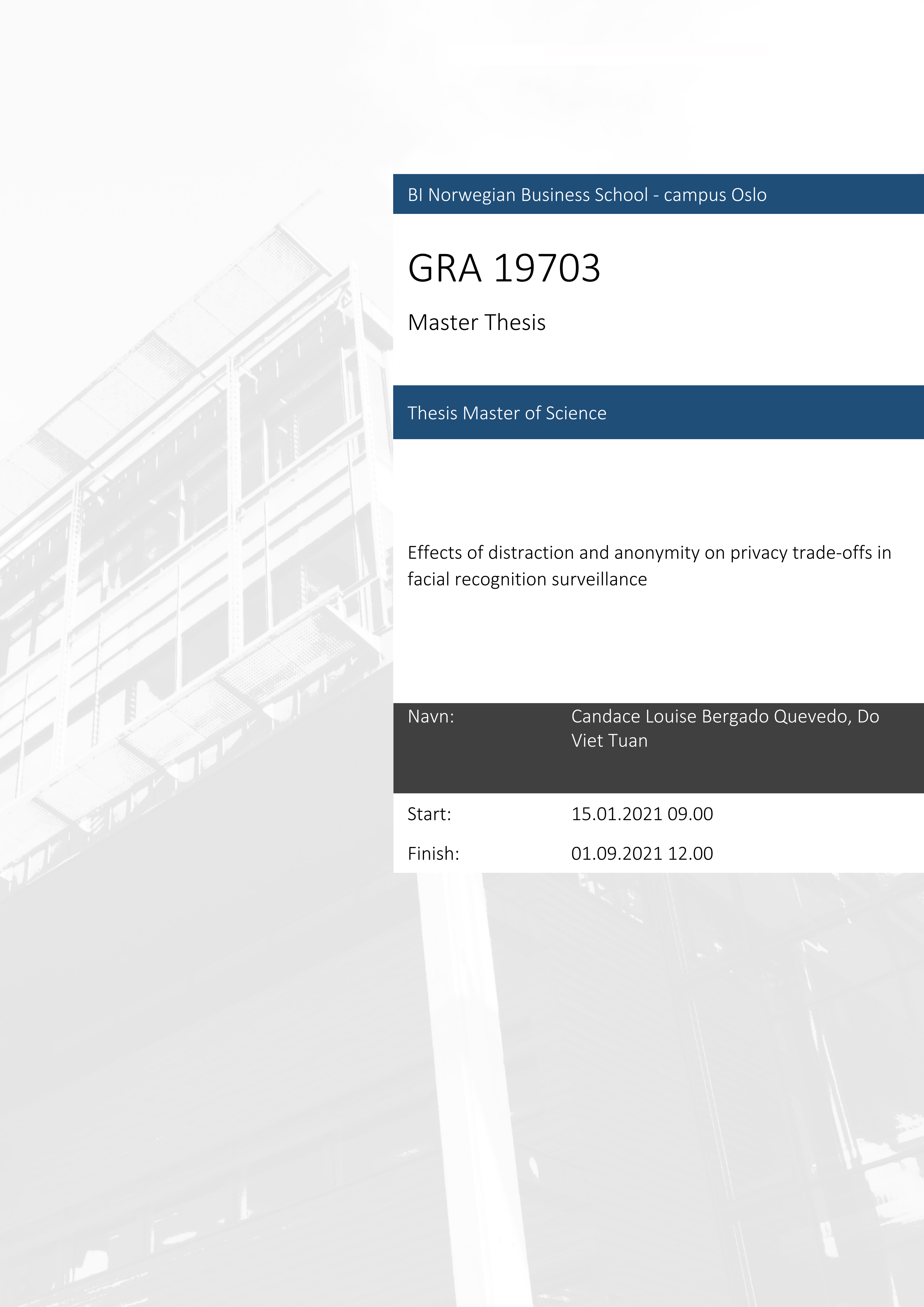


BI Norwegian Business School - campus Oslo

GRA 19703

Master Thesis

Thesis Master of Science

Effects of distraction and anonymity on privacy trade-offs in facial recognition surveillance

Navn:	Candace Louise Bergado Quevedo, Do Viet Tuan
Start:	15.01.2021 09.00
Finish:	01.09.2021 12.00

Master Thesis

--Effects of distraction and anonymity on privacy trade-offs in facial recognition surveillance--

Hand-in date:
01.07.2021

Campus:
BI Oslo

Examination code and name:
GRA 19703 Thesis Master of Science

Programme:
Master of Science in Strategic Marketing Management

Supervisor:
Matilda Dorotic

Table of Contents

Table of Contents

List of Tables

List of Figures

Abstract

Despite the recent development of facial recognition technology (FRT) using AI, its implementation and applications are still controversial in countries. Amid the COVID-19 pandemic, FRT could be an effective crisis exit strategy for nations. However, there was a lack of empirical evidence in privacy literature or marketing research on how authorities, governments, and private sectors should implement the technology. Using the ground theory of ELM models, privacy calculus to examine privacy attitude, intention, and behavior, this study provides a theoretical model that illustrated people's thinking and decision-making process with FRT's applications. By conducting an online experiment with the random sampling of 603 respondents in the UK and the US, the study showed a structural model thinking process that led to privacy disclosure behavior. The findings confirmed that distraction and non-anonymized FRT would increase people's concerns about government intrusion, which mediately impact willingness to support and disclosure behavior.

Moreover, moral consideration as moral equity referred that governments should raise awareness of FRT's importance to society to increase biometric data disclosure. Finally, a cluster analysis was conducted to classify people into three groups of "willing-to-share information." This further investigation also suggested a potential factor as stereotypes of people, which can deviate from the privacy paradox of people.

This study contributed to privacy and marketing literatures in the context of FRT government surveillance.

Acknowledgments

We would like to express our gratitude to our supervisor, Dr. Matilda Dorotic, for opening our interest in this topic. Thank you for being involved from the beginning to the end, helping us, and being patient with us throughout the process.

We would also like to thank PhD candidate Emanuela Stagno and Dr. Luk Warlop for their constructive and valuable comments. Lastly, we would like to thank everyone who participated in our pre-test and gave us their honest feedback. Thank you all for making it possible for us to complete our research.

BI Norwegian Business School funded the data collection of this study. Hence, the data is a property of BI Norwegian Business School.

Sincerely,
Tuan Do Viet and Candace Louise Quevedo

Introduction

Technologies have transformed how people live (Schmitt, 2019). There has been an increase in the implementation of government surveillance technologies (Fox, 2021). For instance, surveillance technologies such as contact tracing and facial recognition technology (FRT) played a crucial role in responding to the COVID-19 pandemic (Rasdale et al., 2020). However, such technologies are primarily viewed as invasive due to their impact on individual's privacy and their potential to broaden power asymmetries between the government and citizens (Veliz, 2021).

A biometric system creates seamless, intelligent, and secure authentication (Bhalla, 2020). It is considered more secure because 'the body does not lie' (Kloppenburg & van der Ploeg, 2020). Face recognition systems are a technology that detects and recognizes images of people captured by a camera lens (Yeung et al., 2020). Its primary purpose is to identify and verify identities.

An industry point of view survey conducted by the Biometric Institute found that 55% of respondents believe that face biometric is one of the most likely technologies to increase over the following years (Biometric Institute, 2019). It is projected to grow from 3.8 billion USD in 2020 to 4.5 billion USD in 2021 (Dialani, 2021). Currently, the most accepted and widespread use of FRT is in smartphone access, social media such as Facebook, airports, and brands' virtual try-ons.

Today, face mask detection surveillance allows contactless solutions for a safe and sustainable lockdown exit strategy and post-pandemic life (Rasdale et al., 2020). It can slow down the rate of spread of the disease and lessen citizens' COVID-19 fears. If implemented, there will be no more necessary lockdowns, which negatively impact citizens' mental health (Holmes et al., 2020) and physical health (Piertrobelli et al., 2020)

However, although the implementation of FRT surveillance comes with many potential benefits, concerns such as perceived invasion of privacy, mass surveillance concerns, and government intrusion concerns prevent people from fully adopting it. A survey conducted by Biometrics Institute (2019) found that 66%

of respondents consider privacy/data concerns to restrain the adoption to the greatest extent, and 43% considered data-sharing concerns. Thus, many perceive FRT to be disruptive and intrusive (North-Samardzic, 2019). Some cities, such as San Francisco, have banned FRT application by any local agencies and law enforcement (Rasdale et al., 2020).

FRT surveillance can only be effective and beneficial if people trust and adopt it. Therefore, it is crucial to find the balance between collecting data and citizens' privacy concerns to achieve mass acceptance (Trudinger and Steckermeier, 2017). Consequently, this study examines factors that influence public acceptance of FRT in the public environment, specifically, the introduction of face mask detection surveillance in public spaces such as buses, train stations, etc.

Research Question: How will the level of FRT intrusiveness and distraction influence individuals' concerns and decision-making regarding willingness to support and disclose privacy behavior of face mask detection surveillance in the COVID-19 pandemic?

To examine this research question, we conducted an online survey experiment of 603 respondents. We address the research gap by developing a model that considers factors that empirically drive acceptance. Firstly, this study combines the elaboration likelihood model (ELM) framework with privacy calculus to consider the central and peripheral route processing roles in making trade-off decisions. Secondly, this study investigates the discrepancy between willingness and behavioral intentions to support the surveillance solution. This study contributes to existing privacy literature in the domain of government surveillance and the COVID-19 context. The results of this study can help citizens, public officials, and technology developers to find common ground where the implementation of FRT will meet citizens' privacy rights.

The remainder of the paper proceeds as follows. The following section discusses a review of relevant conceptual constructs of our study, followed by our research model and hypotheses. Section 4 describes our measurements and methods. Then, a report of the analysis follows. Lastly, the final section discusses the conclusion, implications, limitations, and potential future research avenues.

Literature Review

Privacy has been studied in many different disciplines and lenses. For some, privacy is believed as one of the highest forms of individual rights (Rosen 2001; Bernal, 2016), a moral right (Corlett, 2002), or a legal right (Clarke, 1999). Therefore, due to the differing perspectives, there is no agreement on one the general definition of privacy (Pavlou, 2011). The privacy concept used in this paper is focused on the individual right, the right of a person to control his/her generated data with society's protection to safeguard any misuse of information without his/her permission. Although research in the privacy literature is quite extensive, there is an increasing demand for a more contextual approach to information privacy (Wu et al., 2019; Wirth, 2018; Yun et al., 2019). For instance, research on privacy in the context of digital government surveillance has only emerged in recent years.

This section will discuss government surveillance technology acceptance and its antecedents, including privacy concern, perceived usefulness, recent relevant factors such as perceived needs for government surveillance, and perceived government intrusion. Then, privacy trade-offs, including privacy calculus and privacy disclosure, will be elaborated.

Government surveillance technology acceptance

Government surveillance has been linked to the development of technology and current events (Nam, 2019). The governments justify their implementation by emphasizing the need for surveillance to maintain order (Dinev et al., 2008). Thus, the emergence of the COVID-19 pandemic has resulted in the introduction of surveillance technologies such as tracking applications, monitoring sensors, and facial recognition systems (Fox, 2021). However, despite the recent growing attention in research on governmental-based surveillance technologies, very few research focused on citizen’s acceptance of specific technologies (Nam, 2019). Lyon (2001) refers to surveillance as “any collection and processing of personal data, whether identifiable or not, for purposes of influencing or managing those whose data have been garnered.” Hence, in the context of facial recognition government surveillance, personal data are images, biometrics, etc.

Public acceptance is key to reap the benefits of surveillance technologies. Prior studies found that public acceptance is influenced by various factors such as privacy concerns (Dinev & Hart, 2006; Dinev et al., 2008), the perceived need for surveillance (Brown & Korff, 2009), trust in the government (Thompson et al., 2020), citizens’ perceptions of benefits from using governmental surveillance (Nam, 2018), policy transparency (Thompson et al., 2020), and the presence of privacy (Dinev et al., 2006).

Privacy concerns

The role of privacy concern has been investigated in many studies in the context of advertisers and companies' privacy intrusion to consumers (Nam, 2018). However, very few studies focus on its role in the context of government surveillance (e.g., Dinev et al., 2006; Dinev et al., 2008; Pavone & Esposti, 2012). Privacy concern has a complex role on information privacy literature. Some studies focus on its role as an explanatory variable, others as an explained variable, or both (Smith et al., 2011), as table 1. Dinev et al. (2008) defined privacy concerns as “the extent to which individuals believe they might lose their privacy.”

Smith et al.'s (2011) review on privacy literature found the antecedents of privacy concern to be privacy experiences, privacy awareness, personality differences, and demographic differences. Prior research also found empirical evidence that privacy control is key to decreasing privacy concerns (Dinev & Hart, 2004; Phelps et al., 2000). This finding is also supported by Xu et al. (2011), claiming that constructs such as perceived information control and perceived value of control explain how privacy control influences privacy concerns. Other factors such as information sensitivity can also determine the extent of privacy concerns (Phelps et al., 2000).

Table 1

Summary of Privacy concerns literature and findings

Privacy Concern as		Category of effect (Negative/ Positive) on Privacy Concern	Research
Explanatory Variable for	Explained Variable of		
Willingness	Privacy experiences	+	Smith et al. (2011)
	Personality differences		
	Demographic differences		
	Surveillance awareness	+	Nam (2018)
	Privacy control	-	Dinev & Hart (2004); Phelps et al. (2000); Nam (2008)
	Perceived information control	-	Xu et al. (2011)
	Perceived value of control	-	
	Information Sensitivity	+	Phelps et al. (2000)
	Perceived need for government Surveillance	-	Dinev et al. (2008)
	Government intrusion Concerns	+	

In the context of surveillance, Dinev et al. (2008) investigated the relationship between Internet privacy concerns and government surveillance factors. They found that the perceived need for government surveillance is positively related to privacy concerns, while government intrusion concerns were negatively related.

Another study by Nam (2018) found that the usual empirical antecedents of privacy concern, such as perception of privacy control, past negative experiences, surveillance awareness, and information sensitivity, can also be applied in the surveillance context. In the study, the author replaced the term "privacy concern" with "surveillance concern" and found that it also significantly influences surveillance acceptability. However, recent research by Fox et al. (2021) found that privacy concerns do not affect acceptance before or post-launch of the contact-tracing application and only exhibit a weak influence on willingness to rely on the application.

The conflicting findings on the role of privacy concerns and the lack of studies in the government's use of facial recognition surveillance context call for further investigation. Will the antecedents of privacy concern in other studies' context also confirm the relationship in the context of high intrusive technology such as facial recognition surveillance technology? How will other factors such as level of intrusiveness of the surveillance technology and distraction play a role?

Perceived usefulness of surveillance

Perceived usefulness is one of the two beliefs from the Technology Acceptance Model (TAM), which claims that it relates to accepting a new technology (Davis, 1989). The other belief is perceived ease of use; however, since the nature of FRT is seamless and contactless, and respondents did not experience the technology, then it is irrelevant for this study. Perceived usefulness refers to "a person's subjective probability that using an application system will be helpful in improving performance" (Ruggieri et al., 2021). For this study's context, face mask detection surveillance can be helpful as it can help society to sustainably exit lockdowns which negatively impact citizen's mental health (Holmes et al., 2020) and physical health (Piertrobelli et al., 2020).

Perceived need for surveillance

Perceived need for government surveillance is defined as the belief that the government should increase national security to ensure safety and social order (Dinev et al., 2008). Thus, this construct intends to capture the beneficial factor of FRT surveillance. Dinev et al.'s (2008) study showed the beneficial role of perceived need for surveillance. They found that the perceived need for surveillance has a negative relationship with privacy concerns and a positive relationship to the willingness to disclose personal information. Additionally, Thompson et al. (2020) investigated the perceived need for surveillance in different cultures, namely, Australia and Sri Lanka. They found that it has a positive influence on the acceptance of surveillance in both cultures. This finding means that despite the difference in cultures, the perceived need for surveillance still negatively affects privacy concerns and positively affects willingness and acceptance of surveillance.

Government intrusion concerns

Government intrusion concerns are defined as individuals' concerns about government monitoring activities (Dinev et al., 2008). The concerns occur when the cost of surveillance is higher than the need for surveillance. Additionally, there are concerns about the potential consequences of the government's greater access to information. For example, getting fined for not wearing a face mask. Dinev et al. (2008) confirmed that government intrusion concerns increase privacy concerns, consecutively reducing willingness.

The intrusiveness of Facial Recognition System technology

From a citizen's perspective, collecting a large quantity of personal data is perceived as intrusive (Kleek et al., 2008). Conversely, many devices that we use regularly collect personal data such as location, habits, health from wearable devices, etc. A study by Maiorescu et al. (2021) revealed that video data are perceived as more intrusive than data about habits from IoT devices. The findings explain why there is more resistance to accept of FRT.

The intrusiveness of FRT and its applications both in private and public settings before and amid COVID-19 is one of the most controversial issues that legislators, courts, and citizens are continuously dealing with to balance human rights, privacy protection, public welfare, and security (Etteldorf, 2020). According to the European Commission's Common Union (2020), AI technologies such as contact-tracing applications and facial recognition should help combat the spread and assist countries in exiting the COVID-19 pandemic. This notion is supported by Pagliari's (2020) study about contact-tracing apps in Scotland. The author suggested that FRT should be an option to reduce the contagion of the COVID-19 pandemic for the future of public health protection. Currently, 32 countries in Europe are using FRT. Some of them, such as France, are using the technology to reduce the spread of the coronavirus. However, FRT is banned in some places such as San Francisco and Belgium due to its highly intrusive nature.

A study by Feng & Xie (2019) found that more privacy-friendly reduces perceived intrusiveness, which leads to increase adoption intentions. Additionally, a recent EDPB (2020) guidelines on processing personal data through video devices suggest strict regulations that FRT should consider a privacy-friendly solution that only collects necessary data. Davis (2020) also advised FRT with anonymization, where people will not be identified.

Recently, a group of researchers from the University of Science and Technology in Norway introduced an AI face anonymization model, called DeepPrivacy, to protect user's privacy without interrupting the original data distribution (Pascu, 2019). Hence, the rise of a privacy-friendly feature of FRT raises the question of whether citizens will perceive the intrusiveness differently, which leads to increase surveillance acceptance. This study will examine the difference between anonymized and non-anonymized FRT in surveillance acceptance in the context of COVID-19.

Examining Privacy Trade-offs in Elaboration Likelihood Model

As discussed above, public acceptance of FRT depends on various factors such as privacy concern, perceived usefulness, needs for government surveillance, or perceived government intrusion, and how intrusive the FRT is. The intercorrelation of these factors in a specific situation was regarded a as privacy tradeoff. Hence, the privacy trade-offs, including privacy calculus and actual privacy behavior, would be elaborated.

Privacy calculus

Privacy calculus theory (PCT) is one of the most used theories in privacy literature. Privacy calculus theory is a reasoned action of personal calculations of expected risk and benefits that influence personal information disclosure behavior (Dinev & Hart, 2006). It is usually incorporated into other theories such as expectancy-value theory and utility maximization theory to explain the trade-off behavior (Li, 2012). PCT is considered flexible as it has been used as an antecedent to privacy-related decision-making behavior in various domains such as the Internet (Barth & De Jong, 2017), Internet of Things (IoT), and applications (Morosan & DeFranco, 2015).

Since it involves a complex psychological process that has different considerations, prior studies found that there have been various factors that influence privacy calculus and disclosure behavior (Li, 2012). For instance, in this study's context, negative factors can be termed privacy/surveillance concerns, perceived risk, previous experience with privacy invasion (Bansal et al., 2010), need for privacy (Yao et al., 2007), government intrusion concerns (Dinev et al., 2008) while positive factors can be termed as perceived usefulness (Fox, 2021), level of information sensitivity, trust in government, benefit to the society, the perceived need for government surveillance (Dinev et al., 2008; Thompson et al., 2020).

Privacy Trade-off

According to Rainie and Duggan (2016), the privacy trade-off should be defined as behavior that people share their data or accept surveillance to get perceived benefits (e.g., security, personalization (Kobsa et al., 2016), financial incentives (Tsai et al., 2011) in return. The interchange between cost and benefits of users creates the economic exchange where people must scarify their exclusively personal information to receive the benefits. Thus, the above-discussed privacy calculus tends to provide the rationale for the trade-off behavior. Researchers examined the privacy trade-offs in privacy literature, including privacy attitude, intention, and behavior in myriad facets. There are two prominent approaches to explaining the phenomenon (Barth & De Jong, 2017).

The first one evaluates privacy intention and reasonable behavior through the rationale, cognitive processing of people in privacy issues where the behavioral intention stems from a careful privacy calculus of the pros and cons of the situation. Grounded theories that support this approach are Theory of Planned Behavior (Ajzen, 1991) and Extended Privacy Calculus model (Dinev & Hart, 2006). Meanwhile, the second approach is that in a boundary condition, people tend to base on a heuristic evaluation (system 2) or to decide by diligently calculating the cost and benefit of the situation (system 1). The most prominent research in this stream relies on groundworks as the dual-process model of cognition (Kahneman, 2003).

However, Elaboration Likelihood Model (Petty & Cacioppo, 1986) reconciled both approaches by examining people's attitude changes through the thinking process as two routes: central route processing and peripheral route processing. By examining attitude changes, privacy intention and behavior should follow accordingly (Ajzen, 1991). The central route refers to high cognitive processing where people consider the privacy trade-offs as a balance between cost and benefit. In contrast, the peripheral route reflects the heuristic evaluation of the situation.

The Elaboration Likelihood Model (ELM)

In the context of FRT for public settings to reduce COVID-19 contagion, the complexity of privacy policy, the sensitivity of biometric data, and the benefit of public safety in pandemic should result in an ambiguous outcome of privacy trade-offs calculation. To sequentially capture the privacy attitude, intention, and behavior, this study adopts the Elaboration Likelihood Model (ELM) framework. In addition, this study examines privacy trade-offs to understand how peripheral and central route processing affect privacy attitude, intention, and privacy disclosure behavior. For this context, we define surveillance acceptance behavior in the same way as a privacy disclosure.

Petty and Cacioppo (1986) proposed the ELM to explain people's attitude changes based on the information processing route. To process a specific persuasive communication, people process information according to the MAO framework: motivation (personal relevance), ability, and opportunity (distraction, message comprehensibility). According to the framework, the central route processing occurs when people have high MAO to process the message; otherwise, peripheral route processing would occur.

In the central route processing, people evaluate the situation based on relevant attributes of the privacy trade-off as a privacy calculus process. The stream of studies provides various drivers of privacy calculus with economic-oriented drivers such as perceived risk, perceived benefit or interest (Dinev & Hart, 2006; Kim et al., 2019), perceived usefulness, perceived ease of use (Davis, 1989; Distler et al., 2020). These drivers illustrate transparent costs and benefits of the trade-offs where people can rationally evaluate information.

However, in peripheral route processing, Acquisti & Grossklags (2005) argued that bounded rationality limits people's ability to thoroughly process vast amounts of information related to privacy trade-off or the privacy calculus. The result also showed that even with available accessibility to complete knowledge and unbounded ability to process, people rarely have a rational calculus and decision but rather evaluate based on heuristic feeling as information (Mourey & Waldman, 2020). Studies in this stream provide contextual drivers such as intrusiveness (Wottrich et al., 2018), the complexity of privacy management, privacy's importance, perceived control (Mourey & Waldman, 2020). From this perspective, people tend to evaluate the situation heuristically instead of thoughtfully calculating each trade-off's attribute.

Distraction and privacy nudge in privacy trade-offs

Marketing literature on distraction's impact on communication persuasion has been pervasive. According to Petty et al. (1976)'s ELM model, distraction reduces people's ability to process the information that can change people's attitude toward a specific message. Zane et al. (2020) proposed an underlying lay theory driving metacognitive inferences from distraction as interest in the consumer research literature. This approach explained that consumers who are distracted by something (e.g., banner advertisement) from a focal task find the distractor more interesting. Lerouge (2009) depicted that appropriate distraction during the decision-making process can help consumers differentiate attractive from unattractive products.

In the privacy literature, distraction is regarded as “privacy nudges” (Apte, 2020; Kitkowska et al., 2020; Kobsa et al., 2016). It is commonly found in the presentation (Acquisti et al., 2017), which provides necessary contextual cues in the user interface. Specifically, distractions reduce cognitive load, influencing people's decisions as a mental shortcut (peripheral route) in privacy trade-offs. Most of the related results showed that distraction plays a role in deactivating the central route processing and affects people's behavior in a favorable direction of disclosing personal information.

However, Petty et al. (1976) proved that distraction could enhance or reduce the effectiveness of the message's persuasion through thought disruption. In case of a counterarguable message, the distraction would improve the favorable attitude. Nevertheless, if the message elicited favorable thoughts, the distraction would interrupt people's thoughts and negatively impact attitude toward the persuasive message.

Hence, the distraction is not always a privacy nudge (activate peripheral route). Also, its impact on the privacy trade-offs could vary as central or peripheral processing route. Therefore, for this study, we examine the impact of distraction on privacy trade-offs of face mask detection surveillance as a solution (with a favorable message) in the context of public settings amid the COVID-19 pandemic.

Privacy Intention and Willingness to provide information

In the ELM model, Petty and Cacioppo (1986) showed that attitude changes highly correlate with behavioral intention in the high (low) elaboration likelihood central (peripheral) route. This study's link between attitude and behavioral intention is through the impact of perceived government intrusion concerns on the willingness to support technology implementation.

Privacy intention (willingness to provide information) was depicted as behavioral intention to provide personal information (Acquisti et al., 2015; Bidler et al., 2020; Dinev & Hart, 2006; John et al., 2011). The privacy intention of people had various explanations and antecedents from scholars based on prominent ground theories of consumer psychology and behavior across disciplines. Table 2 illustrated a summary of relevant findings of explained variable and effect directions of Willingness.

Table 2

Summary of findings about explained variables of Willingness

Explained Variable of Privacy Behavioral intention (Willingness)	Category of effect (Negative/ Positive)	Research
Privacy norms	-	Gabisch & Milne (2014); Martin (2015)
Fairness and Privacy process	+	Culnan & Bies (2003)

Privacy concerns	-	Dinev & Hart (2006); Wottrich et al. (2018)
Data vulnerability	-	Martin et al. (2017)
Perceived risk	-	Kim et al. (2019)
Sensitivity of information	-	Acquisti & Grossklags (2005); Kim et al. (2019)
Perceived sensitivity	-	Gu et al. (2017)
Organizational trust	+	Kim et al. (2019)
Personalization value/ perceived benefits	+	Ryu & Park (2020)
Consumer control	+	Mourey & Waldman (2020)
Tech hedonism	+	Pizzi & Scarpi (2020)
Perceived usefulness	+	Davis (1989), Ruggieri et al. (2021)
Trust	+	Norberg et al. (2007)

In the Marketing literature, the Social Contract Theory of Dunfee et al. (1999) showed explained factors for privacy intention, including privacy norms and information control (Gabisch & Milne, 2014; Martin, 2015). Social science with the Justice Theory of Rawls (1971) provided ground theories for privacy intention's antecedents such as fairness, privacy process (Culnan & Bies, 2003).

As discussed above, Privacy calculus theory (Dinev & Hart, 2006) proposed relevant antecedents of privacy intention, including privacy concerns (Dinev & Hart, 2008), data vulnerability (Martin et al., 2017), perceived risk (Kim et al., 2019), and perceived usefulness (Davis, 1989; Ruggieri et al., 2021). Furthermore, willingness was also predicted through the sensitivity of information (Acquisti & Grossklags, 2005), perceived sensitivity (Gu et al., 2017); or examined privacy-enhancing factors as organizational trust (Kim et al., 2019), personalization value/perceived benefits (Ryu & Park, 2020), consumer control (Mourey & Waldman, 2020), and tech hedonism (Pizzi & Scarpi, 2020).

Privacy Disclosure Behavior and Privacy Paradox

Privacy behavioral intention, subjective norms, and perceived behavioral control lead to privacy disclosure behavior according to TPB theory (Ajzen, 1991). By examining the actual disclosure behavior, which is conditionally distinctive with intention or willingness, Barnes (2006) and Norberg et al. (2007) suggested the ***privacy paradox*** phenomenon. Despite high privacy concerns, users still voluntarily share their permission for collecting data. Further examining the privacy paradox phenomenon, many studies have depicted that people disclose personal data despite high privacy concerns with context-dependence and uncertainty (Acquisti & Grossklags, 2005; Berendt et al., 2005).

While the Privacy Calculus theory provided a foundation for explaining privacy intention (Becker et al., 2019; John et al., 2011; Mourey & Waldman, 2020; Princi & Kramer, 2020), this rational approach barely explains the privacy paradox. Moreover, other studies demonstrated the privacy paradox from the psychological perspective where the privacy decision-making in a specific situation would be affected by contextual factors, environmental cues, feelings as information rather than thorough calculation because of bounded rationality, asymmetric information, etc. (Becker et al., 2019; John et al., 2011; Mourey & Waldman, 2020; Princi & Kramer, 2020).

This paper examines the privacy disclosure and paradox in central and peripheral routes to detect privacy intention and behavior differences. As far as we know, the privacy paradox literature lacks empirical study in the context of facial recognition. Most prior studies focused on privacy intention. However, facial data exposure behavior should play an important role, especially since both public and private sectors use FRT (Bigg, 2020; Feldstein, 2019).

Table 3

Summary of constructs, variables description

Construct Categories	Constructs	Acronym	Definition
Actual Disclosure	Privacy Disclosure/Acceptance	Disclose	Agree to try FRT
Willingness to support	Privacy Intention/Willingness	Will	Willingness to support FRT implementation
Negative side of privacy calculus	Privacy Concern	PC	The extent to which individuals believe they might lose their privacy
	Government Intrusion Concern	GI	Individuals’ concerns about government monitoring activities

Positive side of privacy calculus	Perceived Usefulness	PU	A person’s subjective probability that using FRT will help improve well-being.
	Government Trust	GT	The extent of trust in government related to FRT implementation
	Perceived Needs for Government Surveillance	GS	Belief that the government should increase national security.
Potential factors can impact perceived concern of government intrusion	Intrusiveness of Technology	Intru	Refer to two types of FRT (Anonymized and Identified) technology.
	Distraction	Distract	Refer to two conditions of distracted or non-distracted.

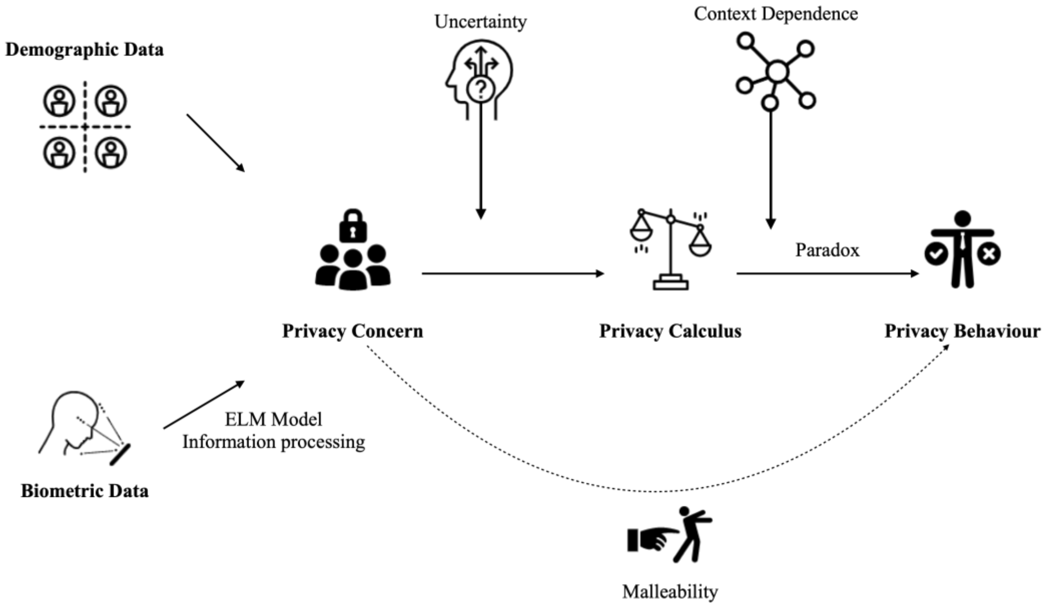
This study includes relevant antecedents as described in Table 3, combining entities such as privacy concern, needs for government surveillance, government intrusion, perceived usefulness to explain privacy intention and behavior.

Literature Gap and Expected Contribution

As discussed above, a robust body of literature related to privacy showed various antecedents, independent and dependent variables. Acquisti et al.'s (2015) review article classified prior research into three themes: Uncertainty, Context-dependence, and Malleability. Each research stream studied privacy in a different lens where uncertainty referred to privacy intention and behavior due to a privacy calculus based on asymmetric information. Context-dependence reflected people's natural behavior in uncertain situations that they tend to search for environmental cues for guidance. Hence, depending on the context, their privacy concerns can be varied from extreme concern to empathy with the situation. Then, malleability referred to the ability of people's privacy behavior to be influenced by intentionally designed "nudge" or environmental cues, such as default settings to public information on social networks. As shown in Figure 1, all of the streams together explained the privacy behavior of people in various privacy situations.

Figure 1

Privacy Research Streams and Potential Gaps



However, in our knowledge, prior findings mainly studied privacy related to demographic information or based on established privacy behaviors of people, e.g., using social media, e-commerce, internet privacy concerns. Moreover, this study fills the gap in the lack of studies in privacy and the government's use of FRT context. As there are growing needs for data in the AI era and needs for government control, biometric information and FRT seem to be timely. Thus, this literature needs further findings on how people behave in this situation. Also, a link between ELM to examine attitude changes and privacy calculus theory to predict behavioral intention and privacy disclosure would establish a more straightforward approach for privacy research. Furthermore, the setting of this study would provide richer materials for public settings on how manipulations impact the calculus and decision-making process and detect potential factors that can affect privacy behavior.

Research Model and Statement of Hypothesis

Intrusiveness and government intrusion

According to prior studies, adding privacy to surveillance technology should lessen concerns and increase acceptance. Currently, most of the applications of FRT identifies people in photos, videos, or in real-time. It can easily collect personal information such as name, gender, race, police record, age, etc. Such application is perceived to harm privacy rights and has caused controversies in France, Germany, and UK (Nesterova, 2020). However, an anonymized version of FRT will make individuals unidentifiable from the collected data, thus ensuring privacy. It would automatically pixelate or blur the captured face data and only collect necessary data for its security purpose (Klomp et al., 2021). This study examines whether a low intrusive technology, such as anonymized face mask detection surveillance, decreases citizens' perceived government intrusion concerns.

H1a: High (low) level of intrusiveness increases (decreases) perceived government intrusion concerns.

Distraction and government intrusion

There has been a lack of focus from scholars regarding the impact of distraction on privacy trade-offs. Most studies in marketing literature supported the doctrine that distraction would reduce concentration, leading to activation of peripheral route processing of the ELM model. In other words, the distraction will lead to lower concentration which leads to privacy disclosure. This finding is commonly found in advertising studies where ad banners are the distractor (Altmann et al., 2014; Rejer & Jankowski, 2017; Sagarin et al., 2003). Ongoing research from Becker et al. (2019) also proposed the same impact of distraction on privacy behavior.

As discussed earlier, a distraction from a focal task can either decrease or enhance people's attitude toward a message. Petty et al. (1976) proved that when persuasive communication favors a topic, the distraction activates central route processing and negatively impacts people's attitudes. For this study, the text about face mask detection surveillance is portrayed as a favorable solution to limit the spread of COVID-19 disease. Hence, we argue that the distraction will activate central route processing and decrease people’s favorable attitude, which will lead to greater perceived government intrusion concerns.

H1b: High (low) distraction, in the context of face mask detection surveillance solution, increases (decreases) government intrusion concerns.

Privacy Calculus in Government Surveillance

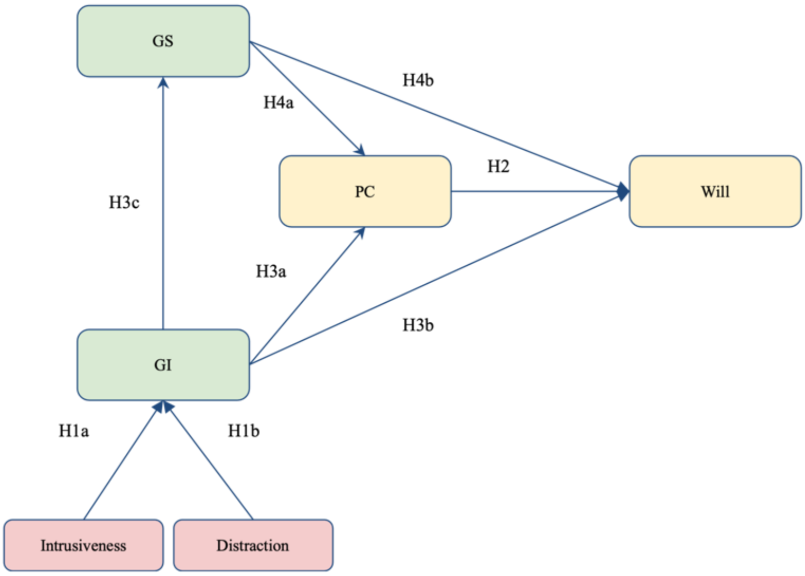
On the one hand, prior studies confirmed that perceived government intrusion concerns negatively impact individuals’ privacy concerns. On the other hand, the belief that the government should increase national security decreases both perceived government intrusion concerns and privacy concerns. Thus, the balance and trade-off between government intrusion and perceived needs for government surveillance intercorrelate with privacy concerns. Then, similar to Dinev et al.’s (2008) study, the three constructs will individually impact the individual’s willingness to support.

In this study, we replicate Dinev et al.’s (2008) findings in the Internet privacy context to public surveillance privacy context. The COVID-19 pandemic can increase the perceived need for surveillance, while FRT can increase perceived government intrusion concerns and privacy concerns (Figure 2)

Still, we hypothesize that similar effects from Dinev et al.’s (2008) Internet privacy context will occur in FRT in public settings.

Figure 2

Privacy Calculus Model



H2: Privacy concerns are negatively related to the willingness to support face mask recognition surveillance

H3a: Government intrusion concerns are negatively related to the willingness to support face mask recognition surveillance

H3b: Government intrusion concerns are positively related to privacy concerns

H3c: Government intrusion concerns are negatively related to perceived need for government surveillance

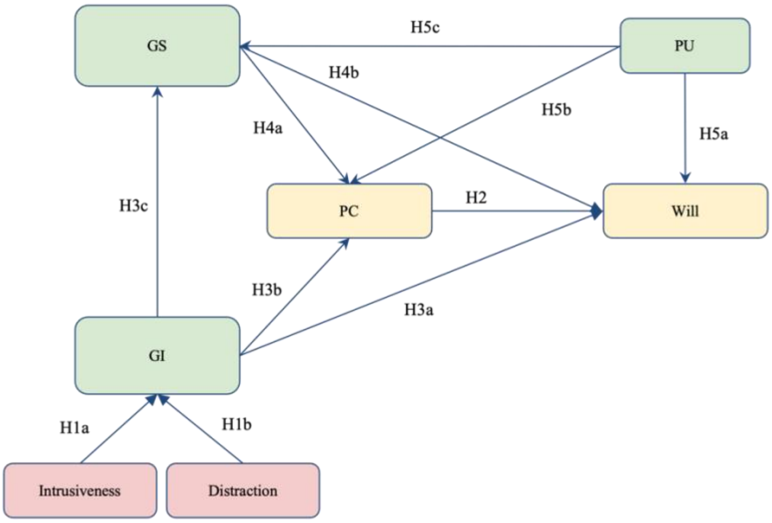
H4a: Perceived need for government surveillance is negatively related to privacy concerns

H4b: Perceived need for government surveillance is positively related to the willingness to support face mask recognition surveillance

As countries transition out of lockdown, face mask-wearing and social distancing will become the longer-term norm. Face mask detection surveillance has the potential to ensure a sustainable transition back to the normality of everyday life. It can support the return to work while providing public security in health, safety, and social order. Thus, the usefulness of the technology is unquestionable. However, to achieve the benefits for the greater common good, citizens must suspend their privacy concerns. They also must trust the government that the benefits of the application of FRT will outweigh the potential risks (Figure 3). Hence, we hypothesize that the perceived usefulness of FRT positively impacts privacy intention/willingness to support FRT surveillance.

Figure 3

Privacy Calculus Model With Covariation of PU



H5a: Perceived usefulness is positively related to privacy intention /willingness to support FRT in public settings.
H5b: Perceived usefulness is negatively related to privacy concerns.
H5c: Perceived usefulness is positively related to perceived needs for government surveillance.

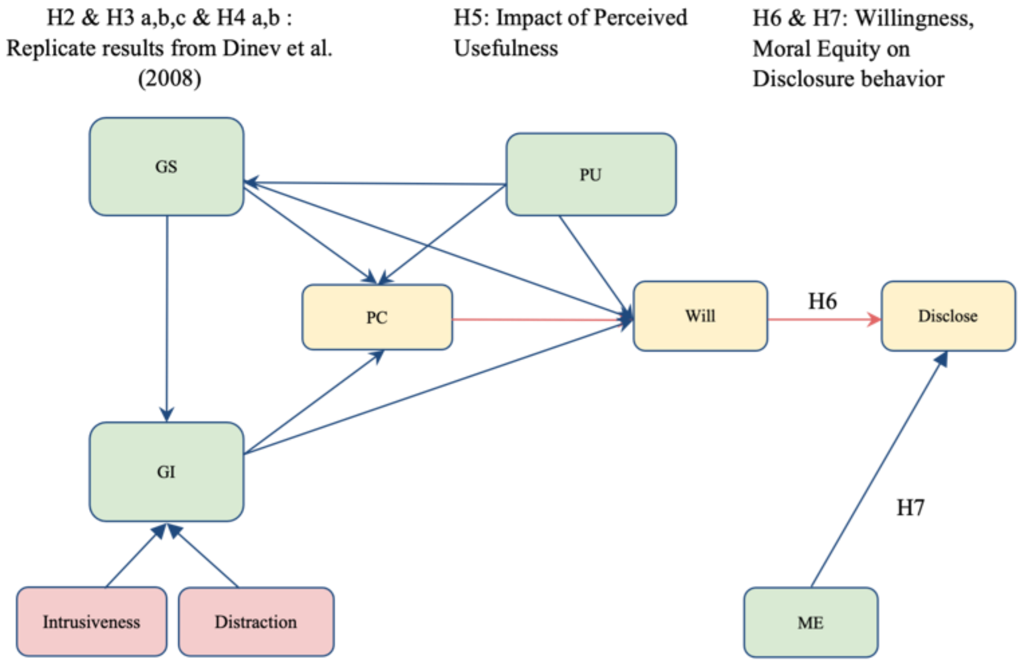
Privacy Trade-off in Government Surveillance

Moral Equity in privacy trade-offs

As the above discussion, willingness or privacy behavioral intention has been widely regarded as an intuitive, primary factor of privacy disclosure (Dienlin & Trepte, 2015; Norberg et al., 2007; Taddicken, 2014). Furthermore, a sequential relationship during the privacy trade-offs from privacy concern to willingness to privacy disclosure has been confirmed by researchers (Dienlin & Trepte, 2015; (Princi & Kramer, 2020). As Figure 4, in a dilemma between perceived usefulness of FRT amid COVID-19 Pandemic and sacrificing people's privacy, the moral consideration in accepting the technology should play a vital role (Anton et al., 2021). Furthermore, with recent evidences related to privacy paradox, we hypothesized a latent factor such as moral equity, besides willingness, would be a potential predictor for actual disclosure.

Figure 4

Full Theoretical Model


H2 & H3 a,b,c & H4 a,b : Replicate results from Dinev et al. (2008)
H5: Impact of Perceived Usefulness
H6 & H7: Willingness, Moral Equity on Disclosure behavior
GS
PU
PC
Will
H6
Disclose
GI
H7
Intrusiveness
Distraction
ME

H6: Willingness to support the technology's implementation positively impact actual disclosure
H7: Moral Equity positively impacts Disclosure in the Decision-making process.

Methodology

In this study, we conducted an anonymous online survey experiment with a 2x2 between-subjects design. It was developed and administered using the Qualtrics platform. The data were gathered on Prolific, a European online panel, on June 2021, then analyzed using SPSS 27.

The survey begins with a reading task about introducing a new governmental AI solution to reduce the contagion of COVID-19 disease. The second section asked about their evaluation of the AI solution. Then, the last section asked some general questions such as demographics.

Study Context

Governments are using face mask recognition surveillance to limit the spread of coronavirus disease. Russia, China, India, and South Korea have used FRT for contact tracing and enforcing COVID-19 regulations such as quarantines, face mask-wearing, and social distancing (Roussi, 2020). Some western countries, for example, France, started using FRT to check if people are wearing masks on public transport. Unlike Russia and other mentioned Asian countries, France's FRT protects the privacy and only collects anonymous statistical data to guide authorities' decision-making (Vincent, 2020). Thus, the text on our survey has two FRT intrusiveness conditions: identifiable and anonymized. (See Appendix 1)

Pre-test

We conducted a pre-test to check that the text and questions were understandable, the length was appropriate, especially if our intentional manipulation is effective. For this pre-test, we took out time constraints to measure the respondents' actual time reading the text and finishing the survey. On average, our respondents used more time than we intended. We also tested two versions of our distraction manipulation: the counting task. In one version, eight red dots appear in 30 seconds at once, which can cause more potent distractions while reading the text. While in the other version, eight red dots appear one by one in 30 seconds, which can cause a weaker distraction. We modified our survey based on all the feedback accordingly. We took out repetitive questions to decrease the length, added a progress bar, simplified questions to make it understandable, and used the weaker version of our distraction manipulation.

Research design and procedure

Table 4

Research Design, measured factors, and measurement scale

Research Design	**Step 1: Online Experiment**		**Step 2: DV Measurements**			**Step 3: Variable Mesuarements**
Experiment & Survey Flow	**Manipulation 2 x 2 ANOVA** Distraction (Yes/No) x Intrusiveness (Yes/No)	Article Reading Task	Willingness to support	Type of information allowed to collect by FRT	Try the Technology	Thought Listings & Survey
Measured Factors	Distraction Intrusiveness		Will	Type of information	Disclose	PC, PU, GI, GS, GT Social, Demographic Data
Scale	Binary		7 Point – Likert Scale	Selected & Ranked data	Binary	7 Point – Likert Scale Nominal data

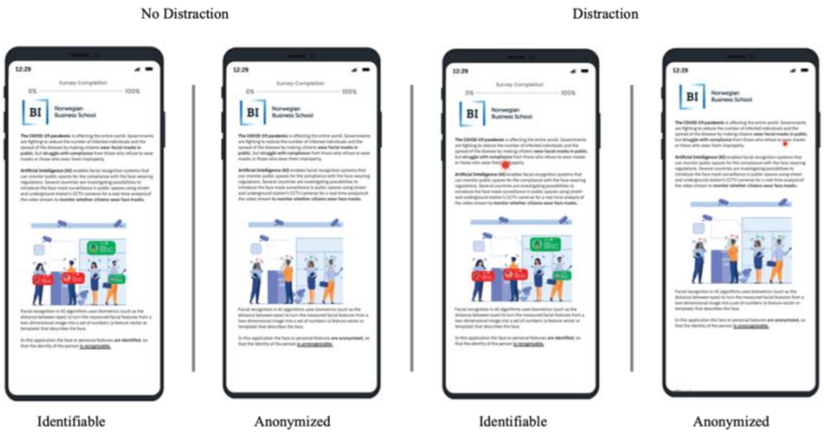
As described in table 4, the research design includes three steps.

Step 1: Online Experiment

The online experiment had 2x2 (Distraction x Intrusiveness) between-subjects designs, and respondents were randomly assigned to each condition. All four conditions were identical in the main text of the article, or position, number of cameras, number of people in the pictures to avoid potential invalidity in the experiment (Figure 5). The only differences are intrusiveness and distraction, as described in Appendix 1.

Figure 5

Four Conditions

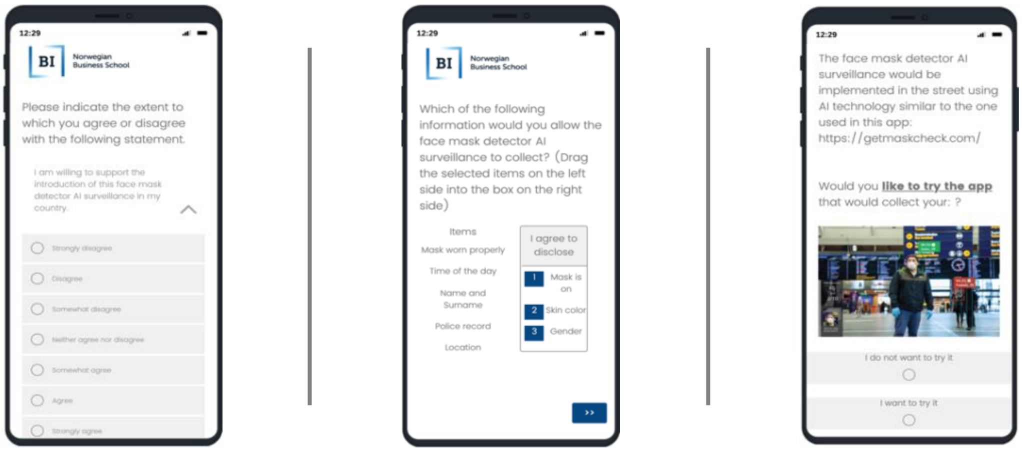


Step 2: Dependent Variable Measurement

In the second section of our survey, we asked respondents to evaluate the introduction of the FRT solution in public spaces, see Figure 6. Here, we intend to measure our dependent variables such as willingness to support FRT surveillance solution (privacy disclosure intention), types of information they agree to share, and intent to try the technology (privacy disclosure behavior).

Figure 6

Dependent variables measurement



12:29

BI Norwegian Business School

Please indicate the extent to which you agree or disagree with the following statement.

I am willing to support the introduction of this face mask detector AI surveillance in my country.

○ Strongly disagree
○ Disagree
○ Somewhat disagree
○ Neither agree nor disagree
○ Somewhat agree
○ Agree
○ Strongly agree

12:29

BI Norwegian Business School

Which of the following information would you allow the face mask detector AI surveillance to collect? (Drag the selected items on the left side into the box on the right side)

Items	I agree to disclose
Mask worn properly	1 Mask is on
Time of the day	2 Skin color
Name and Surname	3 Gender
Police record	
Location	

››

12:29

The face mask detector AI surveillance would be implemented in the street using AI technology similar to the one used in this app: https://getmaskcheck.com/

Would you **like to try the app** that would collect your: ?

I do not want to try it
○
I want to try it
○

Willingness

Type of information allowed to collect

Try the technology

Step 3: Variables measurements

Table 5

Operationalization of constructs

Construct	Items	Scale	Source
Privacy Concerns	3	7-Likert scale (from 1 "Strongly Disagree" to 7 "Strongly Agree")	Dinev et al. (2008)
Perceived Usefulness	3	7-Likert scale (from 1 "Strongly Disagree" to 7 "Strongly Agree")	Venkatesh & Davis (2000); Anton et al. (2021)
Perceived Need for government surveillance	4	7-Likert scale (from 1 "Strongly Disagree" to 7 "Strongly Agree")	Dinev et al. (2008)
Government Intrusion Concerns	3	7-Likert scale (from 1 "Strongly Disagree" to 7 "Strongly Agree")	Dinev et al. (2008)
Moral Equity	5	7-point Likert scale	Anton et al. (2021)
Willingness to support/Privacy Intention	1	7-Likert scale (from 1 "Strongly Disagree" to 7 "Strongly Agree")	Self-generated
FRT acceptance/Privacy Disclosure	1	(I do not want to try it; I want to try it)	Self-generated

In the final section, we asked them their perceptions of constructs in Table 5 that could explain their choices and behavior. It includes their privacy concerns, perceived usefulness of FRT, their perceived need for government surveillance, government intrusion concerns. Finally, the survey ended with control measurements such as government trust, COVID-19 fear, and demographic information.

Manipulation checks

We included attention and manipulation checks to examine respondents' engagement and whether they understood the assigned scenario.

Data Collection

Data Screening

The data were gathered on Prolific, a European online panel, and collected on Qualtrics from a sample of 603 respondents with £1.10 incentives per respondent. We took a conservative approach in cleaning and sorting out our data. The data were filtered for pre-designed validation choices. Of 603 respondents, 3 did not consent, and they were automatically excluded from the study. 185 respondents were removed due to manipulation check and 15 due to attention check. There were 203 respondents excluded from our research and 400 respondents left to use for our data analysis, with a ratio of 22 observations per variable.

Besides, univariate outlier examination was conducted on the sample (N=400) by calculating the z-score of each variable (Appendix 2) to define cases with z-score outside the acceptable range. According to Wheeler and Chambers (1992), the outlier would have the absolute value of z-score larger than 3. This threshold showed that there are 29 on 400 cases that would be classified as outliers. However, Tabachnick and Fidell (2013) suggested that an acceptable range of z-score could be within ± 3.29. This more extensive range revealed that there are 10 outliers in 400 cases. The outliers appeared in items of perceived government surveillance construct.

Specifically, there is a particular case showed a clear pattern of an outlier who rating all construct’s items equally except for government surveillance construct with an extreme value of “7” on 1 item, while the other 3 item is “1”. Hence, this case would be excluded after carefully examining its effects on the results, all the main effects of this study were unchanged.

In summary, we decide to exclude one outlier while keeping the rest from the case (N = 399) because these outliers were not caused by data entry errors, measurement errors but genuinely extreme perception of respondents. To reduce the effect of outliers on later analysis, the data would be examined with skewness and kurtosis statistics in items measurement section.

Data and Sample Descriptive

Manipulations

In this study, manipulation variables would be coded as binominal variables with “0” and “1”. Thus, the distraction would be coded as “1” in case of distraction, and “0” in non-distracted condition. Intrusiveness would be coded as “1” in identifiable FRT, as high intrusiveness, and “0” with anonymized FRT, as low intrusiveness.
Respondents would be assigned to each of four conditions randomly and equally. After the data filtering and screening process, each condition had a fairly equal percentage of total cases, in Table 6.

Demographics

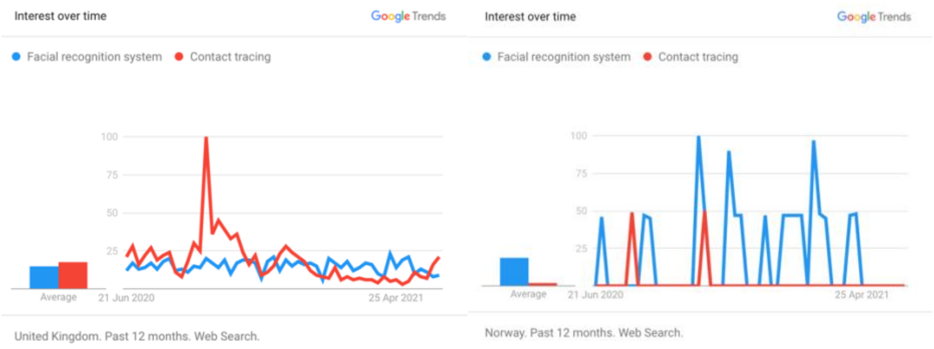
The sample had most respondents (96.7%) from the United Kingdom of Great Britain and Northern Ireland (UK), while 3.3% from the United States of America. The recruitment procedure focused on citizens from countries where FRT’s awareness has been pervasive to reduce the bias from asymmetric knowledge among respondents.

Figure 7

Google Trends related to FRT and contact tracing

Data Source: Google Trends

(https://trends.google.com/trends/explore?geo=GB&q=%2Fm%2F02vghg,%2Fm%2F05rbkm)



According to Google trends, UK's interest over the past 12 months in facial recognition has been close to their interest in contact tracing solutions. In comparison, Norway shows low interest in contact tracing but high interest in facial recognition, see Figure 7. Thus, the UK respondents' sample should avoid the bias of a single possible solution for COVID-19 that could positively impact the attitude toward FRT and create history confound, which can harm the validity of the study's results.

Table 6

Demographic descriptives

Baseline Characteristic	Non-distraction				Distraction					
	Anonymized		Identifiable		Anonymized		Identifiable		Full Sample	
	n = 113		n = 90		n = 109		n = 87			
	n	%	n	%	n	%	n	%	n	%
Country										
United Kingdom	109	96	89	99	105	96	83	95	386	97
United States of America	4	4	1	1	4	4	4	5	13	3
Gender										
Female	70	62	63	70	77	71	57	66	267	67
Male	41	36	23	26	28	26	28	32	120	30
Third gender/binary	1	1	1	1	3	3	0	0	5	1
Prefer not to answer	0	0	2	2	0	0	2	2	4	1
Other	1	1	1	1	1	1	0	0	3	1

Due to our conservative data cleaning approach, our targeted distribution of demographic characteristics has been changed correspondingly. For example, females occupy 66.9% (N=267) of our current data sample. This uneven split could have a potential effect on our findings. See Appendix 3 for the summary of our respondents' characteristics.

Scaling and measurements

Most of our items to measure the constructs in our model were based on validated instruments from previously published research. The items to assess perceptions (PU, PC, ME, GI, and GS) and willingness (coded as Will) were measured on 7-point Likert scales from 1 “Strongly Disagree” to 7 “Strongly Agree.” While our privacy disclosure (coded as Disclose) behavior/acceptance of the FRT trial was measured by “I do not agree to try it” and “I agree to try it.” A detailed overview of sources of the constructs, number of items, and scales are provided in table 5.

As presented in Appendix 4, moral equity items had the highest skewness statistic of .196 *(SE=.122)*, kurtosis of -.913 *(SE=.244)* with ME3; While perceived usefulness had lowest skewness statistic of -.336 *(SE =.122)*, kurtosis of -.981 *(SE=.244)* with PU1. Hence, according to Brown (2011), items of perceived usefulness (PU), moral equity (ME) would have approximately symmetric distribution (skewness between ± ½).

Privacy concerns and government intrusion concerns were highly negatively skewed and moderately negatively skewed, reflecting that most responses showed high privacy concerns and perceived government intrusion in the FRT context. The need for government surveillance had positive-skewed, revealed most respondents had a relatively low demand for surveillance from the public sector. According to Hair et al. (2010), initial observation pointed that all items have skewness (between ± ½) and kurtosis (between ±2) statistic in the acceptable range for further analysis, except for the GS2 item *“The government needs to have greater access to individual bank accounts.”* GS2 showed an abnormally high kurtosis of 8.414 *(SE=.244)*, which is much higher than 3. This statistic showed that GS2 had a higher and shaper central peak and longer, fatter tail, indicating that the item might not be suitable for further sophisticated analysis that requires normality of variable.

In summary, the 7 points Likert-scale naturally reflects the evaluation of a specific statement and topic, which can observe respondents' different views. Furthermore, skewness and kurtosis statistics of item measurements would be appropriate for further analysis in this study except for the GS2 item.

Principal Component Analysis

In this analysis, we perform principal component analysis (PCA) with 12 items to measure 399 respondent’s evaluation toward four constructs, including perceived usefulness (3 items), privacy concerns (3 items), perceived needs for government surveillance (3 items, GS2 was excluded), and government intrusion (3 items). The moral equity construct and its item were measured in a different semantic scale with the purpose of examining whether moral equity plays a role in the decision-making process with a close relationship to privacy behavior. Hence, this construct would be analyzed separately in the latter part of the study.

The suitability of PCA was accessed prior to analysis. Inspection of the correlation matrix showed that all items had at least one correlation coefficient greater than 0.3 (Appendix 5). Then, Kaiser-Meyer-Olkin (KMO)'s measure of sampling adequacy of 12 items is .86 with all individual KMO measures greater than 0.799, classification of ‘meritorious’ (Kaiser, 1960). Furthermore, Bartlett's Test of Sphericity was significant with $\chi 2(66) = 3873.326$, $p < .001$, indicating that data was likely factorizable.

We used principal components analysis because the primary purpose was to identify and compute composite scores for the factors underlying the 12 items. PCA revealed four components with initial Eigenvalues greater than 1, which explained 48.28%, 16.12%, 10.22%, and 9.21% of the total variance, respectively. The fourth to twelfth factors had eigenvalues over 1, and each explained the rest of 16.1% of the variance.

The four-component solution explained 83.827% of the variance, was preferred because of: (a) previous theoretical support; (b) the 'leveling off' of eigenvalues on the scree plot after four factors, and (c) the insufficient number of primary loadings and difficulty of interpreting the fifth factor and subsequent factors.
A Promax oblique rotation was employed to aid interpretability. According to Thurstone (1931), the rotated solution should reveal 'simple structure' as Table 7.
Furthermore, the solution was adopted to retain the naturally intercorrelate between constructs.

Table 7

Results of a Principal Component Analysis of Privacy – related items

Privacy-related Items	Component Loading				**Cronbach's alpha**
	1	2	3	4	
Component 1: Perceived Usefulness (PU)					
PU1 - Using face mask detector AI surveillance technology would increase public safety from COVID-19 contamination	**.99**	.05	-.01	-.02	0.958
PU2 - Using face mask detector AI surveillance would increase my safety from COVID-19 contamination	**.97**	.00	.01	-.02	
PU3 - I find face mask detector AI surveillance useful to prevent COVID-19 contamination	**.94**	-.06	.01	-.01	
Component 2: Privacy Concern (PC)					
PC1 - I am concerned that the information collected by government in this way could be misused.	-.05	**.88**	.02	-.05	0.937
PC2 - I am concerned about allowing the collection of information because the data could be used in a way I did not foresee.	-.05	**.94**	-.02	-.01	
PC3 - I am concerned about submitting information to the system because of what others might do with it (e.g., if third parties hack the data).	.08	**1.00**	-.02	.05	
Component 3: Perceived Government Intrusion (GI)					
GI1 - I am concerned that my internet accounts and database information (e.g., e-mails, shopping records, tracking my Internet surfing, etc.) will be more open to government/business scrutiny.	.02	.15	**.82**	.04	0.84
GI2 - I am concerned about the government's ability to monitor internet activities.	.10	.06	**.90**	-.02	
GI3 - I am willing to take additional actions to avoid tracking	-.11	-.18	**.89**	.00	
Component 4: Perceived Needs for Government Surveillance (GS)					
GS1 - The government needs to have greater access to personal information.	.18	-.08	-.02	**.70**	0.82
GS3 - The government needs broader wiretapping authority.	-.13	.05	.08	**1.02**	
GS4 - The government needs to have more authority to use high tech surveillance.	.04	.00	-.10	**.80**	

Extraction Method: Principal Component Analysis.
Rotation Method: Promax with Kaiser Normalization.
Rotation converged in 6 iterations.

$\chi 2$ (66) = 3873.326, p < .001

The interpretation of data was consistent with the privacy-related constructs were designed to measure with strong loadings of perceived usefulness (PU) items on Component 1, privacy concern (PC) items on Component 2, perceived government intrusion (GI) items on Component 3, and perceived needs for government surveillance (GS) on Component 4. Each component would be extracted as a component score using a regression method to reflect its corresponding respondent's privacy-related construct.

Construct Validity

As a result of PCA, privacy-related constructs reflected items in the questionnaire in a simpler structure, consistent with previous findings. Furthermore, the analysis of internal consistency of each construct showed relatively high Cronbach's alpha > 0.8 in all four constructs, consisting of PU with 3 items *(α = .958),* PC– 3 items *(α = .937),* GS – 3 items *(α = .820), and* GI – 3 items *(α = .840).*

Consistent with the above analysis of items' skewness, the GS2 was excluded and caused a higher Cronbach's alpha (from *α = .810 to α = .820*), which also increase the internal consistency of the construct and validity of the underlying factor in the principal components analysis (CPA).

Result

Correlations between variables

Firstly, despite the skewness and kurtosis statistic of variables showed a decent level of symmetric distribution, variables in this study hardly qualified as perfect normal distribution due to the limited number of recruited respondents (N = 399).

Hence, a Spearman's rank-order correlation was run to assess the relationship between variables. The correlations between variables, as the table below, suggest a significant relationship between PU, PC, GI, GS, and dependent variables, including Will and Disclose.

Distraction has no significant correlation with both Willingness (r_s(397) = .002, p > .05) and Disclosure (r_s(397) = .006, p > .05), while Intrusiveness has a significant - negative relationship with Willingness (r_s(397) = -.119, p < .05). From these initial findings, the manipulation have low significant impact on dependent variables.

According to table 8, intention and behavior variables, including Willingness and Disclosure, showed a significant and high magnitude relationship with privacy-related constructs from PCA component scores. These variables also preserved natural intercorrelation due to obligin rotation method.

Table 8

Results of Spearman's rank – order correlations

Variable	n	M	SD	Distract	Intru	Will	Disclose	PU	PC	GI	GS
Distract	399	.491	.501	--							
Intru	399	.444	.497	0.001	--						
Will	399	3.7	1.99	0.02	-.119*	--					
Disclose	399	.303	.460	0.006	-0.073	.438**	--				
PU	399	.000	1.00	-0.003	0.015	.746**	.397**	--			
PC	399	.000	1.00	0.053	.144**	-.528**	-.294**	-.414**	--		
GI	399	.000	1.00	.100*	.115*	-.404**	-.215**	-.319**	.513**	--	
GS	399	.000	1.00	-0.039	-0.085	.524**	.311**	.455**	-.503**	-.467**	--

*. Correlation is significant at the 0.05 level (2-tailed).

**. Correlation is significant at the 0.01 level (2-tailed).

Impact of manipulation on perceived government intrusion

Based on Elaboration Likelihood Model, H1a and H1b aimed to test the impact of manipulation (intrusiveness and distraction) on perceived government intrusion as the belief, attitude of respondents toward FRT in the public setting.

A 2x2 ANOVA was conducted to examine the effect of distraction (Yes, No) and intrusiveness (identifiable FRT, anonymized FRT) on perceived government intrusion. A Shapiro-Wilk's normality testing for each cell of the design also was conducted (p > .05) for 3 cells, except for the no distraction and no intrusion condition (p = 0.08). However, normality testing with dependent's overall residuals analysis also using Shapiro-Wilk's test showed the null hypothesis of normality assumption was not rejected (*p* =0.09). There was homogeneity of variances, as accessed by Levene's test for the equality of variances, p = .066.

Table 9

Results of 2x2 ANOVA - Distraction and Intrusiveness on Government Intrusion

Dependent Variable: Government Intrusion

Source	Sum of Squares	df	Mean Square	F	Sig.	Partial η^2
Distract	4.645	1	4.645	4.751	.030	.012
Intru	6.804	1	6.804	6.960	.009	.017
Distract * Intru	.868	1	.868	.888	.347	.002
Error	386.148	395	.978			

a. R Squared = .030 (Adjusted R Squared = .022)

From the results table 9 and descriptive statistic - table 10, there were statistically significant main effect on perceived government intrusion (GI) of distraction, F(1, 395) = 4.751, $p < .05$, partial η^2 = .012. Thus, H1b was confirmed that people in distraction had statistically significant higher GI (M = .105, SD = .950) than non-distraction (M = -.102, SD =1.038). Besides, there were significant main effect of intrusiveness, with F(1, 395) = 6.960, $p < .05$, partial η^2 = .017, on GI as well. Then, H1a was confirmed when people perceived identifiable FRT (M = .145 , SD = .911) was statistically significant higher GI than anonymized FRT technology (M = -.116, SD = 1.053).

However, the interaction effect between distraction and intrusiveness (Figure 8) was not statistically significant F(1, 395) = .888, p = .347, partial η^2 = .002.

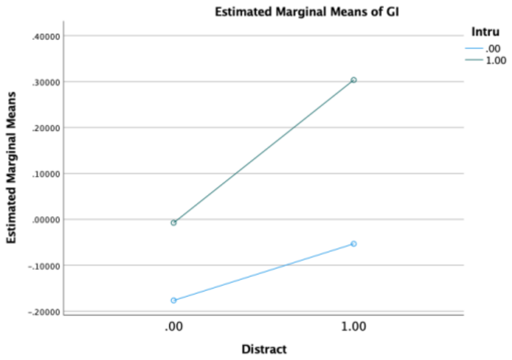
Table 10

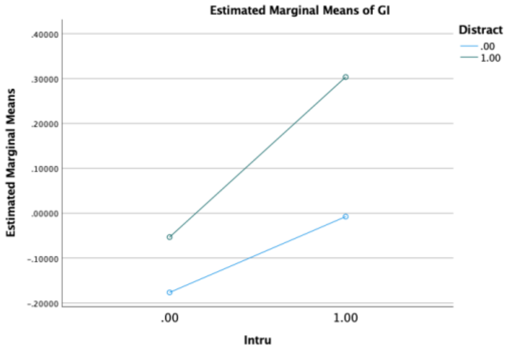
Descriptive statistics of Perceived Government Intrusion

	Mean	SD	n
Non-Distraction			
Anonymized	-0.176	1.103	113
Identifiable	-0.008	0.948	90
Total	-.102	1.038	203
Distraction			
Anonymized	-0.053	0.999	109
Identifiable	0.304	0.849	87
Total	.105	.950	196
Total			
Anonymized	-.116	1.053	222
Identifiable	.145	.911	177
Total	0.00	1.00	399

Figure 8

Effects of manipulations on Government Intrusion





In summary, H1a and H1b were confirmed with main effects from intrusiveness and distraction to increase GI.

Impact of manipulation on Privacy Disclosure behavior

As an initial finding of a correlation between variables, distraction and intrusiveness seem not to affect behavior. A Chi-square test of independence could be conducted to measure association between non-parametric variables. However, we preferred a 2x2 ANOVA analysis to examine effect of manipulations on privacy disclosed behavior. The 2x2 ANOVA possibly still provides reliable results with the dichotomous dependent variable (Disclose) by satisfying conditions of Lunney (1970).

Despite the results showed no main effects of both distraction and intrusiveness, the interaction effect of distraction and intrusiveness (F(1, 395) = 3.659, p = .056, partial η^2 = .009) was marginally significant. Hence, we examined which factor drive the impact.

Table 11

Results of 2x2 ANOVA - Distraction and Intrusiveness on Privacy Disclosure

Dependent Variable: Privacy Disclosure

Source	Sum of Squares	df	Mean Square	F	Sig.	Partial η^2
Distract	.002	1	.002	.009	.926	.000
Intru	.473	1	.473	2.251	.134	.006
Distract * Intru	.770	1	.770	3.659	.056	.009
Error	83.080	395	.210			

a. R Squared = .015 (Adjusted R Squared = .007)

Table 12

Univariate Tests for simple main effect

Dependent Variable: Disclose

Distract		Sum of Squares	df	Mean Square	F	Sig.	Partial η^2
.00	Contrast	.018	1	.018	.087	.769	.000
	Error	83.080	395	.210			
1.00	Contrast	1.204	1	1.204	5.725	.017	.014
	Error	83.080	395	.210			

Each F tests the simple effects of Intru within each level combination of the other effects shown. These tests are based on the linearly independent pairwise comparisons among the estimated marginal means.

The univariate test in table 12 showed that there was a statistical difference in the probability to disclose information between identifiable and anonymized FRT technology of distracted people, F(1, 395) = 5.725, p = .017, partial η^2 = .014, proved the simple main effect of intrusiveness. However, the simple main effect of distraction was not significant.

Table 13

Analyses for interaction of Distraction and Intrusiveness on Disclosure behavior

Dependent Variable: Disclose

						95% Confidence Interval for Difference[b]	
Distract	(I) Intru	(J) Intru	Mean Difference (I-J)	Std. Error	Sig.[b]	Lower Bound	Upper Bound
.00	.00	1.00	-.019	.065	.769	-.146	.108
	1.00	.00	.019	.065	.769	-.108	.146
1.00	.00	1.00	.158*	.066	.017	.028	.287
	1.00	.00	-.158*	.066	.017	-.287	-.028

Based on estimated marginal means

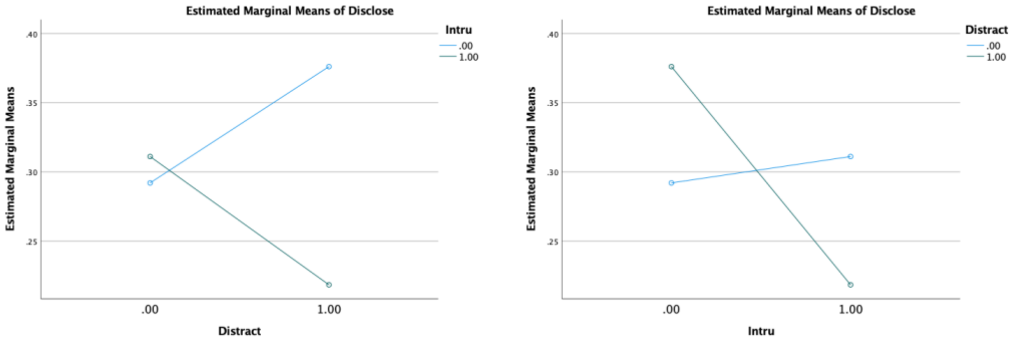
*. The mean difference is significant at the .05 level.

b. Adjustment for multiple comparisons: Bonferroni.

Thus, according to Table 13's result, for people in distraction case, identifiable FRT would decrease the mean "Disclose" of .158 points, 95% CI [-.287, -.028], p = .017.

Figure 9

Interaction effects of manipulations on Disclosure



From Figure 9, this effect confirmed that intrusiveness is the more impactful driver on disclosure as the sole significant simple main effect in the interaction, which can provide different disclosure behavior when people get distracted.

Model of Privacy calculus process

To examine the mediation relationship between these variables as the conceptual framework, we applied the multiple regression with the bootstrapping method, as model 6 of the Hayes PROCESS tool (Hayes, 2017).

In this analysis, we would replicate results from previous studies, including findings of Dinev et al. (2008), where GI, GS, PC together explained Willingness and findings of Chen et al. (2018); Dinev and Hart (2006); Zhang and Kang (2019) about the effect of PU on Willingness. The mediation model with two mediators consisting of GS, PC, and covariates of PU with the sample of 399 responses will be adopted in the regression.

The setting of regression analysis is aligned with the survey setting and previous findings in the literature. Hence, for each respondent, after reading in one of four conditions, people would have a certain attitude, perceived concern about government intrusion resulting from information processing routes in the EML model. Meanwhile, Willingness to support should represent the result of privacy calculus.

The assumptions testing for multiple regression were conducted in each path within model 6. According to Appendix 4, the normality assumption was moderately satisfied with approximately symmetric distribution of Will (skewness statistic of .087, SE =1.22) and acceptable in case of GS, PC (kurtosis statistic < 3). Furthermore, there were independence of residuals, assessed by a Durbin–Watson statistic of 1.917 (Will), 1.845(PC), and 1.961 (GS). There were homoscedasticities in GS, PC, and Will, as accessed by visual inspection of plots of studentized residuals versus unstandardized predicted value. Also, no evidence of multicollinearity with all tolerance value greater than 0.1. There were some outliers detection, but we decide to keep them. All leverage values lower than 0.2 and no values for Cook's distance above 1. Each regression model of direct path significantly predicted dependent variable such as Will (F(4,394) = 164.464, p < .001, adj. R^2 = .622), PC (F(3,395) =77.471 , p < .001, adj. R^2 = .366), and GS (F(2,396) =92.662 , p < .001, adj. R^2 = .315).

Table 14

Result of PROCESS model 6

		Bootstrap results				
Hypotheses	Path				95% bias-corrected CI	
		Estimate	SE	p	Lower	Upper
H3c	GI → GS	-.347***	.043	< .001	-.432	-.261
H5c	PU → GS	.355***	.043	< .001	.270	.441
H3b	GI → PC	.351***	.045	< .001	.262	.439
H4a	GS→ PC	-.233***	.048	< .001	-.328	-.138
H5b	PU → PC	-.194***	.045	< .001	-.283	-.105
H3a	**GI → Will**	-.070	.074	.063	**-.284**	**.007**
H4b	GS → Will	.124**	.076	.001	.096	.397
H2	PC → Will	-.155***	.077	< .001	-.460	-.157
H5a	PU → Will	.611***	.071	< .001	1.074	1.353
Mediation 1	GI → GS → Will	-.043*	.013		-.070	-.018
Mediation 2	GI → PC → Will	-.054*	.016		-.090	-.026
Mediation 3	GI → GS → PC → Will	-.013*	.005		-.024	-.005

Note. If bootstrapped 95% confidence intervals (CI) do not include zero, indirect and direct effects are significant (*). There were 5,000 bootstrap samples. All estimates are standardized. *** p < .001, ** p < .01. GI → GS = Perceived Government Intrusion as predictor for Needs for Government Surveillance.

Impacts of factors on GS

The regression analysis showed support for H3c where GI have a significant negative direct effect on GS (β = -.347; 95% CI: [-.432, -.261]; p < .001). Besides, PU have a direct significant positive effect on GS (β = .355; 95% CI: [.270, .441]; p < .001), H5c was supported.

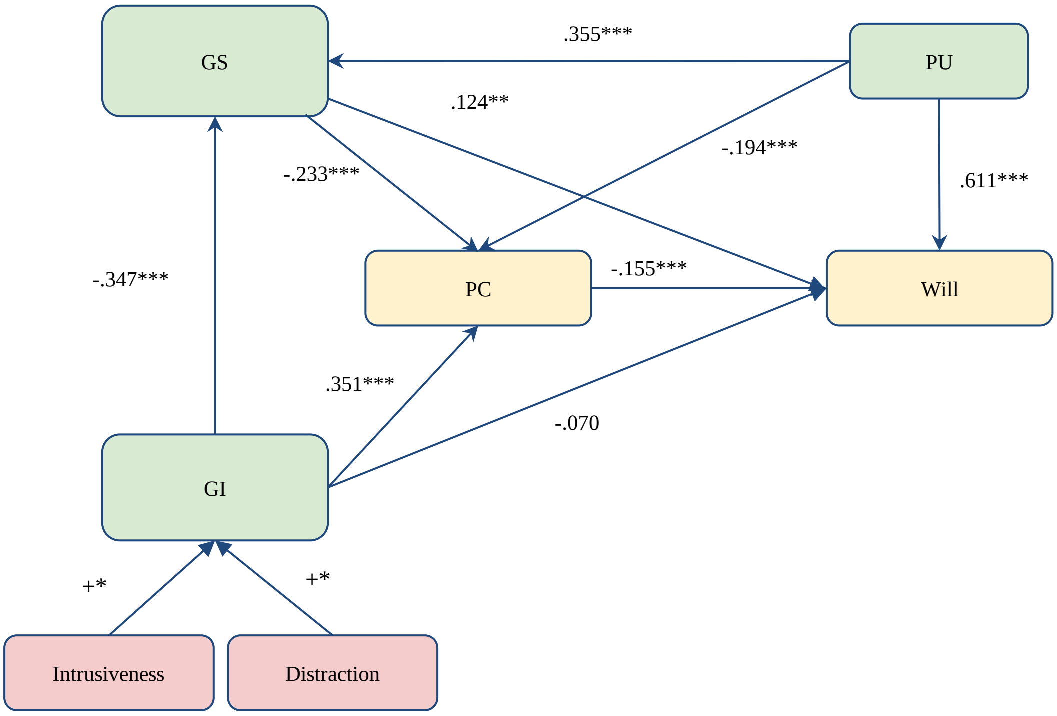
Impacts of factors on PC

The results showed support for H3b where GI have a significant positive direct effect on PC (β = .351; 95% CI: [.262, .439]; p < .001). Meanwhile, GS have a direct significant negative effect on PC (β = -.233; 95% CI: [-.328, -.138]; p < .001), H4a was supported. Similarly, H5b was supported where PU have a direct significant negative effect on PC (β = -.194; 95% CI: [-.283, -.105]; p < .001).

The high intercorrelation between predictors is expected through the initial principal component analysis. However, as the explained variable for constructs, these variables reflected a logical relationship as Figure 10.

Figure 10

Privacy Calculus Model and coefficients



Impacts on dependent variable Willingness

The result showed that GI have a non-significant negative direct effect on Willingness (β = -.070; 95% CI: [-.284, .007]; p = .063). This result showed that

H3a was not supported, which is similar to the finding of Dinev et al. (2008). However, GS, PC, PU have significant direct effect on Willingness with $p < .001$ (Table 14), these results confirmed H4b, H2, H5a. In the model, mediation effect would be tested using the bootstrapping method. If bootstrapped 95% confidence intervals (CI) do not include zero, indirect effects are significant. With Mediation 1 and 2, the effect of GI through mediator GS ($\beta = -.043$; 95% CI: [-.070, -.018]; $p < .05$) and PC ($\beta = -.054$; 95% CI: [-.090, -.026]; $p < .05$) were significant negative on Willingness. The mediation 3 was confirmed in case of the effect from GI to Willingness through GS and PC respectively also was significant negative ($\beta = -.013$; 95% CI: [-.0230, -.0045]; $p < .05$).

Furthermore, the mediation effect would be re-examined with the Sobel test (Preacher & Hayes, 2004; Sobel, 1982). Hence, mediation 1 would be confirmed that mediator GS carries the influence of GI to Will, Sobel test statistic of 3.00, $p < 0.01$. Mediation 2 also confirmed as PC was the mediator between GI and Will with Sobel test statistic of 3.59, $p < 0.01$. The mediation 3 also be supported while PC also be the mediator of GS and Will with Sobel test statistic of 3.08, $p < 0.01$.

Model of Privacy Disclosure

In this part of the analysis, we examined how Willingness impact actual privacy disclosure with H6. The construct ME was analyzed to reveal how moral equity affects the decision-making process. This approach is appropriate according to our survey setting. After the privacy calculus, people selected what type of information they would allow the government to collect via FRT surveillance. Then, they will decide base on a perceived moral consideration of equity.

As discussed above, the ME measure was not included in the PCA process due to its distinguished type of rating. Hence, in the regression, it was presented with all five items. This process should be more effective in understanding how a specific moral consideration impacts the decision-making process.

According to appendix 4, skewness of ME1 is .036 (SE = .122), ME2 is .03 (SE = .122), ME3 is .196 (SE = .122), ME4 is .056 (SE = .122), and ME5 is -.013 (SE = .122), and Will is .087 (SE =1.22). Hence, all of them had approximate symmetric distribution. This result showed that using moral equity items as variables in regression is acceptable. Then, we conducted a binary logistic regression analysis to investigate if moral equity items and willingness to support/privacy behavioral intention predict privacy disclosure behavior.

Firstly, linearity of the continuous variables with respect to the logit of the dependent variable was assessed via the Box and Tidwell (1962) procedure. A Bonferroni correction was applied using all 13 terms in the model resulting in statistical significance being accepted when p < .00384 (Tabachnick & Fidell, 2013). Based on this assessment, all continuous independent variables were found to be linearly related to the logit of the dependent variable. Casewise diagnostics testing showed there was one standardized residual with a value of 2.521, which was kept in the analysis.

The inferential goodness-of-fit test is the Hosmer–Lemeshow (H–L) test that yielded a $\chi2$ (8) of 7.114 and was insignificant (p > .05), suggesting that the model was fit to the data well. Additionally, the logistic regression model was statistically significant, $\chi2$ (6) = 101.715, p < .001. The model explained 31.8% (Nagelkerke R Square) of the variance in privacy disclosure and correctly classified 74.2% of cases. However, only two independent variables were statistically significant, including Will and ME5 (Table 15).

Table 15

Logistic Regression coefficients of variables on Privacy Disclosure

Variables in the Equation	B	S.E.	Wald	df	Sig.	Exp(B)	95% C.I.for EXP(B)	
							Lower	Upper
Will	.313	.119	6.887	1	**.009**	1.367	1.082	1.727
ME1	-.119	.181	.429	1	.513	.888	.622	1.267
ME2	.316	.180	3.070	1	.080	1.372	.963	1.953
ME3	-.056	.151	.140	1	.708	.945	.704	1.270
ME4	-.041	.135	.093	1	.761	.960	.737	1.249
ME5	.305	.115	6.994	1	**.008**	1.356	1.082	1.700
Intercept	-3.839	.407	89.127	1	.000	.022		

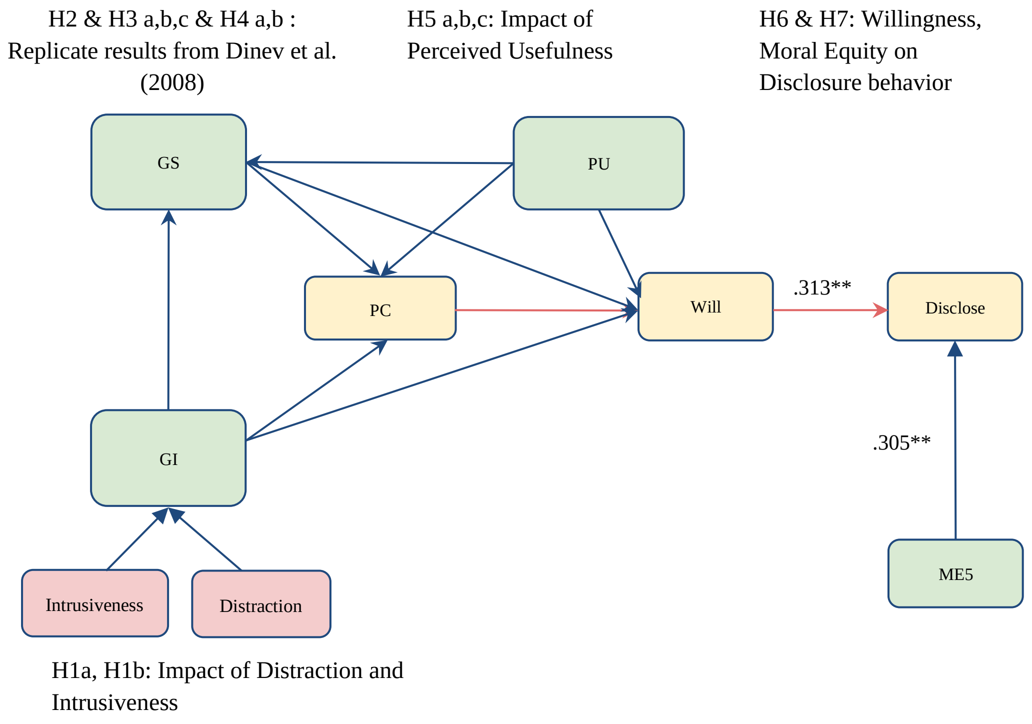
As the result from the logistic regression with dependent variable as privacy disclosure (Disclose) revealed the significant positive impact from Willingness (B = .313, SE = .119, Wald = 6.887, Odds Ratio [95% CI] = 1.367, Nagelkerke's R^2 = 0.318, p < 0.01) was confirmed and support H6.

ME5 had a significant positive impact on disclosure with a positive impact (B = .305, SE = .115, Wald = 6.994, Odds Ratio [95% CI] = 1.356, Nagelkerke's R^2 = 0.318, p < 0.01). Hence, H7 was confirmed only with 7 points Likert-scalce ME5 item *"Accepting face mask detector AI surveillance to combat COVID-19 is unimportant for the society (1) to extremely important for the society (7)"*.

From the result, moral equity showed a significant effect and considerable magnitude on disclosure (Odds ratio 95% CI of 1.356), which was approximate to of willingness (Odds ratio 95% CI of 1.367). These findings confirmed H6 and a part of H7 which were illustrated in Figure 11.

Figure 11

Full theoretical model and coefficients


H2 & H3 a,b,c & H4 a,b :
Replicate results from Dinev et al. (2008)
H5 a,b,c: Impact of Perceived Usefulness
H6 & H7: Willingness, Moral Equity on Disclosure behavior
GS
PU
PC
Will
.313**
Disclose
.305**
GI
ME5
Intrusiveness
Distraction
H1a, H1b: Impact of Distraction and Intrusiveness

In summary, the hypothesis testing was shown in the belowed table.

Table 16

Summary of hypotheses testing

Hypotheses	Results
H1a: High (low) level of intrusiveness would increase (decrease) perceived government intrusion concerns.	Supported
H1b: High (low) distraction would increase (decrease) government intrusion concerns.	Supported
H2: Privacy concerns are negatively related to the willingness to support face mask recognition surveillance	Supported
H3a: Government intrusion concerns are negatively related to the willingness to support face mask recognition surveillance	**Not Supported**
H3b: Government intrusion concerns are positively related to privacy concerns	Supported
H3c: Government intrusion concerns are negatively related to perceived need for government surveillance	Supported
H4a: Perceived need for government surveillance is negatively related to privacy concerns	Supported
H4b: Perceived need for government surveillance is positively related to the willingness to support face mask recognition surveillance	Supported
H5a: Perceived usefulness is postively related to privacy intention/willingness to support FRT in public settings.	Supported
H5b: Perceived usefulness is negatively related to privacy concern.	Supported
H5c: Perceived usefulness is positively related to perceived needs for government	Supported
H6: Willingness to support the technology's implementation positively impact actual disclosure	Supported
H7: Moral Equity positively impacts Disclosure in the Decision-making process.	**Partly Supported**

Further Analysis

Privacy Paradox

The paradox variable was computed according to the phenomenon's definition to examine Privacy Paradox in this study. The paradox was encoded as "0" if there is no paradox and "1" if there is a distinction between respondent's privacy behavioral intention and privacy disclosure behavior.

Table 17

Privacy Paradox cases

Paradox	n	%
.00	298	74.7%
1.00	101	25.3%

People who had privacy paradox (N=101) occupied 25.3% of the total response. Before analyzing the privacy paradox, as discussed above with moral equity, people must consider and select what information they agree to share with the government before the decision. Hence, it's appropriate to have an analysis related to the type of information.

Compute comfortable score on each type of information to disclose

The question about kind of information disclosed had selected and ranked answer (see Figure 6). In which, respondents would select options among 8 information types and rank the priority from “1”. With this setting, “1” would illustrate the most appropriate information, while the last position would show the least desired option. Hence, we recode a new variable name of comfortable score “Score_[info_type]” (Table 18) from the answer about option selection “[info_type]Select” (Yes = 1/No=0) and its ranking as “[info_type]Rank” as:

$$\text{Score\_[info\_type]} = \text{[info\_type]}_{\text{Select}} * (9 - \text{[info\_type]}_{\text{Rank}})$$

This formula intuitively revealed that if a type of information were selected, it would have an extent (score) of comfortable people willing to share with the government. Thus, the higher the score, the more the respondents are **willing to share** that type of information.

Table 18

The comfortable score of providing information

Comfortable score	Information type to disclose
Score_mask1	Mask is on
Score_mask2	Mas wore properly
Score_Gen	Gender
Score_Time	Time
Score_Skin	Skin color
Score_Name	Name
Score_Pol	Police Record
Score_Loc	Location

Type of people

From the comfortable score computing, we explored whether stereotypes of respondents who had different views in information sensitivity would impact the decision-making process in privacy behavior, besides willingness and moral equity, as discussed above. Specifically, we hypothesized that some groups of people would have a higher tendency to have privacy paradox.

Firstly, adapting the clustering process from Milne et al. (2017), we perform a cluster analysis including two-step. At first, the number of clusters would be identified through hierarchical cluster analysis. According to agglomeration schedule coefficients, 3 clusters would be appropriate as Appendix 7, from step 397. Then, we perform a K-mean cluster according to the mean value of variables in each cluster from the previous step. The method is also known to produce tighter clusters (Hair et al., 2010). Hence, we record the cluster membership of each response in the sample (N = 399), where clusters 1, 2, 3 have 218 cases, 108 cases, and 73 cases, respectively.

Table 19 of cluster centers showed a potential pattern in how these groups are willing to share information with the government.

Table 19

Final Cluster Centers

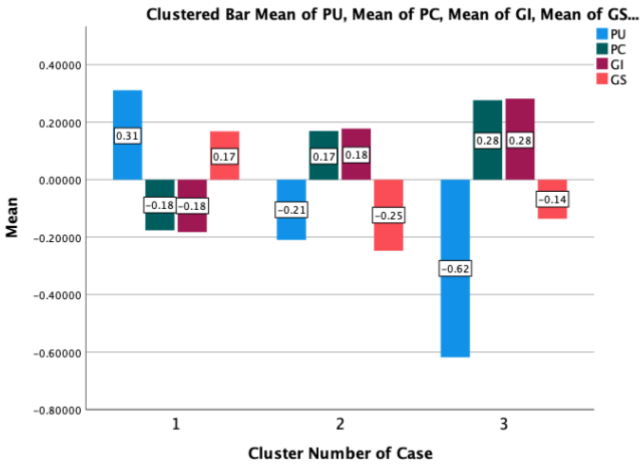
Comfortable scores	Cluster		
	1	2	3
Score_mask1	**7.27**	**7.58**	1.51
Score_mask2	**6.39**	**5.44**	.55
Score_Gen	1.15	.29	2.47
Score_Time	**3.46**	.00	**6.26**
Score_Skin	.56	.10	1.19
Score_Name	1.17	.46	.59
Score_Pol	.43	.11	.97
Score_Loc	**5.06**	.00	3.40

Cluster 1 (N=218) showed a high comfortable score toward providing data related to mask-wearing, time, and location of the surveillance, while Cluster 2 (N=108) tends to share mask-wearing information only. However, Cluster 3 (N = 73) has a different perspective on FRT than the rest of the respondents who perceived low comfortable for all types of information except for time information.

Interestingly, the below Figure showed that there was a different view between cluster 3 and other groups while they have a pretty negative view about FRT technology with much higher privacy concern and perceived government intrusion, much lower perceived usefulness, lower needs for government surveillance.

Figure 12

Differences in PU, PC, GI, GS across cluster

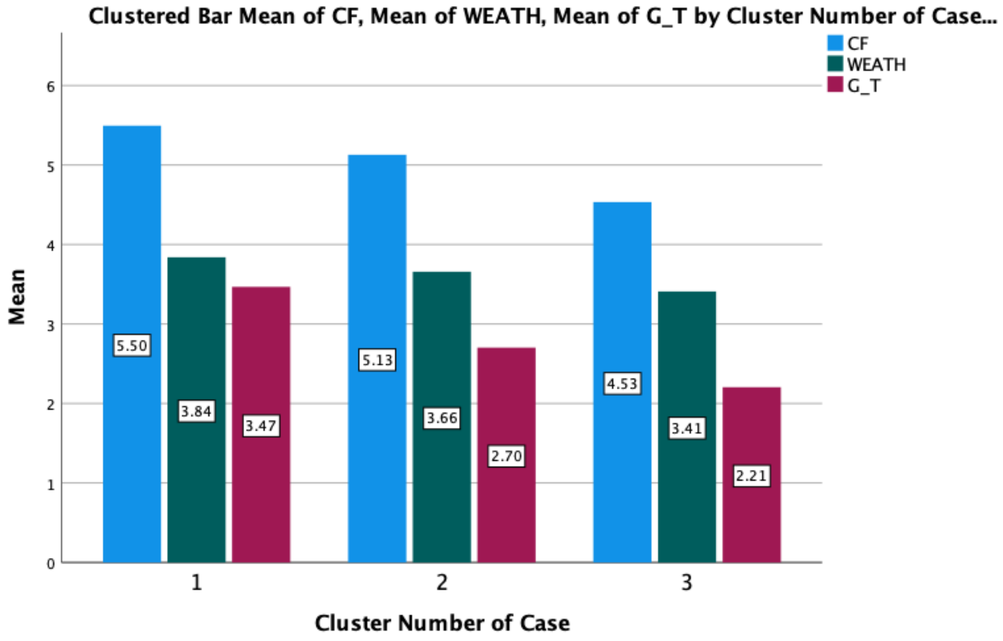


Thus, a quick 3 x 1 ANOVAs between 3 clusters across each dependent variable of PU, PC, GI, GS were conducted. The analysis showed there was a statistically significant difference in means of PU, PC, GI, GS between clusters 1, 2, and 3. Thus, post hoc Bonferroni tests for each ANOVA showed that cluster 1 had the highest PU and lowest PC, while cluster 3 have the lowest PU and highest GI.

The chart below illustrates the differences in demographics of each cluster where cluster 3 seems to have lowest COVID Fear, lowest perceived wealth, and lowest trust in government. In contrast, cluster 1 showed highest wealth, COVID Fear, and highest trust in government.

Figure 13

Demographic characteristics of each cluster



Privacy Paradox Analysis

In this analysis, a Chi-square test of independence was performed to explore the association and strength of effect between stereotypes of people and privacy paradox phenomenon. All expected cell frequencies were greater than five.

Table 20

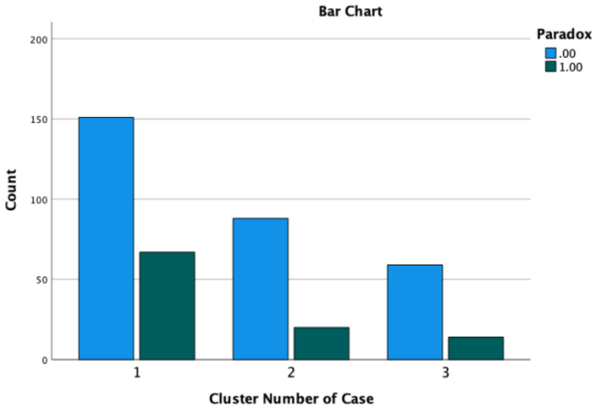
Frequency crosstabulation Results for Cluster group and Paradox behavior

	No Paradox			Paradox Appeared			Total	
	n	%	Adjusted Residual	n	%	Adjusted Residual	n	%
Cluster 1	151	50.7%	-2.7	67	66.3%	2.7	218	54.6%
Cluster 2	88	29.5%	1.9	20	19.8%	-1.9	108	27.1%
Cluster 3	59	19.8%	1.3	14	13.9%	-1.3	73	18.3%
Total	298	100%		101	100%		399	100%

There was a statistically significant association between stereotypes of people and privacy paradox behavior, χ2(2) = 7.479, p = .024. The association was moderately strong (Cohen, 1988), Cramer's V = .137. For the case of people in cluster 1, with the adjusted standardized residual of ± 2.7, there were more people have privacy paradox than expected, if the null hypothesis was true.

Figure 14

Frequency of paradox of each cluster



Thus, the magnitude of effect was highest with cluster 1 means people in cluster 1 tend to have higher probability of privacy paradox. In visual inspection, Figure 14 showed a difference between cluster 1 and other groups. As results of stronger association, among people (N = 27) who have a willingness rating below 4 in 1-7 points (not willing to support) and agree to try the FRT, there were 48% people in cluster 1 (N=13).

Discussion & implication

The primary purpose of this study is to understand how intrusiveness and distractions affect how people trade-off their privacy, how they conduct privacy calculus, and how those affect individuals' actual behavior toward FRT surveillance in public settings.

Citizens' perceived government intrusion concerns can be changed

Our study supported our first hypothesis (H1a) that the high intrusiveness of FRT is positively related to government intrusion concerns. An identifiable FRT raises more significant concerns, which leads to negative attitudes and lower privacy disclosure. In this study, the anonymized feature does not collect any information other than mask detection. Hence, the anonymity feature could be the common ground between the government's intention to maintain order while not harming citizens' privacy. This finding implies that citizens will accept FRT surveillance and have higher privacy disclosure if the government can assure them that their privacy will not be harmed.

Furthermore, the confirmation of H1b showed that distractions could affect the citizens' perceived government intrusion concerns in FRT implementation. The effect of distractions is one of the most notable findings of this study. We found that distractions do not always increase privacy disclosure. In most prior studies, especially in marketing literature, they used distractions to manipulate people to disclose personal information. However, we found that distraction has no significant correlation with willingness/privacy intention and acceptance/privacy disclosure in our context. Instead, we found that distraction is positively related to government intrusion concerns. Our finding aligns with Petty et al.'s (1976) study that distraction possibly activated central route processing and led to negative attitudes towards favorable persuasive messages. The results also confirmed a low direct impact of cognitive distraction/ environmental cues on behaviors, but mediately influence behavior through a cognitive thinking process as privacy calculus, aligned with recent findings in marketing literature. In these results, distraction or interruptions would cause a "psychological or cognitive distance" which then deviate people's behavior (Amaral, 2021; Berger & Fitzsimons, 2008). In our context, since FRT surveillance is considered controversial, collects sensitive information, and harms privacy rights, our distraction manipulation had a negative effect on citizens' attitudes. This finding implies that people do not want to be distracted and manipulated about sensitive and serious topics that involve their privacy and the government. Also, citizens prefer unbiased information towards the implementation of FRT. They want to know the benefits and risks. Thus, instead of distracting and persuading the citizens, being open about FRT applications, risks, and policies may lead to a positive attitude, government trust, and acceptance.

Our findings added a new confirmation regarding the impact of environmental cues, such as distraction, on people's attitudes in FRT technology for marketing and privacy literature. Moreover, distractions could interact with the intrusiveness level of technology to impact privacy behaviors.

Appropriate communication of technology usefulness can harmonize intrusion and privacy concerns to impact people' willingness positively

In the first part of our study, we applied the Elaboration Likelihood Model to explore how government intrusion concerns changes under manipulations of distraction and intrusiveness. In the second part, we adopted the privacy calculus model to analyze the role of government intrusion concerns and other constructs in people's willingness to support/privacy intention behavior. Our findings, the significant direct mediation effects within the privacy calculus model, in this study also confirmed Dinev et al. (2008) 's findings in Internet privacy concerns. Moreover, the significant manipulation effects also showed that privacy calculus would be deviated depending on the technology intrusiveness and whether people were distracted. Thus, the results provided empirical evidence of the privacy calculus model for the context of FRT in public settings. As a covariates variable, perceived usefulness showed its positive and significant relationship with willingness and other constructs. We confirmed that perceived usefulness is negatively related to privacy concerns. From these findings, we know that people's trade-offs calculation in the FRT context was sophisticated and involved a series of evaluations. Since the perceived usefulness has a significant effect, the public sectors should communicate FRT's usefulness to combat COVID-19. For example, FRT surveillance can be a useful and sustainable tool in helping cities exit lockdowns. Communicating the technology's usefulness will also increase the citizens' perceived need for government surveillance. Moreover, concerns regarding privacy and government intrusion would be lower if the FRT is privacy-friendly.

Our findings confirmed previous research on privacy in public settings. Moreover, we extended the boundary from general Internet privacy concerns to an extreme level of privacy disclosure with biometric information in FRT. Finally, we also extended the privacy calculus literature in public settings, with perceived usefulness's significant impact on other factors and willingness.

The role of moral equity

In line with previous findings, willingness played a vital role in people's privacy behavior in this study. However, moral equity could significantly affect disclosure behavior in FRT surveillance due to the COVID-19 pandemic. Specifically, when people perceived technology as necessary to society, it would positively correlate with people's actual behavior. With the approximately equal magnitude with willingness, moral equity should be a potential factor for further findings related to privacy disclosure behavior. The result suggested that government should emphasize the importance of FRT in society and its application, especially in a crisis, rather than seamless, controversial arguments about identifiable FRT technology only.

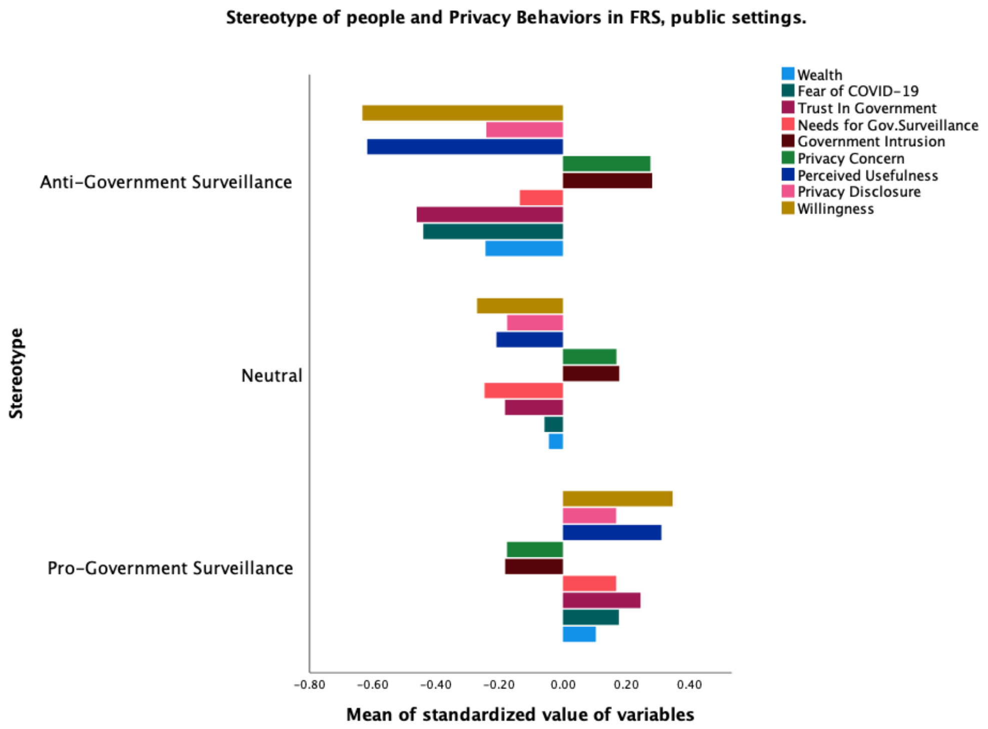
Privacy paradox between "anti" and "pro-government surveillance."

The further analysis related to the privacy paradox depicted different clusters of people with similar perceptions of what information they would allow the FRT and the government to collect. The results revealed that people who share more information with the government are wealthier, have the highest trust in government, and deepest concern about the COVID-19 disease. Unlike other clusters, this cluster has the highest perceived usefulness of FRT, lowest privacy concerns, and government intrusion concerns. In contrast, cluster 3 only wants to share minimal information with the government. This group includes unwealthy people, the lowest trust in government, lowest COVID fear as well. Thus, cluster 3 showed a low need for government surveillance, the deepest privacy concerns, and a negative attitude toward FRT.

Our study identified 3 clusters of people, which explains their disclosure behavior. Statistically, according to our results, people in cluster 1 tend to have the paradox as they appear to have low willingness but choose to disclose information later. Meanwhile, cluster 3 is not likely to have a privacy paradox due to negative prejudice about government surveillance. Thus, a group of pro-government surveillance (cluster 1) and neutral (cluster 2) advocate the FRT implementation in an appropriate setting. The other group is anti-government surveillance (cluster 3) and denies any means to monitor the people (Figure 15). Thus, we reject the hypothesis that there is no association between privacy paradox and type of people. Then, the government should have the appropriate segmentation strategy to communicate, increase awareness, and persuade each target of people.

Figure 15

Stereotypes of people and privacy perceptions



We believe that our study filled the identified gaps in the literature of FRT in public settings. Furthermore, our findings regarding the manipulations we used, and privacy calculus were supplemented with the privacy behavior analysis in both disclosure and privacy paradox. Moral equity and different groups of people in information sharing play important roles in the findings, explaining people's behaviors and decision-making processes. Moreover, the proofs of impact from manipulations and significant mediation process in privacy calculus provide a clearer understanding of people's journey from processing information to deciding privacy behavior.

Limitation & Future research

COVID-19's impacts on study design settings

As with any study, there are several limitations that we need to acknowledge. The major challenge was data collection. Due to the COVID-19 pandemic situation, we used an online survey instead of a physical experiment. In measuring the actual privacy disclosure of FRT, our initial plan was to provide a physical trial of the face mask detection system. If respondents agree to try the technology, they would have automatically disclosed their privacy without thinking so much about the potential risks, replicating our everyday privacy disclosure. However, since we collected our data from the platform Prolific, we had to follow their rules, such as no collection of personal data and no third parties (FRT developers) involvement. Therefore, our current approach might not have captured natural privacy behavior with an actual FRT.

Internal and external validity of experiment

Although we controlled the time of the manipulation tasks, there was a potential issue with internal validity in an online experiment. Also, extraneous variables could be varied, potentially impacting the respondent's perceptions toward FRT, such as recent news about Indian COVID-19 Crisis, or the protest against FRT, the "Tech battle" between citizens and government, .etc.

Moreover, we might not have captured the discrepancies between willingness to support/privacy intentions and acceptance/privacy disclosure. The respondents might not have left the intention behavior phase since we asked about their privacy disclosure right after answering the intention question. In most privacy paradox studies, scholar's methodology is usually separated into two studies with particular time intervals, usually two weeks, in between so that respondents have "forgotten" their stated privacy preferences (Norberg et al., 2007; Barth et al. 2019). Thus, the lack of time in between to "forget" in our methodology might not have captured the actual "privacy paradox." However, we can also argue that immediate measurement of privacy disclosure after privacy calculus could be more empirical and higher validity to avoid extraneous variables such as maturation and history.

Another limitation was that we asked the respondents the type of information they are willing to share without allowing them to choose nothing from the list or providing an "I choose nothing from the list" as an option to proceed. Then, later, when deciding to disagree with trying the app, we asked them to select the types of information they disagree to disclose, again, without allowing them to choose nothing from the list. This limitation might have forced some respondents to select a random type of information that they do not mean to proceed with the survey.

Another limitation is selection bias in our demographic sample while excluding one-third of the collected responses as a conservative approach. Although we used Prolific, a known crowdsourcing platform that is reliable and has nationally representative samples, the data were gathered primarily from the United Kingdom and Northern Ireland (96.7%) and the United States of America (3.3%). We know from prior surveillance literature studies that surveillance/privacy concerns and acceptability are location-dependent. There have been proven differences in perceptions across countries and cultures (Dinev, 2008). The perceptions of respondents from the UK might be more negative than other countries due to their controversial police use of FRT without consent (Croft & Venkataramakrishnan, 2020). Therefore, there is a potential for cultural bias in the results. Similarly, gender could play a potential role in the model, while most respondents (66.9%) were female. However, due to the randomization process of sampling, potential impact of gender would not be included in this study. Future research needs to address these limitations to provide a better understanding of cultural, account for gender balance, and institutional differences.

Statistical regression limitation

In the statistical analysis, despite carefully selecting appropriate methods, there were certain limitations related to the nature of the study. In our survey design, we collected most of the data using the Likert scale. We observed that data distribution depends on people's natural perceptions, such as privacy concerns (negative skewed - when most people perceive FRT intrusive) or needs for government surveillance (positive skewed - with low perceived need for government surveillance). Nevertheless, after data screening and filtering, there was an acceptable range to conduct analysis. However, there was potential bias, especially with ANOVA, since this analysis is extremely sensitive to normal distribution. Similarly, PCA has a decent method to explain latent variables, which should be replaced with confirmatory factor analysis (CFA) with a structural equation model (SEM). This approach was preferred by scholars in researching related to people's perceptions.

Overall, even with the limitation from COVID-19 with our study designs, internal and external well-aware invalidity, and regression bias, the study still provides significant, empirical results based on selective methods. However, future research can avoid these limitations without confounding conditions of the pandemic. They can inherit more flexible privacy policies in the private sector and utilize more sophisticated regression methods such as FCA to dig deeper with FRT in public and private settings.

Conclusion

The current study provided a structural approach to examine privacy trade-offs, starting with possible environment cues such as distraction and level of intrusiveness. Then, the ELM model elaborated how people negatively respond to distraction due to the central route processing activation, which led to greater concerns toward government intrusion. Next, the privacy calculus model explained how privacy-related constructs impact the willingness to support FRT of people. Finally, a proposed factor – moral equity was included in the model to predict the probability of privacy disclosure with FRT in public settings. Further analysis also suggested a potential factor as a stereotype of people (anti, neutral, pro-government surveillance), which is highly associated with the privacy paradox phenomenon.

On the one hand, these findings contributed practical approaches for practitioners, especially governments and authorities, in utilizing proper communication methods, privacy-friendly features in FRT implementation. On the other hand, the results supplemented empirical evidence for privacy literature regarding biometric data. The study demonstrated how environmental cues, such as distraction, impact behavior through a cognitive consideration process for marketing literature. These findings with FRT would be helpful in the coming era of AI when biometric data collection would play a vital role in marketing literature.

References

Acquisti A., & Grossklags, J. (2005) Privacy and rationality in individual decision making. *Security & Privacy, 3*(1), 26–33. doi: 10.1109/MSP.2005.22.

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science (American Association for the Advancement of Science)*, *347*(6221), 509–514. https://doi.org/10.1126/science.aaa1465

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*(2), 179–211. https://doi.org/10.1016/0749-5978(91)90020-T.

Altmann, E. M., Trafton, J. G., & Hambrick, D. Z. (2014). Momentary interruptions can derail the train of thought. *Journal of Experimental Psychology: General*, *143*(1), 215–226. https://doi.org/10.1037/a0030986

Amaral, N. B. (2021). How interruptions influence our thinking and the role of psychological distance. *Journal of Consumer Behaviour, 20*(1), 76—88. https://doi.org/10.1002/cb.1856

Anton, E., Kus, K., & Teuteberg, F. (2021). 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. *Digital Society*. DOI: 10.24251/HICSS.2021.261

Apte, D. S. (2020). Explicit Autonomy, Implicit Control: User Autonomy in the Dichotomous Choice Architecture of Facebook. *Journal of Creative Communications, 15*(2), 165—176. https://doi.org/10.1177/0973258619893787

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.T. (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. https://doi.org/10.1016/j.tele.2017.04.013

Barth, S., de Jong, M. D., Junger, M., Hartel, P. H., & Roppelt, J. C. (2019). Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources. *Telematics and informatics*, *41*, 55—69.

Bhalla, A. (2020). The latest evolution of biometrics. *Biometric Technology Today*, *2020*(8), 5–8. https://doi.org/10.1016/S0969-4765(20)30109-0

Berendt, B., Günther, O., & Spiekermann, S. (2005). Privacy in e-commerce. *Communications of the ACM*, *48*(4), 101–106. https://doi.org/10.1145/1053291.1053295

Berger, J., & Fitzsimons, G. (2008). Dogs on the street, pumas on your feet: How cues in the environment influence product evaluation and choice. *Journal of Marketing Research*, *45*(1), 1—14.

Bernal, P. (2016) Data gathering, surveillance and human rights: recasting the debate. *Journal of Cyber Policy*, *1*(2), 243—264. DOI: 10.1080/23738871.2016.1228990

Becker, M., Klausing, S. M., & Hess, T. (2019, June 8-14). "*UNCOVERING THE PRIVACY PARADOX: THE INFLUENCE OF DISTRACTION ON DATA DISCLOSURE DECISIONS*". In Proceedings of the 27th European Conference on Information Systems (ECIS), Stockholm & Uppsala, Sweden. https://aisel.aisnet.org/ecis2019_rip/69

Bidler, M., Zimmermann, J., Schumann, J. H., & Widjaja, T. (2020). Increasing Consumers’ Willingness to Engage in Data Disclosure Processes through Relevance-Illustrating Game Elements. *Journal of Retailing*, *96*(4), 507–523. https://doi.org/https://doi.org/10.1016/j.jretai.2020.10.001

Biometrics Institute. (2019). Biometrics Institute Industry Survey 2019 Report. https://www.biometricsinstitute.org/wp-content/uploads/Biometrics-Institute-Industry-Survey-Results-2019_Full-Report.pdf?fbclid=IwAR0hLT_3gqEUupk6LvLkluWL9MBHeRzzdscvV8s5G5nreqNBpUIuQF_W3DY

Box, G. E.P, & Tidwell, Paul W. (1962). Transformation of the Independent Variables. *Technometrics*, *4*(4), 531–550. https://doi.org/10.1080/00401706.1962.10490038

Brown, I. & Korff, D. (2009). Terrorism and the Proportionality of Internet Surveillance. *European Journal of Criminology*, *6*(2), 119–134. https://doi.org/10.1177/1477370808100541

Brown, S. (2011). *Measures of shape: Skewness and kurtosis*. Brownmath. https://brownmath.com/stat/shape.htm

Chen, Y., Yang, L., Zhang, M., & Yang, J. (2018). Central or peripheral? Cognition elaboration cues' effect on users' continuance intention of mobile health applications in the developing markets. *International Journal of Medical Informatics*, *116*, 33–45. https://doi.org/10.1016/j.ijmedinf.2018.04.008

Clarke, R. (1999). Internet privacy concerns confirm the case for intervention. *Communications of the ACM*, *42*(2), 60–67. https://doi.org/10.1145/293411.293475

Cohen, J. (1988). *Statistical power analysis for the behavioral sciences* (2nd ed.). Psychology Press.

Corlett, J. A. (2002). The nature and value of the moral right to privacy. *Public Affairs Quarterly*, *16*(4), 329–350.

Croft, J. & Venkataramkrishan, S. (2020, August 11). *Police use of facial recognition breaches human rights law, London court rules*. Financial Times. https://www.ft.com/content/b79e0bee-d32a-4d8e-b9b4-c8ffd3ac23f4

Culnan, M. J., & Bies, R. J. (2003). Consumer privacy: Balancing economic and justice considerations. *Journal of Social Issues, 59*(2), 323—342.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, *13*(3), 319–340. https://doi.org/10.2307/249008

Davis, P. (2020). Facial Detection and Smart Billboards: Analysing the 'Identified' Criterion of Personal Data in the GDPR. *University of Oslo Faculty of Law Research Paper No. 2020-01*. http://dx.doi.org/10.2139/ssrn.3523109

Dialani, P. (2021, January 6). COVID-19 PANDEMIC IS ENCOURAGING FACIAL RECOGNITION TECHNOLOGY. *Analytics Insights*. https://www.analyticsinsight.net/covid-19-pandemic-is-encouraging-facial-recognition-technology/

Dienlin, T., & Trepte, S. (2015). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology*, *45*(3), 285–297. https://doi.org/10.1002/ejsp.2049

Dinev, T., & Hart, P. (2004). Internet privacy concerns and their antecedents - measurement validity and a regression model. *Behaviour & Information Technology*, *23*(6), 413–422. https://doi.org/10.1080/01449290410001715723

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, *17*(1), 61–80. https://doi.org/10.1287/isre.1060.0080

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. https://doi.org/10.4018/jgim.2006100103

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. https://doi.org/10.1016/j.jsis.2007.09.002

Distler, V., Lallemand, C., & Koenig, V. (2020). How acceptable is this? How user experience factors can broaden our understanding of the acceptance of privacy trade-offs. *Computers in Human Behavior*, *106*, 106227. https://doi.org/10.1016/j.chb.2019.106227

Dunfee, T. W., Smith, N. C., & Ross Jr, W. T. (1999). Social contracts and marketing ethics. *Journal of Marketing, 63*(3), 14–32.

EDPB. (2020). *Guidelines 3/2019 on processing of personal data through video devices*. https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf

Etteldorf, C. (2020). EDPB Publishes Guidelines on Data Processing through Video Devices. *Eureopean. Data Protection Literature Review, 6*(102).

European Commission. (2020). *On a Common Union Toolbox for the Use of Technology and Data to Combat and Exit from the COVID-19 Crisis, In*

Particular Concerning Mobile Applications and the Use of Anonymised Mobility Data. European Commission.

Feldstein, S. (2019). *The global expansion of AI surveillance*. Carnegie Endowment for International Peace. https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847

Feng, Y., & Xie, Q. (2019). Privacy concerns, perceived intrusiveness, and privacy controls: An analysis of virtual try-on apps. *Journal of Interactive Advertising*, *19*(1), 43–57. https://doi.org/10.1080/15252019.2018.1521317

Fox, G., Clohessy, T., van der Werff, L., Rosati, P., & Lynn, T. (2021). Exploring the competing influences of privacy concerns and positive beliefs on citizen acceptance of contact tracing mobile applications. *Computers in Human Behavior*, *121*, 106806. https://doi.org/10.1016/j.chb.2021.106806

Gabisch, J. A. & Milne, G. R. (2014). The impact of compensation on information ownership and privacy control. *The Journal of Consumer Marketing*, *31*(1), 13–26. https://doi.org/10.1108/JCM-10-2013-0737

Gu, J., Xu, Y. J., Xu, H., Zhang, C., & Ling, H. (2017, Feb). Privacy concerns for mobile app download: An elaboration likelihood model perspective. *Decision Support Systems*, *94*, 19—28. https://doi.org/10.1016/j.dss.2016.10.002

Hayes, A. F. (2017). *Introduction to mediation, moderation, and conditional process analysis : a regression-based approach* (Second edition.). The Guilford Press.

Holmes, E. A., O'Connor, R. C., Perry, V. H., Tracey, I., Wessely, S., Arseneault, L., Ballard, C., Christensen, H., Silver, R. C., Everall, I., Ford, T., John, A., Kabir, T., King, K., Madan, I., Michie, S., Przybylski, A. K., Shafran, R., Sweeney, A., Worthman, C. M., Yardley, L., Cowan, K., Cope, C., Hotopf, M., & Bullmore, E. (2020). Mutltidisiciplinary research priorities for the COVID-19 pandemic: a call for action for mental health science. *The Lancet Psychiatry*, *7*(6), 547—560.

John, L. K., Acquisti, A., & Loewenstein, G. (2011). Strangers on a plane: context-dependent willingness to divulge sensitive information. *The*

Journal of Consumer Research, *37*(5), 858–873. https://doi.org/10.1086/656423

Kahneman, D. (2003). A Perspective on Judgment and Choice. *The American Psychologist*, *58*(9), 697–720. https://doi.org/10.1037/0003-066X.58.9.697

Kaiser, H. F. (1960). The application of electronic computers to factor analysis. *Educational and psychological measurement*, *20*(1), 141–151.

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. https://doi.org/10.1016/j.chb.2018.11.022

Kitkowska, A., Shulman, Y., Martucci, L. A., & Wastlund, E. (2020). Psychological Effects and Their Role in Online Privacy Interactions: A Review. *IEEE Access*, *8*, 21236–21260. https://doi.org/10.1109/ACCESS.2020.2969562

Klomp, S. R., van Rijn, M., Wijnhoven, R. G., Snoek, C. G., & de With, P. H. (2021). Safe Fakes: Evaluating Face Anonymizers for Face Detectors. *arXiv preprint arXiv:2104.11721*

Kloppenburg, Sanneke, & van der Ploeg, Irma. (2020). Securing Identities: Biometric Technologies and the Enactment of Human Bodily Differences. *Science as Culture*, *29*(1), 57–76. https://doi.org/10.1080/09505431.2018.1519534

Kobsa, A., Cho, H., & Knijnenburg, B. P. (2016). The effect of personalization provider characteristics on privacy attitudes and behaviors: An Elaboration Likelihood Model approach. *Journal of the Association for Information Science and Technology*, *67*(11), 2587–2606. https://doi.org/10.1002/asi.23629

Lerouge, D. (2009). Evaluating the Benefits of Distraction on Product Evaluations: The Mind-Set Effect. *Journal of consumer research, 36*(3), 367–379. https://doi.org/10.1086/599047

Li, Y. (2012). Theories in online information privacy research: A critical review and an integrated framework. *Decision Support Systems*, *54*(1), 471–481. https://doi.org/10.1016/j.dss.2012.06.010

Lunney, G. H. (1970). Using analysis of variance with a dichotomous dependent variable: An empirical study. *Journal of Educational Measurement*, *7*(4), 263–269. https://doi.org/10.1111/j.1745-3984.1970.tb00727.x

Lyon, D. (2001). *Surveillance society: Monitoring everyday life*. McGraw-Hill Education.

Maiorescu, I., Gabudeanu, L., Vîlcea, A. L., Sabou, G. C., & Dârdală, M. (2021). Intrusiveness and data protection in IoT solutions for smart homes. *Amfiteatru Economic, 23*(57), 429–447. doi:http://dx.doi.org.ezproxy.library.bi.no/10.24818/EA/2021/57/429

Martin, K. (2015). Privacy notices as tabula rasa: An empirical investigation into how complying with a privacy notice is related to meeting privacy expectations online. *Journal of Public Policy & Marketing*, *34*(2), 210–227.

Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data Privacy: Effects on Customer and Firm Performance. *Journal of Marketing, 81*(1), 36–58. https://doi.org/10.1509/jm.15.0497

Milne, G. R., Pettinico, G., Hajjat, F. M., & Markos, E. (2017). Information Sensitivity Typology: Mapping the Degree and Type of Risk Consumers Perceive in Personal Data Sharing. *Journal of Consumer Affairs, 51*(1), 133–161. https://doi.org/10.1111/joca.12111

Morosan, C., & DeFranco, A. (2015). Disclosing personal information via hotel apps: A privacy calculus perspective. *International Journal of Hospitality Management*, *47*, 120–130. https://doi.org/10.1016/j.ijhm.2015.03.008

Mourey, J., & Waldman, A. (2020). Past the privacy paradox: The importance of privacy changes as a function of control and complexity. *Journal of the Association for Consumer Research*, *5*, 162–180.

Nam, T. (2018). Untangling the relationship between surveillance concerns and acceptability. *International Journal of Information Management*, *38*(1), 262–269. https://doi.org/10.1016/j.ijinfomgt.2017.10.007

Nesterova, I. (2020). Mass data gathering and surveillance: the fight against facial recognition technology in the globalized world. *SHS Web of Conferences*.

Norberg, Patricia A, Horne, Daniel R, & Horne, David A. (2007). The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *The Journal of Consumer Affairs*, *41*(1), 100–126. https://doi.org/10.1111/j.1745-6606.2006.00070.x

North-Samardzic, A. (2019). Biometric Technology and Ethics: Beyond Security Applications. *Journal of Business Ethics*, *167*(3), 433. https://doi.org/10.1007/s10551-019-04143-6

Pagliari, C. (2020). The ethics and value of contact tracing apps: International insights and implications for Scotland's COVID-19 response. *Journal of Global Health*, *10*(2). https://doi.org/10.7189/jogh.10.020103

Pascu, L. (2019, September 19). Researchers introduce AI face anonymization model to secure privacy. Biometric Update.com. https://www.biometricupdate.com/201909/researchers-introduce-ai-face-anonymization-model-to-secure-privacy

Pavone, V., & Esposti, S. D. (2012). Public assessment of new surveillance-oriented security technologies: Beyond the trade-off between privacy and security. *Public Understanding of Science*, *21*(5), 556–572. https://doi.org/10.1177/0963662510376886

Petty, R. E., Wells, G. L., & Brock, T. C. (1976). Distraction can enhance or reduce yielding to propaganda: Thought disruption versus effort justification. *Journal of Personality and Social Psychology*, *34*(5), 874.

Petty, R. E., & Cacioppo, J. T. (1986). The Elaboration Likelihood Model of persuasion. *Advances in Experimental Social Psychology*, *19*, 123–205. https://doi.org/10.1016/S0065-2601(08)60214-2

Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy Concerns and Consumer Willingness to Provide Personal Information. *Journal of Public Policy & Marketing*, *19*(1), 27–41. https://doi.org/10.1509/jppm.19.1.27.16941

Pietrobelli, A., Pecoraro, L., Ferruzzi, A., Heo, M., Faith, M., Zoller, T., Antoniazzi, F., Piacentini, G., Fearnbach, S. N., & Heymsfield, S. B. (2020). Effects of COVID-19 Lockdown on lifestyle behaviors in children with obesity living in Verona, Italy: A longitudinal study. *Obesity, 28*(8), 1382–1385. https://doi.org/10.1002/oby.22861

Pizzi, G., & Scarpi, D. (2020). Privacy threats with retail technologies: A consumer perspective. *Journal of Retailing and Consumer Services, 56*(11). https://doi.org/10.1016/j.jretconser.2020.102160

Preacher, K. J., & Hayes, A. F. (2004). SPSS and SAS procedures for estimating I ndirect effects in simple mediation models. *Behavior Research Methods*, *36*(4), 717–731.

Princi, E., & Kramer, N. C. (2020). Out of control - Privacy calculus and the effect of perceived control and moral considerations on the usage of IoT healthcare devices. *Frontiers in Psychology, 11*, 582054–582054. https://doi.org/10.3389/fpsyg.2020.582054

Rasdale, M., Magee, J., Bicki, C., McDonald, E., Plas, M. W., Thuesen, E. A., & Bigg, C. (2020). *Facial recognition technology: Supporting a sustainable lockdown exit strategy?* DLA Piper. https://www.dlapiper.com/en/uk/insights/publications/2020/05/facial-recognition-technology/

Rawls, J. (1971). 1971: *A theory of justice*. Harvard University Press.

Rejer, I., & Jankowski, J. (2017). Brain activity patterns induced by interrupting the cognitive processes with online advertising. *Cognitive Processing, 18*(4), 419–430. https://doi.org/10.1007/s10339-017-0815-8

Roussi, A. (2020, November 18). Resisting the rise of facial recognition. *Nature*. https://www.nature.com/articles/d41586-020-03188-2

Ruggieri, S., Bonfanti, R. C., Passanisi, A., Pace, U., & Schimmenti, A. (2021). Electronic surveillance in the couple: The role of self-efficacy and commitment. *Computers in Human Behavior*, *114*. https://doi.org/10.1016/j.chb.2020.106577

Ryu, S., & Park, Y. N. (2020). How consumers cope with location-based advertising (LBA) and personal information disclosure: The mediating role of persuasion knowledge, perceived benefits and harms, and attitudes toward LBA. *Computers in Human Behavior*, *112*(9). https://doi.org/10.1016/j.chb.2020.106450

Sagarin, B. J., Britt, M. A., Heider, J. D., Wood, S. E., & Lynch, J. E. (2003). Bartering Our Attention: The Distraction and Persuasion Effects of On-Line Advertisements. *Cognitive Technology, 8*(2), 4–17.

Schmitt, B. (2019). From Atoms to Bits and Back: A Research Curation on Digital Technology and Agenda for Future Research. *Journal of Consumer Research*, 46(4), 825–832.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *IS Quarterly*, *35*(4), 989–1015. https://doi.org/10.2307/41409970

Sobel, Michael E. (1982). Asymptotic Confidence Intervals for Indirect Effects in Structural Equation Models. *Sociological Methodology*, *13*, 290–312. https://doi.org/10.2307/270723

Tabachnick, B. G., & Fidell, L. S. (2013). *Using multivariate statistics: International edition*. Pearson.

Taddicken, M. (2014). The 'Privacy Paradox' in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure. *Journal of Computer-Mediated Communication*, *19*(2), 248–273. https://doi.org/10.1111/jcc4.12052

Thompson, N., McGill, T., Bunn, A., & Alexander, R. (2020). Cultural factorsand the role of privacy concerns in acceptance of government surveillance. *Journal of the Association for Information Science and Technology*, *71*(9), 1129–1142. https://doi.org/10.1002/asi.24372

Thurstone, L. L. (1931). Multiple factor analysis. *Psychological Review*, *38*(5), 406–427. https://doi.org/10.1037/h0069792

Trüdinger, Eva-Maria, & Steckermeier, Leonie C. (2017). Trusting and controlling? Political trust, information and acceptance of surveillance policies: The case of Germany. *Government Information Quarterly*, *34*(3), 421–433. https://doi.org/10.1016/j.giq.2017.07.003

Tsai, J. Y., Egelman, S., Cranor, L., & Acquisti, A. (2011). The effect of online privacy information on purchasing behavior: An experimental study. *Information Systems Research, 22*(2), 254–268.

Van Kleek, M., Liccardi, I., Binns, R., Zhao, J., Weitzner, D., Shadbolt, N. (2018). Better the devil you know: Exposing the data sharing practives of smartphone apps. *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. http://doi.acm.org/10.1145/3025453.3025556

Véliz, C. (2021). Privacy and digital ethics after the pandemic. Nat Electron 4, 10–11. https://doi.org/10.1038/s41928-020-00536-y

Vincent, J. (2020, May 7). France is using AI to check whether people are wearing masks on public transport. *The Verge*. https://www.theverge.com/2020/5/7/21250357/france-masks-public-transport-mandatory-ai-surveillance-camera-software

Wheeler, D. J. & Chambers, D. S. (1992). *Understanding Statistical Process Control*, 2nd edition. SPC Press.

Wirth, J. (2018). Dependent variables in the privacy-related field: A descriptive literature review. In *Proceedings of the 51st Hawaii International Conference on system sciences.*

Wottrich, V. M., van Reijmersdal, E. A., & Smit, E. G. (2018). The privacy trade-off for mobile app downloads: The roles of app value, intrusiveness, and privacy concerns. *Decision Support Systems*, *106*, 44–52. https://doi.org/10.1016/j.dss.2017.12.003

Wu, P. F., Vitak, J., & Zimmer, M. T. (2019). A contextual approach to information privacy research. *Journal of the Association for Information Privacy Research*, *71*(1). https://doi.org/10.1002/asi.24232

Xu, H., Dinev, T., Smith, J., & Hart, P. (2011). Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems*, *12*(12), 798–824. https://doi.org/10.17705/1jais.00281

Yao, M. Z., Rice, R. E., & Wallis, K. (2007). Predicting user concerns about online privacy. *Journal of the American Society for Information Science and Technology*, *58*(5), 710–722.

Yeung, D., Balebako, R., Gaviria, C. I. G., & Chaykowsky, M. (2020). Face Recognition Technologies: Designing Systems that Protect Privacy and Prevent Bias. Homeland Security Operational Analysis Center operated by the RAND Corporation. https://www.rand.org/pubs/research_reports/RR4226.html

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. https://doi.org/10.1016/j.im.2018.10.001

Zane, D. M., Smith, R. W., & Reczek, R. W. (2020). The Meaning of Distraction: How Metacognitive Inferences from Distraction during Multitasking Affect Brand Evaluations. *Journal of consumer research*, *46*(5), 974–994. https://doi.org/10.1093/jcr/ucz035

Zhang, W. K., & Kang, M. J. (2019). Factors Affecting the Use of Facial-Recognition Payment: An Example of Chinese Consumers. *IEEE*

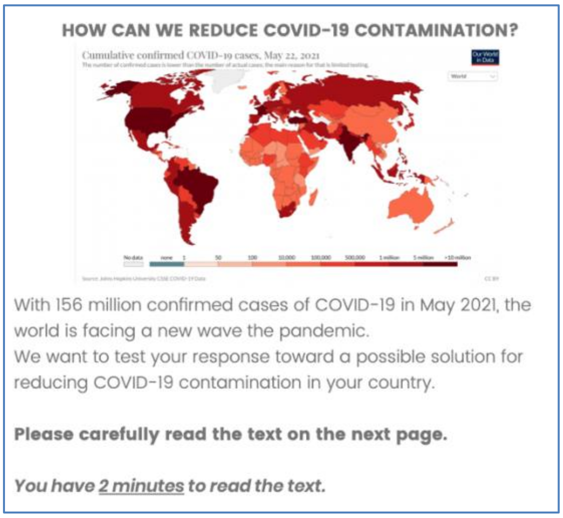
Access, *7*, 154360–154374. https://doi.org/10.1109/ACCESS.2019.2927705

APPENDICES

APPENDIX 1. Four conditions

1.1.Low intrusive/anonymized and no distraction condition

- Explicit mention of the terms “anonymized” and “unidentifiable” in the text, and
- No counting tasks

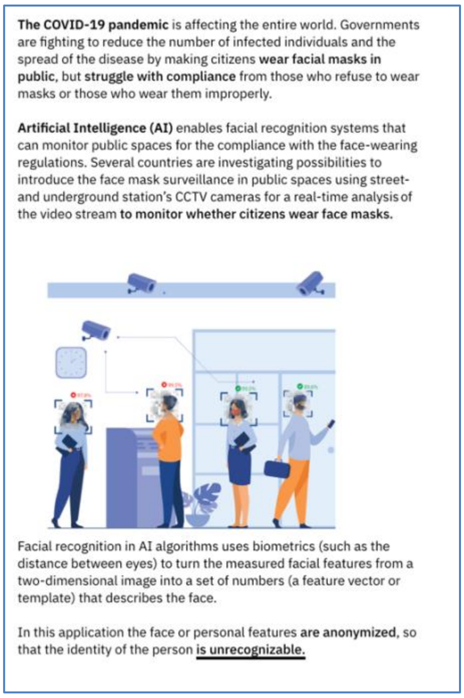

HOW CAN WE REDUCE COVID-19 CONTAMINATION?

Cumulative confirmed COVID-19 cases, May 22, 2021
The number of confirmed cases is lower than the number of actual cases; the main reason for that is limited testing.
Our World in Data
World
No data
none
1
50
100
10,000
100,000
500,000
1 million
5 million
>10 million
Source: Johns Hopkins University CSSE COVID-19 Data
CC BY

With 156 million confirmed cases of COVID-19 in May 2021, the world is facing a new wave the pandemic.
We want to test your response toward a possible solution for reducing COVID-19 contamination in your country.

Please carefully read the text on the next page.

You have 2 minutes to read the text.


The COVID-19 pandemic is affecting the entire world. Governments are fighting to reduce the number of infected individuals and the spread of the disease by making citizens **wear facial masks in public**, but **struggle with compliance** from those who refuse to wear masks or those who wear them improperly.

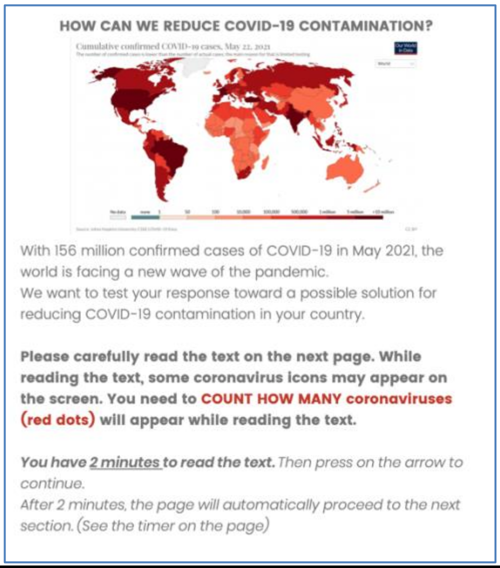
Artificial Intelligence (AI) enables facial recognition systems that can monitor public spaces for the compliance with the face-wearing regulations. Several countries are investigating possibilities to introduce the face mask surveillance in public spaces using street- and underground station's CCTV cameras for a real-time analysis of the video stream **to monitor whether citizens wear face masks.**

Facial recognition in AI algorithms uses biometrics (such as the distance between eyes) to turn the measured facial features from a two-dimensional image into a set of numbers (a feature vector or template) that describes the face.

In this application the face or personal features **are anonymized**, so that the identity of the person **is unrecognizable.**

Low intrusive/anonymized and distraction condition

- Explicit mention of the terms “anonymized” and “unidentifiable” in the text, and
- with red dots counting task

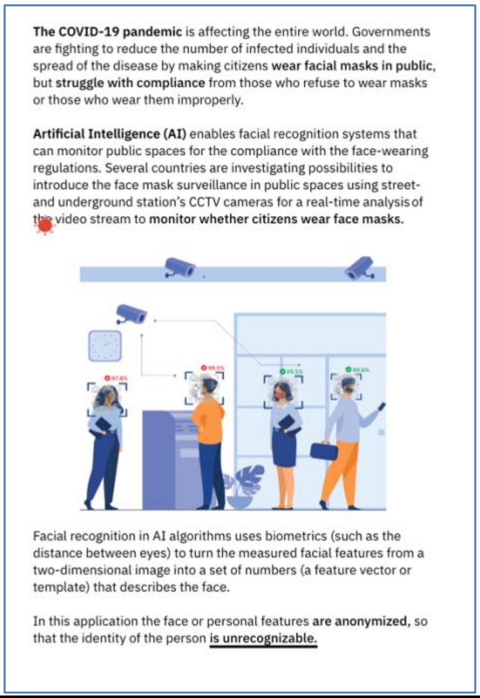

HOW CAN WE REDUCE COVID-19 CONTAMINATION?

Cumulative confirmed COVID-19 cases, May 22, 2021
The number of confirmed cases is lower than the number of actual cases; the main reason for that is limited testing.
Our World in Data
World
No data
none
1
50
100
10,000
100,000
500,000
1 million
5 million
>10 million
Source: Johns Hopkins University CSSE COVID-19 Data
CC BY

With 156 million confirmed cases of COVID-19 in May 2021, the world is facing a new wave of the pandemic.
We want to test your response toward a possible solution for reducing COVID-19 contamination in your country.

Please carefully read the text on the next page. While reading the text, some coronavirus icons may appear on the screen. You need to COUNT HOW MANY coronaviruses (red dots) will appear while reading the text.

You have 2 minutes to read the text. *Then press on the arrow to continue.*
After 2 minutes, the page will automatically proceed to the next section. (See the timer on the page)


The COVID-19 pandemic is affecting the entire world. Governments are fighting to reduce the number of infected individuals and the spread of the disease by making citizens **wear facial masks in public,** but **struggle with compliance** from those who refuse to wear masks or those who wear them improperly.

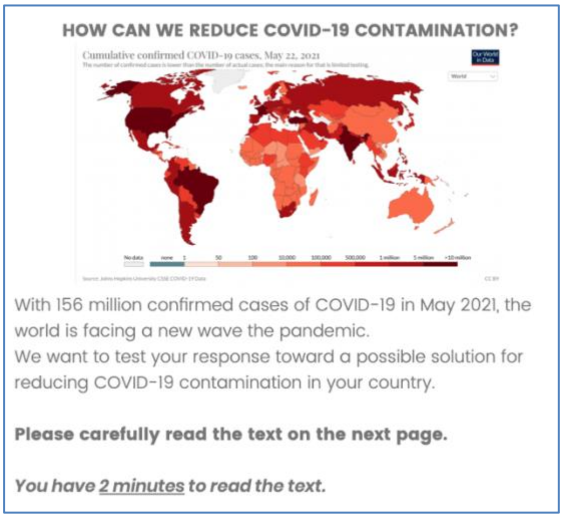
Artificial Intelligence (AI) enables facial recognition systems that can monitor public spaces for the compliance with the face-wearing regulations. Several countries are investigating possibilities to introduce the face mask surveillance in public spaces using street- and underground station's CCTV cameras for a real-time analysis of the video stream to **monitor whether citizens wear face masks.**

Facial recognition in AI algorithms uses biometrics (such as the distance between eyes) to turn the measured facial features from a two-dimensional image into a set of numbers (a feature vector or template) that describes the face.

In this application the face or personal features **are anonymized,** so that the identity of the person **is unrecognizable.**

High intrusive/non-anonymized and no distraction condition

- Explicit mention of terms “identified” and “recognizable” in the text, and
- No counting tasks



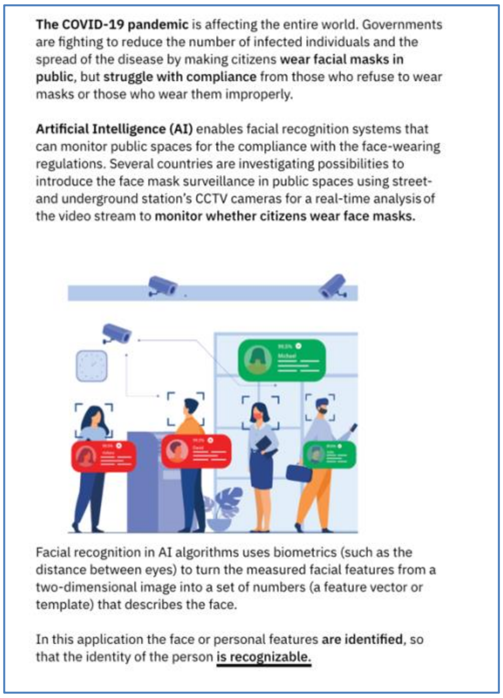
HOW CAN WE REDUCE COVID-19 CONTAMINATION?

Cumulative confirmed COVID-19 cases, May 22, 2021
The number of confirmed cases is lower than the number of actual cases; the main reason for that is limited testing.
Our World in Data
World
No data
none
1
50
100
10,000
100,000
500,000
1 million
5 million
>10 million
Source: Johns Hopkins University CSSE COVID-19 Data
CC BY

With 156 million confirmed cases of COVID-19 in May 2021, the world is facing a new wave the pandemic.
We want to test your response toward a possible solution for reducing COVID-19 contamination in your country.

Please carefully read the text on the next page.

You have <u>2 minutes</u> to read the text.



The COVID-19 pandemic is affecting the entire world. Governments are fighting to reduce the number of infected individuals and the spread of the disease by making citizens **wear facial masks in public**, but **struggle with compliance** from those who refuse to wear masks or those who wear them improperly.

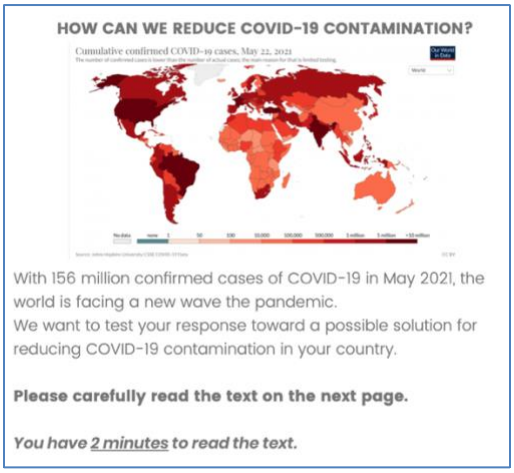
Artificial Intelligence (AI) enables facial recognition systems that can monitor public spaces for the compliance with the face-wearing regulations. Several countries are investigating possibilities to introduce the face mask surveillance in public spaces using street- and underground station’s CCTV cameras for a real-time analysis of the video stream to **monitor whether citizens wear face masks.**

Facial recognition in AI algorithms uses biometrics (such as the distance between eyes) to turn the measured facial features from a two-dimensional image into a set of numbers (a feature vector or template) that describes the face.

In this application the face or personal features **are identified**, so that the identity of the person **<u>is recognizable.</u>**

High intrusive/non-anonymized and distraction condition

- Explicit mention of terms “identified” and “recognizable” in the text, and
- With red dots counting tasks



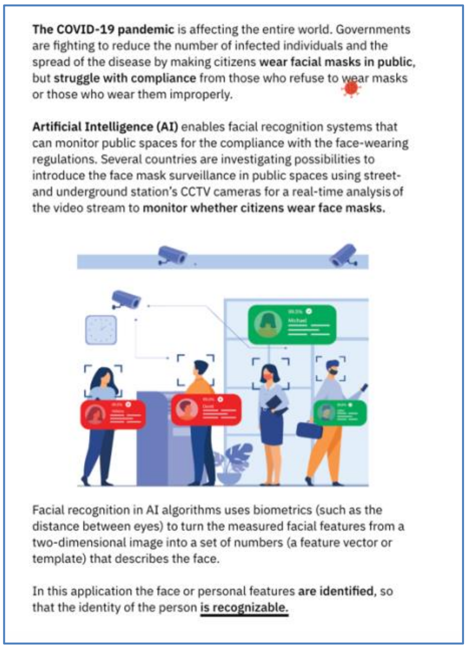
HOW CAN WE REDUCE COVID-19 CONTAMINATION?

Cumulative confirmed COVID-19 cases, May 22, 2021
The number of confirmed cases is lower than the number of actual cases; the main reason for that is limited testing.
Our World in Data
World
No data
none
1
50
100
10,000
100,000
500,000
1 million
5 million
>10 million
Source: Johns Hopkins University CSSE COVID-19 Data
CC BY

With 156 million confirmed cases of COVID-19 in May 2021, the world is facing a new wave the pandemic.
We want to test your response toward a possible solution for reducing COVID-19 contamination in your country.

Please carefully read the text on the next page.

You have <u>2 minutes</u> to read the text.



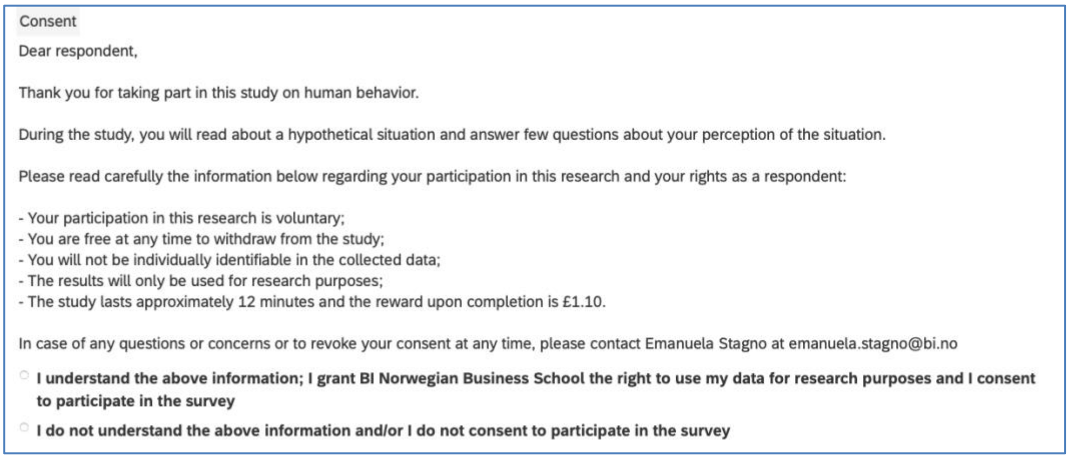
The COVID-19 pandemic is affecting the entire world. Governments are fighting to reduce the number of infected individuals and the spread of the disease by making citizens **wear facial masks in public**, but **struggle with compliance** from those who refuse to wear masks or those who wear them improperly.

Artificial Intelligence (AI) enables facial recognition systems that can monitor public spaces for the compliance with the face-wearing regulations. Several countries are investigating possibilities to introduce the face mask surveillance in public spaces using street- and underground station’s CCTV cameras for a real-time analysis of the video stream to **monitor whether citizens wear face masks.**

Facial recognition in AI algorithms uses biometrics (such as the distance between eyes) to turn the measured facial features from a two-dimensional image into a set of numbers (a feature vector or template) that describes the face.

In this application the face or personal features **are identified**, so that the identity of the person **<u>is recognizable.</u>**

APPENDIX: Survey flow with low intrusive/anonymized and distraction condition



Consent

Dear respondent,

Thank you for taking part in this study on human behavior.

During the study, you will read about a hypothetical situation and answer few questions about your perception of the situation.

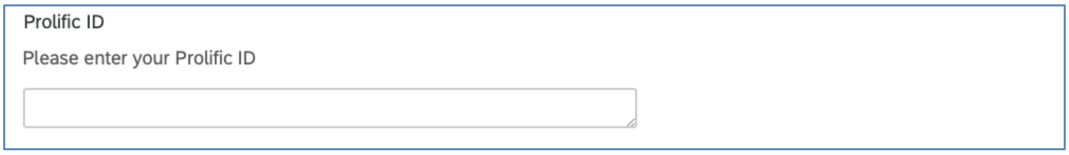
Please read carefully the information below regarding your participation in this research and your rights as a respondent:

- Your participation in this research is voluntary;
- You are free at any time to withdraw from the study;
- You will not be individually identifiable in the collected data;
- The results will only be used for research purposes;
- The study lasts approximately 12 minutes and the reward upon completion is £1.10.

In case of any questions or concerns or to revoke your consent at any time, please contact Emanuela Stagno at emanuela.stagno@bi.no

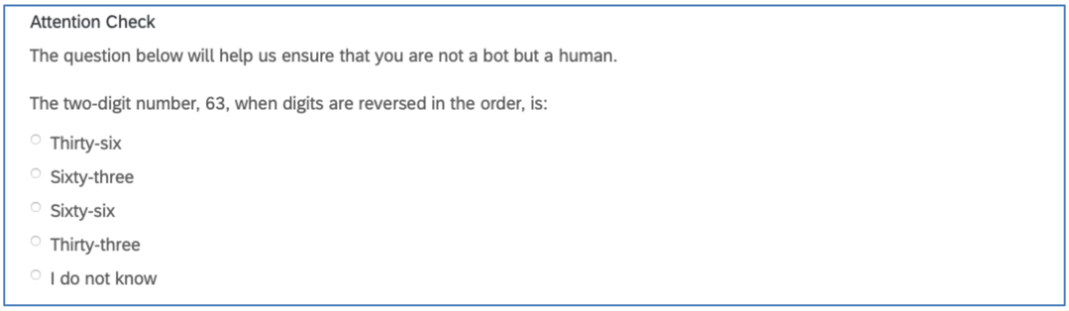
○ **I understand the above information; I grant BI Norwegian Business School the right to use my data for research purposes and I consent to participate in the survey**

○ **I do not understand the above information and/or I do not consent to participate in the survey**



Prolific ID

Please enter your Prolific ID



Attention Check

The question below will help us ensure that you are not a bot but a human.

The two-digit number, 63, when digits are reversed in the order, is:

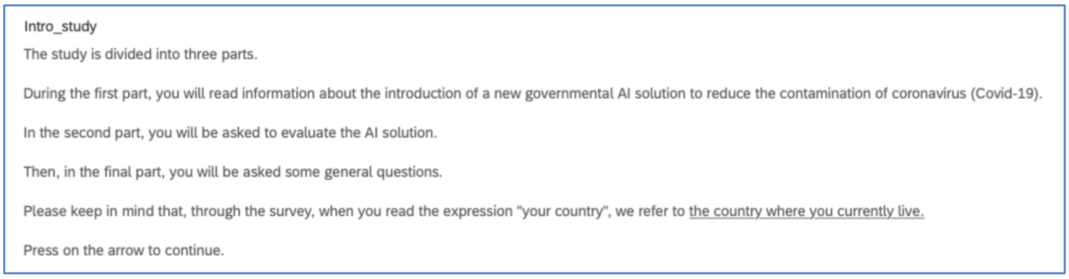
○ Thirty-six

○ Sixty-three

○ Sixty-six

○ Thirty-three

○ I do not know



Intro_study

The study is divided into three parts.

During the first part, you will read information about the introduction of a new governmental AI solution to reduce the contamination of coronavirus (Covid-19).

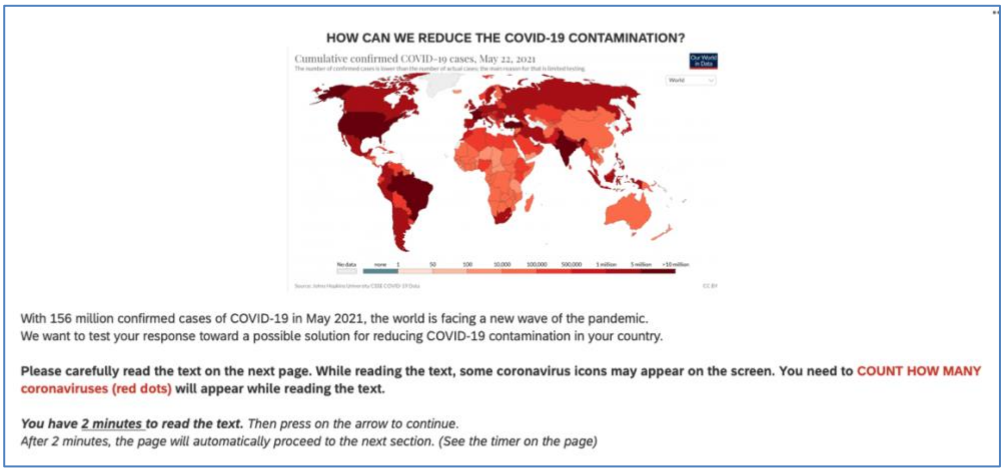
In the second part, you will be asked to evaluate the AI solution.

Then, in the final part, you will be asked some general questions.

Please keep in mind that, through the survey, when you read the expression "your country", we refer to the country where you currently live.

Press on the arrow to continue.

Distraction condition



HOW CAN WE REDUCE THE COVID-19 CONTAMINATION?

Cumulative confirmed COVID-19 cases, May 22, 2021

The number of confirmed cases is lower than the number of actual cases; the main reason for that is limited testing.

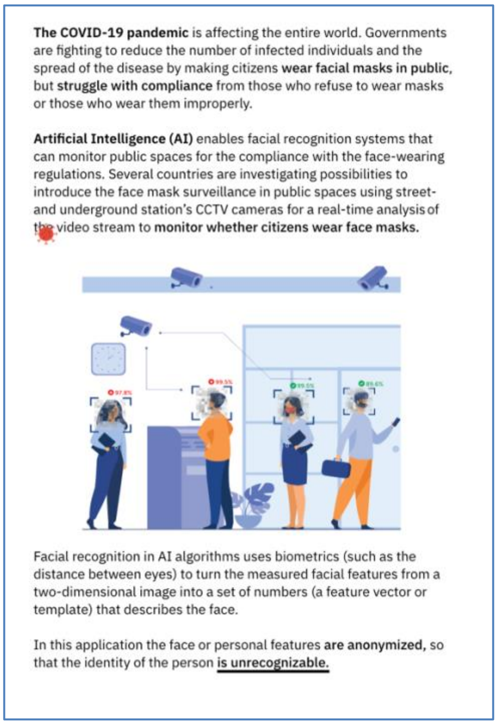
Source: Johns Hopkins University CSSE COVID-19 Data

With 156 million confirmed cases of COVID-19 in May 2021, the world is facing a new wave of the pandemic.
We want to test your response toward a possible solution for reducing COVID-19 contamination in your country.

Please carefully read the text on the next page. While reading the text, some coronavirus icons may appear on the screen. You need to COUNT HOW MANY coronaviruses (red dots) will appear while reading the text.

You have 2 minutes to read the text. *Then press on the arrow to continue.*
After 2 minutes, the page will automatically proceed to the next section. (See the timer on the page)

Non-intrusive/anonymized condition + distraction condition

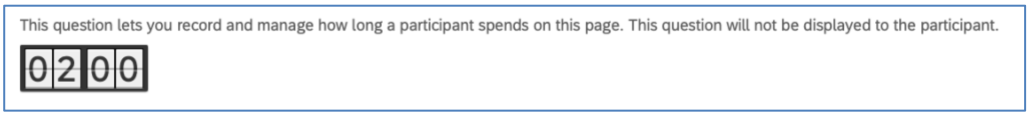


The COVID-19 pandemic is affecting the entire world. Governments are fighting to reduce the number of infected individuals and the spread of the disease by making citizens **wear facial masks in public**, but **struggle with compliance** from those who refuse to wear masks or those who wear them improperly.

Artificial Intelligence (AI) enables facial recognition systems that can monitor public spaces for the compliance with the face-wearing regulations. Several countries are investigating possibilities to introduce the face mask surveillance in public spaces using street- and underground station's CCTV cameras for a real-time analysis of the video stream to **monitor whether citizens wear face masks.**

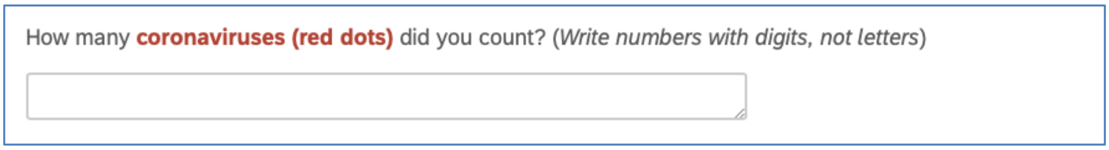
Facial recognition in AI algorithms uses biometrics (such as the distance between eyes) to turn the measured facial features from a two-dimensional image into a set of numbers (a feature vector or template) that describes the face.

In this application the face or personal features **are anonymized**, so that the identity of the person **is unrecognizable.**

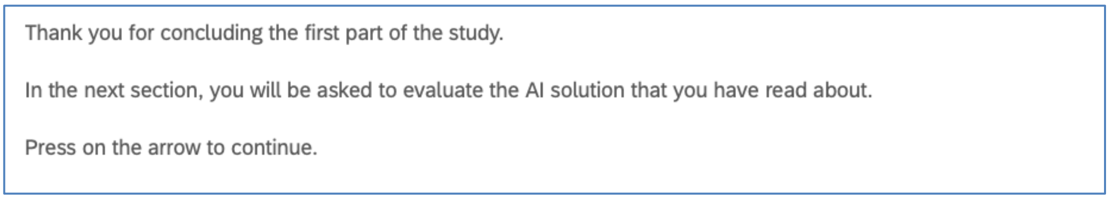


This question lets you record and manage how long a participant spends on this page. This question will not be displayed to the participant.

02 00



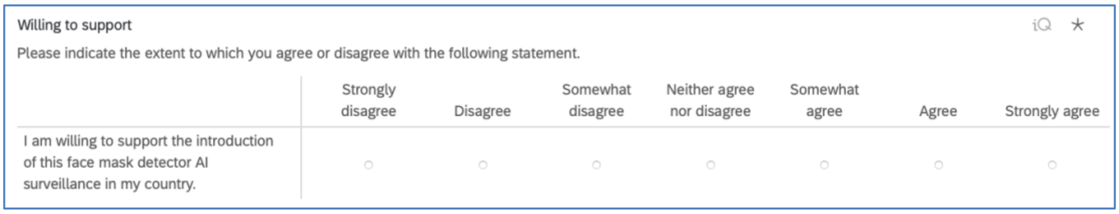
How many **coronaviruses (red dots)** did you count? (*Write numbers with digits, not letters*)



Thank you for concluding the first part of the study.

In the next section, you will be asked to evaluate the AI solution that you have read about.

Press on the arrow to continue.

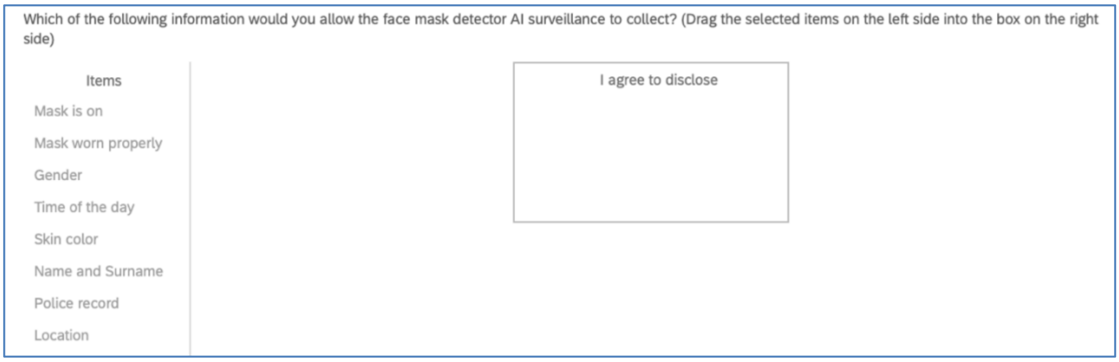


Willing to support

Please indicate the extent to which you agree or disagree with the following statement.

	Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
I am willing to support the introduction of this face mask detector AI surveillance in my country.	○	○	○	○	○	○	○

Type of information to disclose

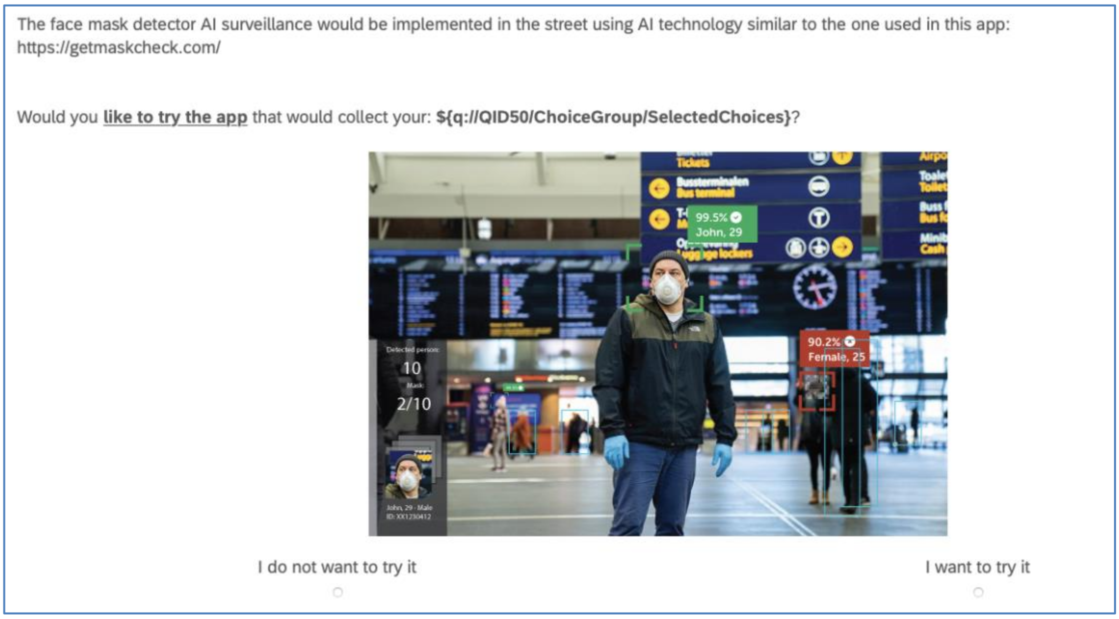


Which of the following information would you allow the face mask detector AI surveillance to collect? (Drag the selected items on the left side into the box on the right side)

Items

- Mask is on
- Mask worn properly
- Gender
- Time of the day
- Skin color
- Name and Surname
- Police record
- Location

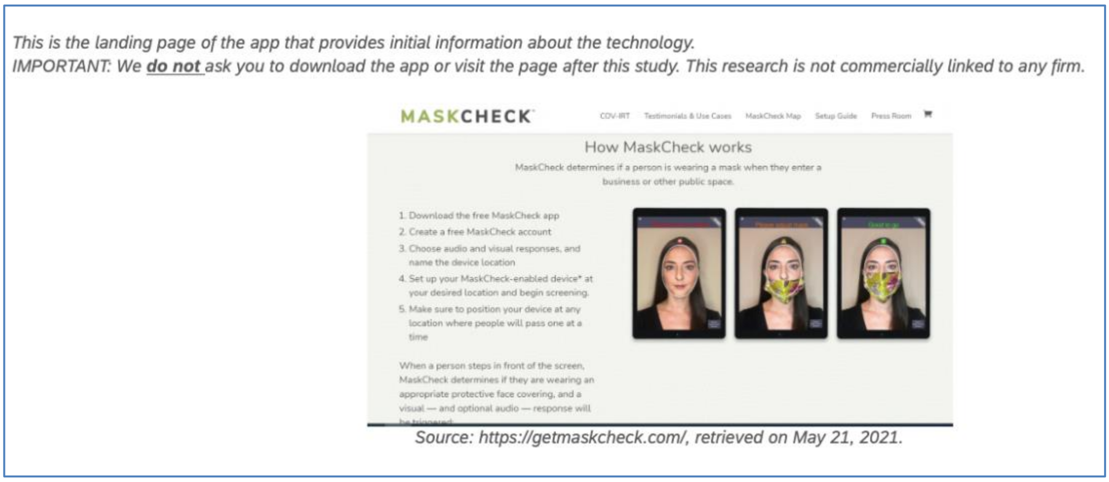
I agree to disclose



The face mask detector AI surveillance would be implemented in the street using AI technology similar to the one used in this app: https://getmaskcheck.com/

Would you **like to try the app** that would collect your: **${q://QID50/ChoiceGroup/SelectedChoices}**?

I do not want to try it ○ I want to try it ○



This is the landing page of the app that provides initial information about the technology.
*IMPORTANT: We **do not** ask you to download the app or visit the page after this study. This research is not commercially linked to any firm.*

How MaskCheck works

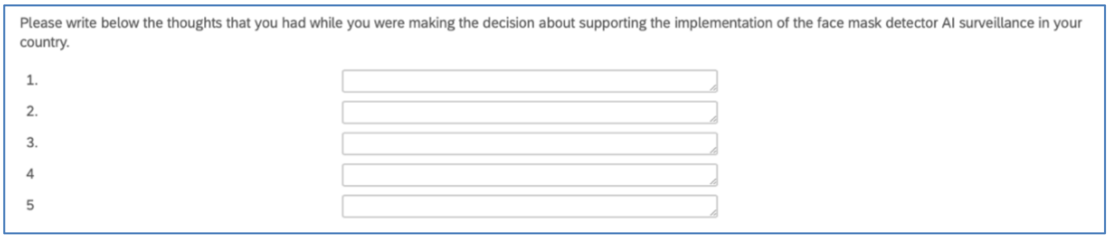
MaskCheck determines if a person is wearing a mask when they enter a business or other public space.

1. Download the free MaskCheck app
2. Create a free MaskCheck account
3. Choose audio and visual responses, and name the device location
4. Set up your MaskCheck-enabled device* at your desired location and begin screening.
5. Make sure to position your device at any location where people will pass one at a time

When a person steps in front of the screen, MaskCheck determines if they are wearing an appropriate protective face covering, and a visual — and optional audio — response will be triggered.

Source: https://getmaskcheck.com/, retrieved on May 21, 2021.

Thought listing



Please write below the thoughts that you had while you were making the decision about supporting the implementation of the face mask detector AI surveillance in your country.

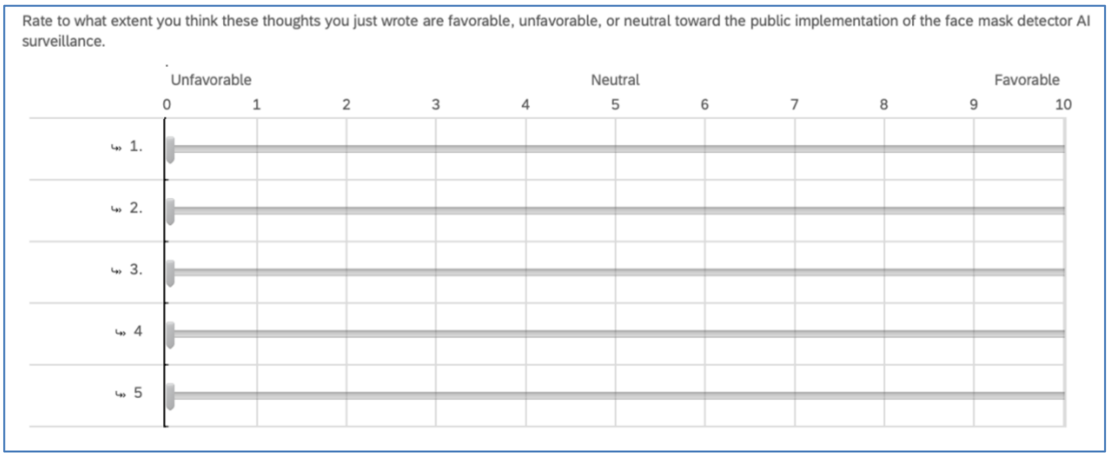
1.

2.

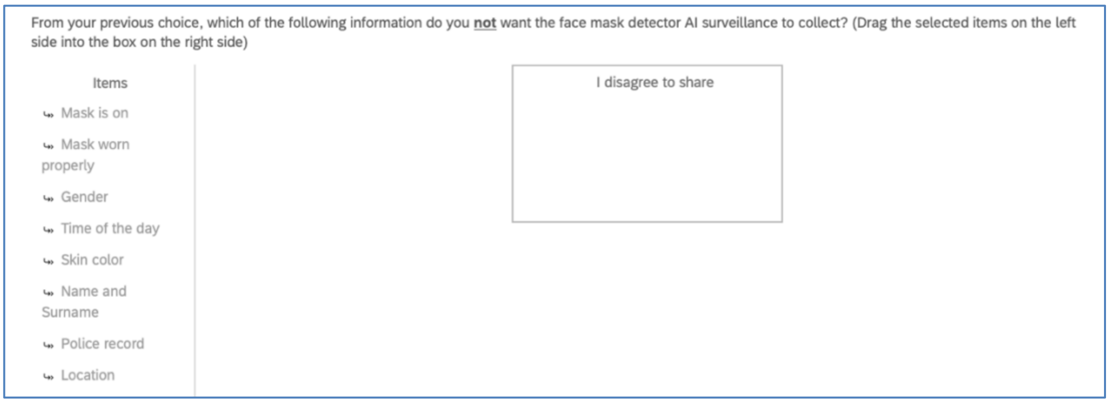
3.

4

5



Rate to what extent you think these thoughts you just wrote are favorable, unfavorable, or neutral toward the public implementation of the face mask detector AI surveillance.

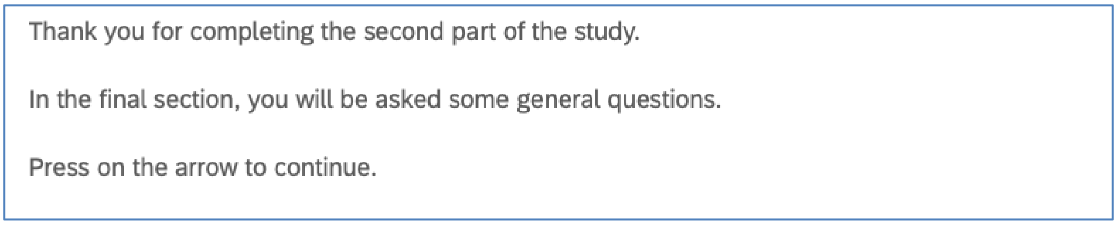


From your previous choice, which of the following information do you **not** want the face mask detector AI surveillance to collect? (Drag the selected items on the left side into the box on the right side)

Items

- ↪ Mask is on
- ↪ Mask worn properly
- ↪ Gender
- ↪ Time of the day
- ↪ Skin color
- ↪ Name and Surname
- ↪ Police record
- ↪ Location

I disagree to share

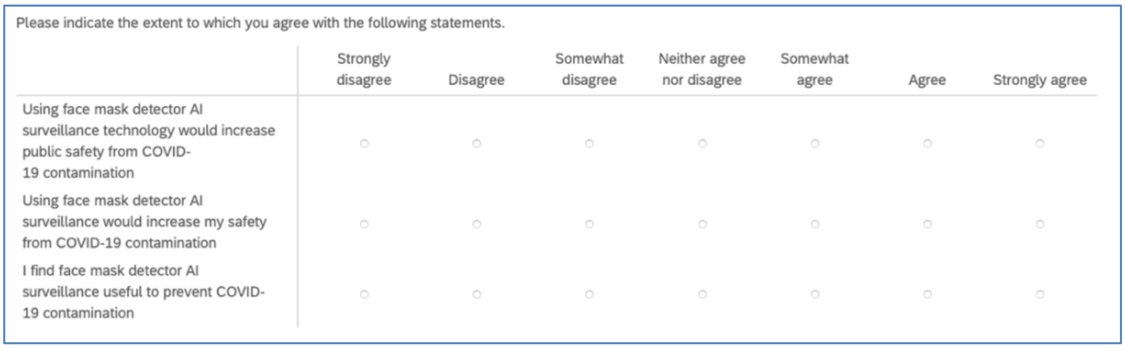


Thank you for completing the second part of the study.

In the final section, you will be asked some general questions.

Press on the arrow to continue.

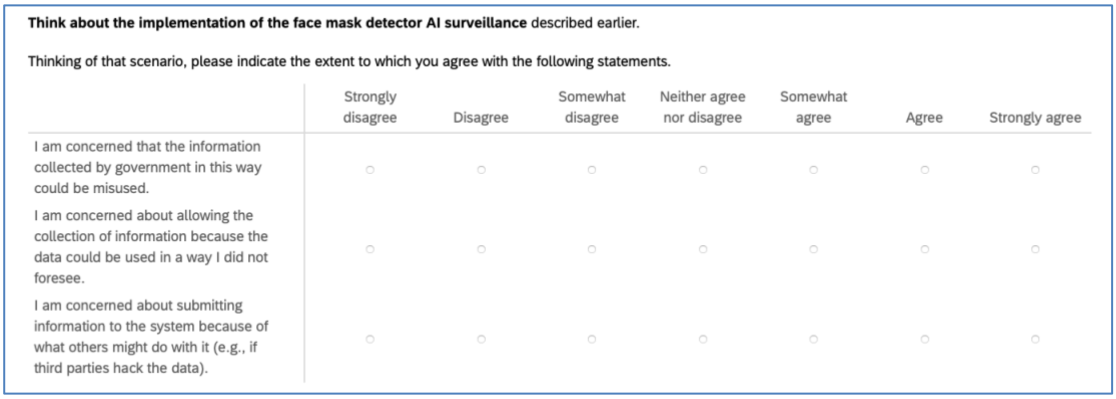
Perceived usefulness



Please indicate the extent to which you agree with the following statements.

	Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
Using face mask detector AI surveillance technology would increase public safety from COVID-19 contamination	○	○	○	○	○	○	○
Using face mask detector AI surveillance would increase my safety from COVID-19 contamination	○	○	○	○	○	○	○
I find face mask detector AI surveillance useful to prevent COVID-19 contamination	○	○	○	○	○	○	○

Privacy concerns

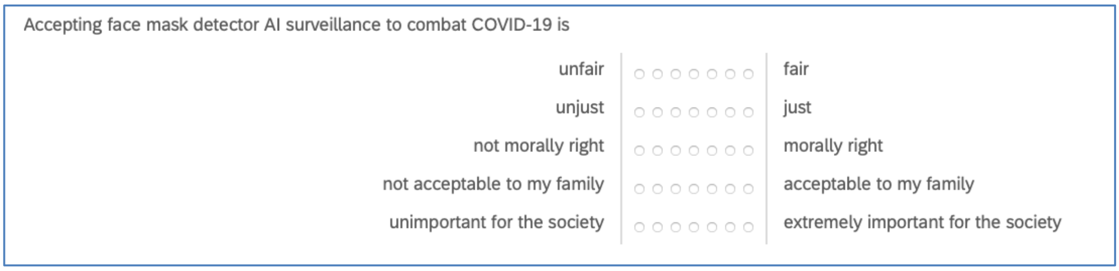


Think about the implementation of the face mask detector AI surveillance described earlier.

Thinking of that scenario, please indicate the extent to which you agree with the following statements.

	Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
I am concerned that the information collected by government in this way could be misused.	○	○	○	○	○	○	○
I am concerned about allowing the collection of information because the data could be used in a way I did not foresee.	○	○	○	○	○	○	○
I am concerned about submitting information to the system because of what others might do with it (e.g., if third parties hack the data).	○	○	○	○	○	○	○

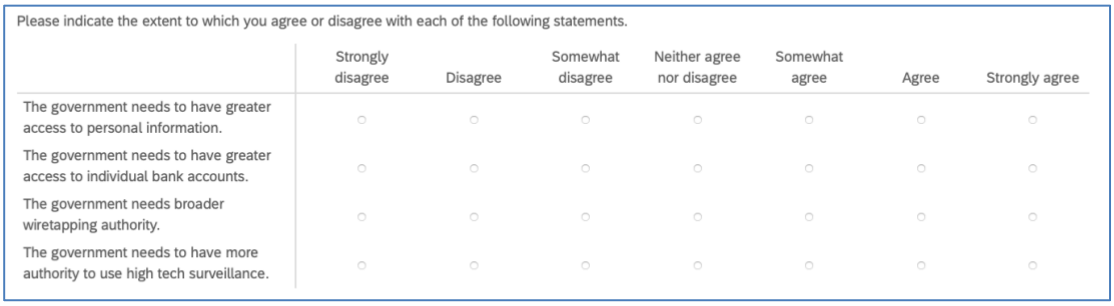
Moral equity



Accepting face mask detector AI surveillance to combat COVID-19 is

unfair	○	○	○	○	○	○	○	fair
unjust	○	○	○	○	○	○	○	just
not morally right	○	○	○	○	○	○	○	morally right
not acceptable to my family	○	○	○	○	○	○	○	acceptable to my family
unimportant for the society	○	○	○	○	○	○	○	extremely important for the society

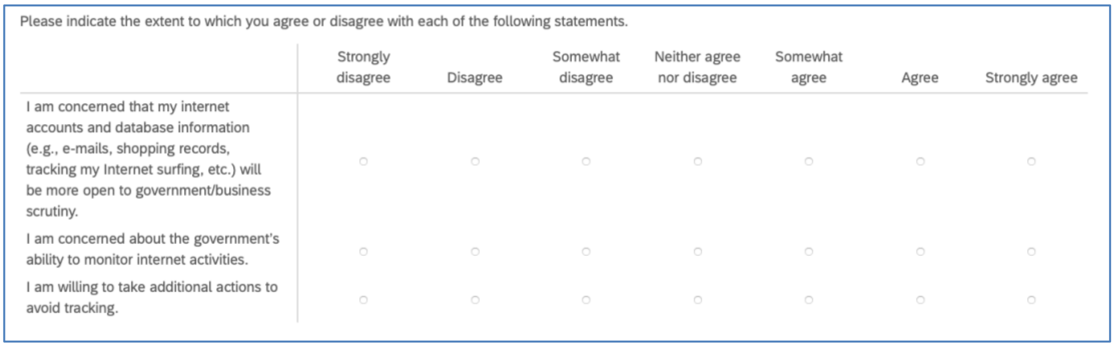
Perceived need of government surveillance



Please indicate the extent to which you agree or disagree with each of the following statements.

	Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
The government needs to have greater access to personal information.	○	○	○	○	○	○	○
The government needs to have greater access to individual bank accounts.	○	○	○	○	○	○	○
The government needs broader wiretapping authority.	○	○	○	○	○	○	○
The government needs to have more authority to use high tech surveillance.	○	○	○	○	○	○	○

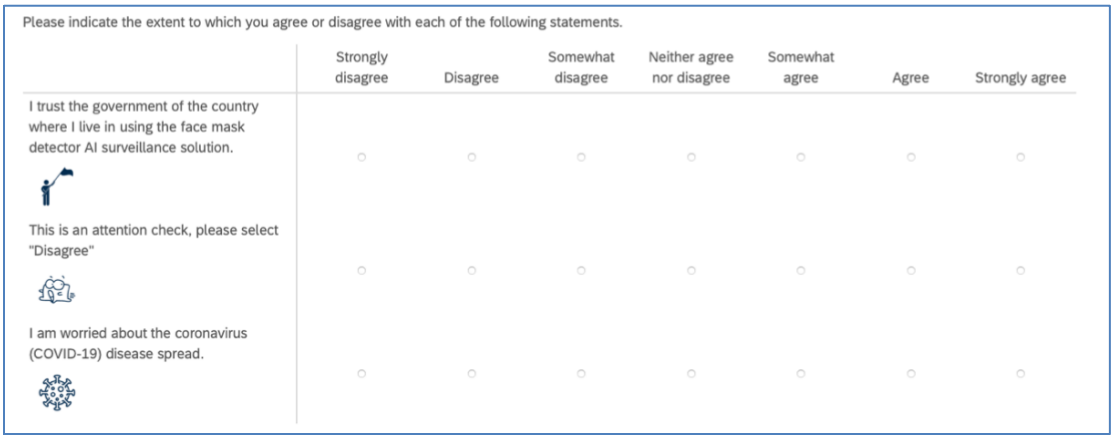
Government intrusiveness concerns



Please indicate the extent to which you agree or disagree with each of the following statements.

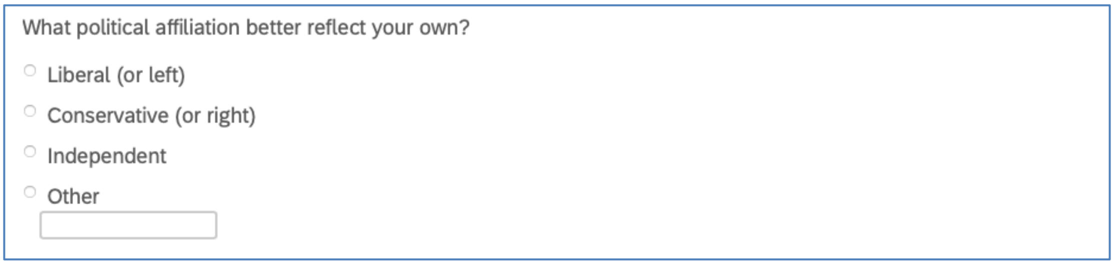
	Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
I am concerned that my internet accounts and database information (e.g., e-mails, shopping records, tracking my Internet surfing, etc.) will be more open to government/business scrutiny.	○	○	○	○	○	○	○
I am concerned about the government's ability to monitor internet activities.	○	○	○	○	○	○	○
I am willing to take additional actions to avoid tracking.	○	○	○	○	○	○	○

Controls: GT, attention check, COVID-19 fear, demographics



Please indicate the extent to which you agree or disagree with each of the following statements.

	Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
I trust the government of the country where I live in using the face mask detector AI surveillance solution.	○	○	○	○	○	○	○
This is an attention check, please select "Disagree"	○	○	○	○	○	○	○
I am worried about the coronavirus (COVID-19) disease spread.	○	○	○	○	○	○	○



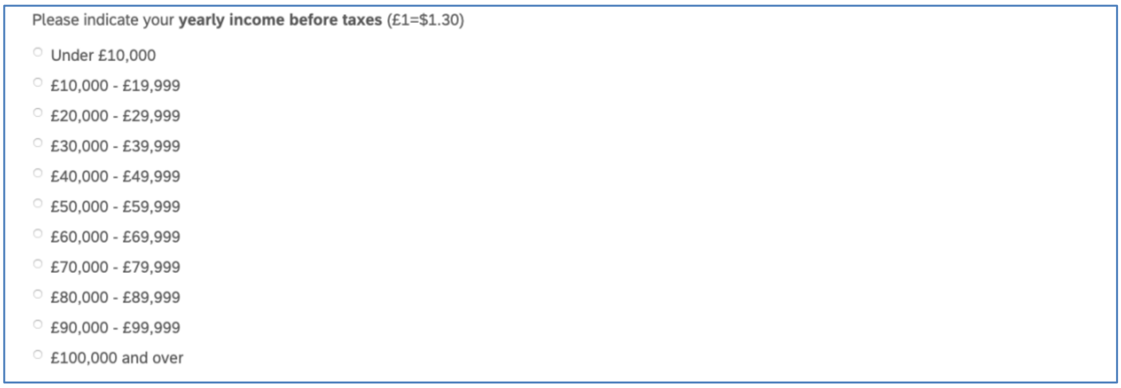
What political affiliation better reflect your own?

○ Liberal (or left)

○ Conservative (or right)

○ Independent

○ Other



Please indicate your **yearly income before taxes** (£1=$1.30)

○ Under £10,000

○ £10,000 - £19,999

○ £20,000 - £29,999

○ £30,000 - £39,999

○ £40,000 - £49,999

○ £50,000 - £59,999

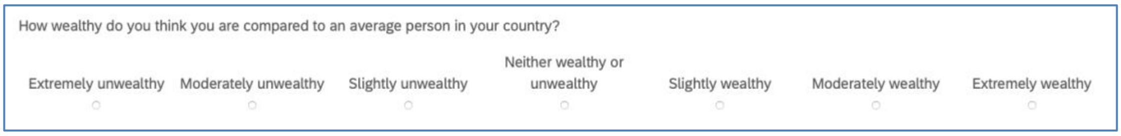
○ £60,000 - £69,999

○ £70,000 - £79,999

○ £80,000 - £89,999

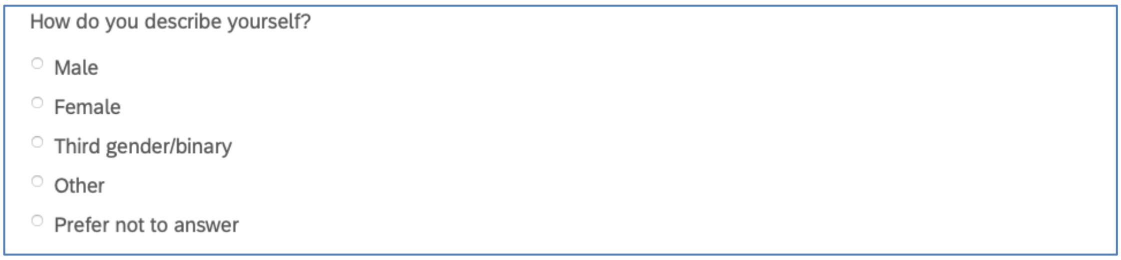
○ £90,000 - £99,999

○ £100,000 and over



How wealthy do you think you are compared to an average person in your country?

Extremely unwealthy	Moderately unwealthy	Slightly unwealthy	Neither wealthy or unwealthy	Slightly wealthy	Moderately wealthy	Extremely wealthy
○	○	○	○	○	○	○



How do you describe yourself?

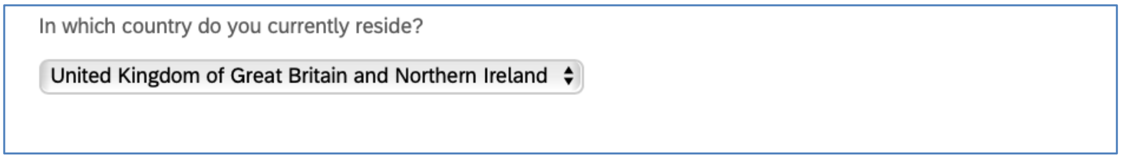
○ Male

○ Female

○ Third gender/binary

○ Other

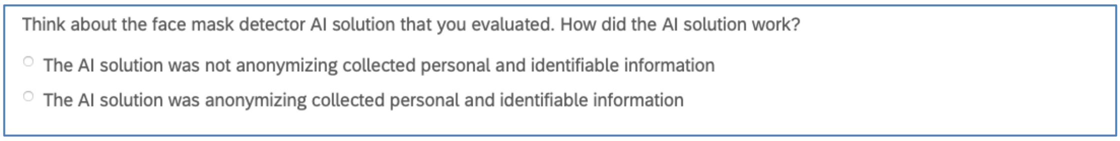
○ Prefer not to answer



In which country do you currently reside?

United Kingdom of Great Britain and Northern Ireland

Manipulation check

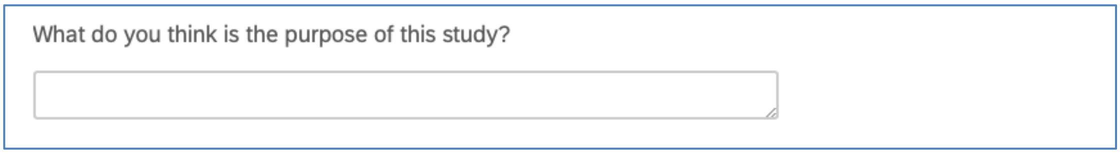


Think about the face mask detector AI solution that you evaluated. How did the AI solution work?

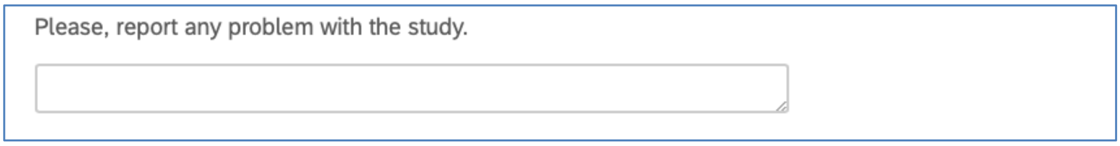
○ The AI solution was not anonymizing collected personal and identifiable information

○ The AI solution was anonymizing collected personal and identifiable information

Attention check



What do you think is the purpose of this study?



Please, report any problem with the study.

Appendix 2: Tables of data analysis

Outliers examination by computing z-score of variables

Descriptive Statistics

	n	Minimum	Maximum
Zscore(Will)	400	-1.35796	1.65415
Zscore(Disclose)	400	-.66163	1.50764
Zscore(PU1)	400	-1.77146	1.49893
Zscore(PU2)	400	-1.57460	1.59042
Zscore(PU3)	400	-1.46981	1.67978
Zscore(PC1)	400	-3.03951	1.07025
Zscore(PC2)	400	-3.28171	1.04582
Zscore(PC3)	400	-3.27520	1.04137
Zscore(ME1)	400	-1.47122	1.70408
Zscore(ME2)	400	-1.45022	1.76951
Zscore(ME3)	400	-1.38551	1.96991
Zscore(ME4)	400	-1.43435	1.65303
Zscore(ME5)	400	-1.53276	1.62215
Zscore(GS1)	400	-.86209	3.72553
Zscore(GS2)	400	-.45738	5.48261
Zscore(GS3)	400	-.71144	3.34236
Zscore(GS4)	400	-.95244	2.61921
Zscore(GI1)	400	-2.84576	1.28102
Zscore(GI2)	400	-2.57719	1.25982
Zscore(GI3)	400	-2.38716	1.55042
Valid N (listwise)	400		

Appendix 3: Demographic descriptives

Demographic descriptives

Baseline Characteristic	Non-distraction				Distraction				Full Sample	
	Anonymized		Identifiable		Anonymized		Identifiable			
	n	%	n	%	n	%	n	%	n	%
Country										
United Kingdom of Great Britain and Northern Ireland	109	96	89	99	105	96	83	95	386	97
United States of America	4	4	1	1	4	4	4	5	13	3
Gender										
Female	70	62	63	70	77	71	57	66	267	67
Male	41	36	23	26	28	26	28	32	120	30
Third gender/binary	1	1	1	1	3	3	0	0	5	1
Prefer not to answer	0	0	2	2	0	0	2	2	4	1
Other	1	1	1	1	1	1	0	0	3	1
Income										
Under £10,000	25	22	21	23	23	21	21	24	90	23
£10,000 - £19,999	25	22	22	24	26	24	11	13	84	21
£20,000 - £29,999	19	17	17	19	28	26	25	29	89	22
£30,000 - £39,999	22	19	12	13	18	17	12	14	64	16
£40,000 - £49,999	10	9	10	11	4	4	8	9	32	8
£50,000 - £59,999	4	4	4	4	3	3	4	5	15	4
£60,000 - £69,999	2	2	0	0	2	2	3	3	7	2
£70,000 - £79,999	0	0	3	3	1	1	2	2	6	2
£80,000 - £89,999	2	2	1	1	2	2	0	0	5	1
£90,000 - £99,999	2	2	0	0	0	0	1	1	3	1
£100,000 and over	2	2	0	0	2	2	0	0	4	1
Perceived Wealth										
Extremely unwealthy	2	2	9	10	4	4	4	5	19	5
Moderately unwealthy	14	12	8	9	20	18	11	13	53	13
Slightly unwealthy	18	16	18	20	24	22	15	17	75	19
Neither wealthy or unwealthy	54	48	36	40	35	32	30	34	155	39

Slightly wealthy	20	18	13	14	20	18	19	22	72	18
Moderately wealthy	5	4	5	6	6	6	8	9	24	6
Extremely wealthy	0	0	1	1	0	0	0	0	1	0
Political Orientation										
Liberal (or left)	51	45	50	56	63	58	55	63	219	55
Conservative (or right)	27	24	16	18	22	20	15	17	80	20
Independent	18	16	13	14	13	12	8	9	52	13
Other	17	15	11	12	11	10	9	10	48	12
Fear of COVID-19 (I am worried about the coronavirus (COVID-19) disease										
Strongly disagree	5	4	2	2	6	6	3	3	16	4
Disagree	5	4	1	1	2	2	5	6	13	3
Somewhat disagree	12	11	7	8	11	10	6	7	36	9
Neither agree nor disagree	4	4	8	9	8	7	6	7	26	7
Somewhat agree	35	31	16	18	18	17	26	30	95	24
Agree	40	35	36	40	39	36	22	25	137	34
Strongly agree	12	11	20	22	25	23	19	22	76	19
Government Trust (I trust the government of the country where I live in using the face mask detector AI surveillance solution)										
Strongly disagree	31	27	24	27	34	31	29	33	118	30
Disagree	15	13	17	19	22	20	16	18	70	18
Somewhat disagree	11	10	12	13	10	9	16	18	49	12
Neither agree nor disagree	17	15	11	12	11	10	8	9	47	12
Somewhat agree	29	26	20	22	22	20	11	13	82	21
Agree	7	6	6	7	6	6	6	7	25	6
Strongly agree	3	3	0	0	4	4	1	1	8	2

Appendix 4: Normality examination with Skewness and Kurtosis Statistic

Descriptive Statistics

	N	Skewness		Kurtosis	
	Statistic	Statistic	Std. Error	Statistic	Std. Error
Will	399	.087	.122	-1.328	.244
Disclose	399	.859	.122	-1.268	.244
PU1	399	-.336	.122	-.981	.244
PU2	399	-.115	.122	-1.150	.244
PU3	399	-.028	.122	-1.189	.244
PC1	399	-1.083	.122	.907	.244
PC2	399	-1.292	.122	1.666	.244
PC3	399	-1.124	.122	.966	.244
ME1	399	.036	.122	-1.062	.244
ME2	399	.030	.122	-1.042	.244
ME3	399	.196	.122	-.913	.244
ME4	399	.056	.122	-1.136	.244
ME5	399	-.013	.122	-1.092	.244
GS1	399	1.259	.122	1.209	.244
GS2	399	2.769	.122	**8.414**	.244
GS3	399	1.447	.122	1.315	.244
GS4	399	.738	.122	-.576	.244
GI1	399	-.706	.122	.015	.244
GI2	399	-.678	.122	-.232	.244
GI3	399	-.385	.122	-.456	.244
Valid N (listwise)	399				

Appendix 5: Principal Component Analysis

Items correlation

Spearman's rank-order Correlations

	PU1	PU2	PU3	PC1	PC2	PC3	ME1	ME2	ME3	ME4	ME5	GS1	GS2	GS3	GS4	GI1	GI2	GI3
PU1	--																	
PU2	.897**	--																
PU3	.886**	.871**	--															
PC1	-.402**	-.415**	-.475**	--														
PC2	-.375**	-.423**	-.459**	.877**	--													
PC3	-.261**	-.294**	-.333**	.779**	.820**	--												
ME1	.716**	.699**	.770**	-.585**	-.573**	-.461**	--											
ME2	.709**	.683**	.752**	-.580**	-.563**	-.448**	.912**	--										
ME3	.683**	.660**	.724**	-.604**	-.587**	-.477**	.822**	.831**	--									
ME4	.723**	.686**	.760**	-.542**	-.520**	-.423**	.814**	.805**	.827**	--								
ME5	.733**	.718**	.765**	-.456**	-.436**	-.326**	.770**	.765**	.732**	.750**	--							
GS1	.502**	.514**	.533**	-.537**	-.550**	-.434**	.579**	.559**	.587**	.554**	.502**	--						
GS2	.235**	.260**	.246**	-.277**	-.312**	-.283**	.267**	.264**	.298**	.239**	.239**	.502**	--					
GS3	.281**	.274**	.298**	-.405**	-.371**	-.340**	.346**	.342**	.338**	.315**	.299**	.613**	.487**	--				
GS4	.419**	.415**	.450**	-.491**	-.487**	-.382**	.557**	.541**	.538**	.492**	.447**	.640**	.371**	.664**	--			
GI1	-.250**	-.266**	-.295**	.530**	.523**	.487**	-.407**	-.419**	-.426**	-.407**	-.305**	-.425**	-.274**	-.314**	-.432**	--		
GI2	-.218**	-.221**	-.235**	.486**	.473**	.463**	-.345**	-.345**	-.379**	-.350**	-.256**	-.399**	-.229**	-.348**	-.444**	.773**	--	
GI3	-.258**	-.268**	-.265**	.362**	.340**	.296**	-.294**	-.299**	-.303**	-.291**	-.275**	-.380**	-.265**	-.291**	-.382**	.517**	.612**	--

**. Correlation is significant at the 0.01 level (2-tailed).

Items	Indidual KMO
PU1	.824a
PU2	.855a
PU3	.877a
PC1	.899a
PC2	.819a
PC3	.865a
GS1	.920a
GS3	.814a
GS4	.903a
GI1	.848a

GI2	.799a
GI3	.902a

Total Variance Explained

	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings[a]
Component	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total
1	5.793	48.279	48.279	5.793	48.279	48.279	3.968
2	1.934	16.120	64.399	1.934	16.120	64.399	4.311
3	1.226	10.218	74.617	1.226	10.218	74.617	3.698
4	1.105	9.210	83.827	1.105	9.210	83.827	3.860
5	.477	3.976	87.803				
6	.394	3.280	91.083				
7	.316	2.637	93.719				
8	.222	1.850	95.569				
9	.201	1.676	97.245				
10	.128	1.063	98.308				
11	.109	.910	99.218				
12	.094	.782	100.000				

Extraction Method: Principal Component Analysis.

a. When components are correlated, sums of squared loadings cannot be added to obtain a total variance.

Communalities

	Initial	Extraction
PU1	1.000	.926
PU2	1.000	.921
PU3	1.000	.914
PC1	1.000	.869
PC2	1.000	.923
PC3	1.000	.881
GS1	1.000	.718
GS3	1.000	.839
GS4	1.000	.746
GI1	1.000	.771
GI2	1.000	.842
GI3	1.000	.708

Extraction Method: Principal Component Analysis.

Appendix 6: Logistic Regression

According to Tabachnick & Fidell (2014), Bonferroni correction based on all terms (including the intercept) in the model when assessing this linearity assumption. If the interaction effect is statistically significant, the original continuous independent variable would be not linearly related to the logit of the dependent variable. Thus, the linearity assumption would be failed if p-value less than new alpha (α) level of 0.05/13 = .00384. As belowed table, all p-value is larger than .00384, the linearity assumption would not be rejected.

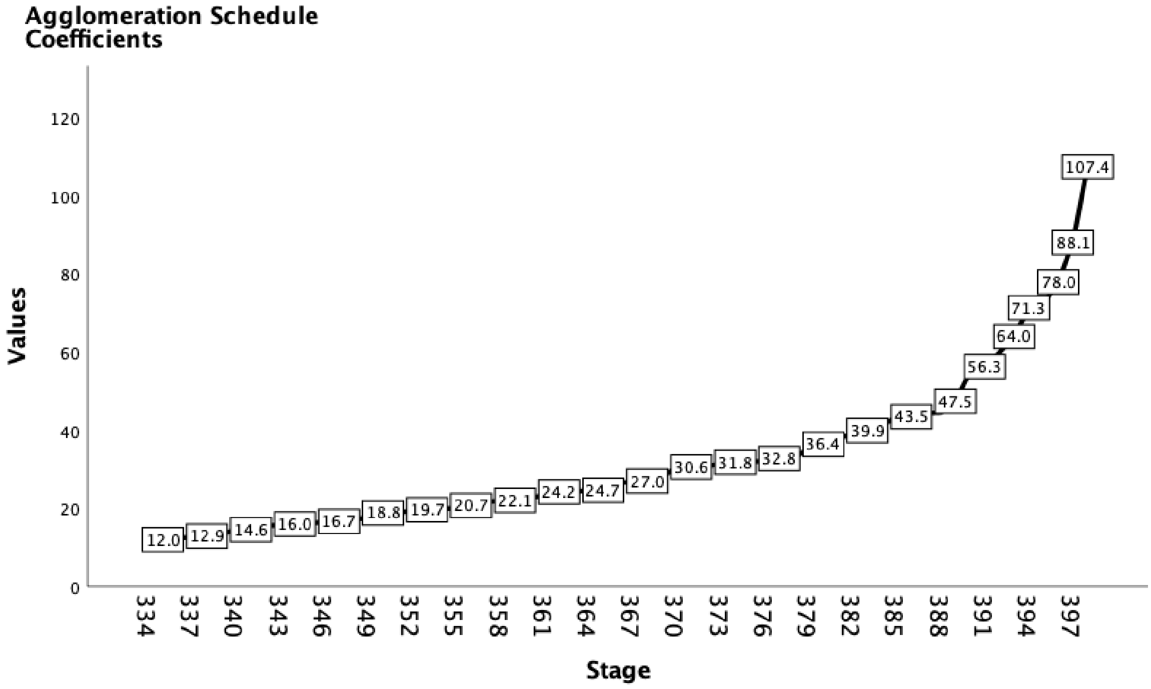
Variables in the Equation

								95% C.I.for EXP(B)	
		B	S.E.	Wald	df	p	Exp(B)	Lower	Upper
Step 1[a]	Will	-.106	.907	.014	1	.907	.899	.152	5.324
	ME1	-1.074	1.395	.592	1	.441	.342	.022	5.264
	ME2	2.965	1.534	3.737	1	.053	19.387	.960	391.639
	ME3	.186	1.173	.025	1	.874	1.204	.121	12.002
	ME4	-.852	.951	.803	1	.370	.427	.066	2.751
	ME5	.550	.969	.322	1	.570	1.733	.259	11.576
	LNME1 by ME1	.396	.573	.478	1	**.489**	1.486	.483	4.568
	LNME2 by ME2	-1.121	.637	3.095	1	**.079**	.326	.094	1.136
	LNME3 by ME3	-.088	.498	.031	1	**.860**	.916	.345	2.430
	LNME4 by ME4	.343	.398	.740	1	**.390**	1.409	.645	3.074
	LNME5 by ME5	-.104	.406	.065	1	**.798**	.901	.407	1.999
	LNWILL by Will	.175	.385	.206	1	**.650**	1.191	.560	2.533
	Constant	-5.345	1.584	11.384	1	.001	.005		

a. Variable(s) entered on step 1: Will, ME1, ME2, ME3, ME4, ME5, LNME1 * ME1 , LNME2 * ME2 , LNME3 * ME3 , LNME4 * ME4 , LNME5 * ME5 , LNWILL * Will .

Appendix 7: Cluster Analysis

Agglomeration Schedule Coefficients



ANOVA

	Cluster		Error			
	Mean Square	df	Mean Square	df	F	Sig.
Score_mask1	1030.191	2	3.443	396	299.191	.000
Score_mask2	945.175	2	5.078	396	186.138	.000
Score_Gen	103.391	2	5.304	396	19.494	.000
Score_Time	897.087	2	6.339	396	141.518	.000
Score_Skin	25.898	2	2.805	396	9.233	.000
Score_Name	21.619	2	4.326	396	4.997	.007
Score_Pol	16.201	2	2.404	396	6.738	.001
Score_Loc	924.429	2	4.272	396	216.393	.000

The F tests should be used only for descriptive purposes because the clusters have been chosen to maximize the differences among cases in different clusters. The observed significance levels are not corrected for this and thus cannot be interpreted as tests of the hypothesis that the cluster means are equal.