Since January 2020 Elsevier has created a COVID-19 resource centre with free information in English and Mandarin on the novel coronavirus COVID-19. The COVID-19 resource centre is hosted on Elsevier Connect, the company's public news and information website.

Elsevier hereby grants permission to make all its COVID-19-related research that is available on the COVID-19 resource centre - including this research content - immediately available in PubMed Central and other publicly funded repositories, such as the WHO COVID database with rights for unrestricted research re-use and analyses in any form or by any means with acknowledgement of the original source. These permissions are granted for free by Elsevier for as long as the COVID-19 resource centre remains active.
Privacy and surveillance attitudes during health crises: Acceptance of surveillance and privacy protection behaviours

Athina Ioannou a, b, *, Iis Tussyadiah b

a Surrey Business School, University of Surrey, United Kingdom
b School of Hospitality and Tourism Management, University of Surrey, United Kingdom

A R T I C L E   I N F O

Keywords:
- Government surveillance
- Privacy concerns
- Pandemic
- Track and trace
- Personal data

A B S T R A C T

The wide deployment of digital technologies for the management of the COVID-19 pandemic has triggered concerns about privacy and intrusion from government surveillance. This study investigates individual privacy and surveillance attitudes by developing a theoretical model to explain acceptance of government surveillance and privacy protection behaviours during health crises, such as the COVID-19 pandemic. Results from a US sample reveal that people are concerned about the collection and use of their personal information via mobile applications and the monitoring of their online activities by authorities. Findings reveal the important roles of political trust and belief that governments’ need to be proactive in protecting peoples’ welfare during a crisis that can increase acceptance of surveillance and thus assist in the management of the health crisis. Implications for research and practice are discussed.

1. Introduction

The COVID-19 pandemic has rapidly spread in numerous parts of the world, bringing severe economic, social, political, and psychological consequences. Approximately 230 million people have been infected and more than four million deaths recorded as of September 2021 [1]. In response to this crisis, governments and scientists around the globe have been working tirelessly to discover a vaccine and/or medication to treat the disease, in order to safeguard societies and allow economies to recover from the unprecedented costs brought by the pandemic and its associated lockdown measures. In particular, global efforts have been intensified towards leveraging advanced technologies to better understand the virus (e.g. deep learning models predicting old and new medications that could be used for the treatment of COVID-19), to detect, diagnose, and monitor the outbreak (e.g. early warning systems), to limit the contagion and prevent the spread of the virus (e.g. population surveillance), and to assist in the response to the crisis (e.g. virtual chatbots deployed by healthcare systems triaging patients) [2].

Digital technologies have been heavily deployed in the management of a pandemic. The most popular example of such technology implementation is contact tracing applications, “a mobile platform that assists the identification of people who may have come into contact with an infected person, and the subsequent collection of further information about these contacts for containing the virus’ spreading” (J. [3]; p. 1). Using Bluetooth and/or GPS technologies, contact tracing tools attempt to identify people’s movements allowing the tracing and tracking of infections as well as alerting people of a potential contagion risk [2]. Several countries, such as China, Germany, Singapore, Israel, Australia, and the UK, have rolled out contact tracing applications, collecting a wide range of data, such as CCTV images from surveillance cameras and smartphone geolocation data, gaining detailed timelines of people’s physical movements to better understand the establishment of virus chains in the community [4]. Apart from contact tracing, digital technologies are integrated into several mitigation and containment strategies, ranging from tracking, screening, and testing to quarantine and clinical management [4]. The collection of big data and analysis using Artificial Intelligence (AI) have allowed for better planning and tracking of the spread of the pandemic. Tools such as migrations maps have been used, collecting data from mobile payment applications and social media in order to identify people’s real-time location of people (e.g. China) and integrating immigration records with health insurance databases to access patients’ travel history (e.g. Taiwan) [4]. Various tools are also used for screening and evaluating signs of the virus in asymptomatic populations. These include applications that collect data regarding symptoms that people are reporting (e.g., Iceland, UK), digital thermometers and smartwatches that collect real-time data to identify
local or regional outbreaks (e.g., USA), and biometric data such as pulse, temperature, and sleep pattern to identify infected patients (e.g., Germany) [4]. GPS technologies have been deployed to enforce quarantine or self-isolation measures, tracking people through their mobile phones (e.g., Taiwan) and specific mobile applications (e.g., South Korea), as well as wearable devices, such as a wristbands, linked to cloud technology, alerting authorities in case of a breach (e.g., Hong Kong) [4].

The implementation of digital technology and surveillance tools has proved to be of significant value during past disease outbreaks, such as cholera and Ebola [5]. However, imminent threats to individual privacy have been raised, triggered by the collection of personal information with contact tracing applications (e.g., real time location), monitoring of online activities (e.g., Google search terms), and biometric verification (e.g., thermal cameras checking body temperature in airports and other places). The media and privacy advocates have highlighted the emergence of ‘extreme’ tracking solutions, such as the implementation of a repurposed counter-terrorism technology by the Israeli security and intelligence services, which has been criticized by the High Court that “severely violates the constitutional right to privacy” [6]. This becomes a subject of controversy and attracts public attention to individual rights to privacy. Privacy experts have noted fears that such surveillance measures and tracking tools might become a standard practice in the future [6]. High uncertainty also revolves around future use of the aggregated data after the pandemic crisis is over.

While extensive research has been conducted on privacy concerns and information disclosure with online providers in commercial settings, there is a surprising paucity of research on public views and opinions regarding government surveillance [7,8], acceptance of such monitoring activities, and the subsequent influence on privacy behaviour [9–11]. Considering its heightened relevance due to COVID-19, it is imperative to understand in more depth people’s attitudes towards governmental data collection and monitoring during the pandemic to offer valuable knowledge and insights in the battle of the pandemic as well as future ones [12]. Recently, studies on public attitudes towards government surveillance and implemented measures to manage the COVID-19 pandemic have emerged. Most of them are theoretical evaluations and opinion papers, with a limited base of empirical research. Most empirical studies focus on the acceptance and use of contact tracing applications, with little consideration of other types of digital surveillance, such as real time location tracking, travel history, and biometric data. Moreover, these studies mainly present public opinion and their demographic characteristics, but lacking an overarching theoretical framework explaining the phenomenon of government surveillance, its predictors, and other influential factors. The present study aims to address this gap by developing a theoretical model, grounded in well-established IS theories, aiming to identify the antecedents of acceptance of surveillance and the subsequent impact on privacy protection behaviour during the COVID-19 pandemic. The model explains the factors that affect acceptance of surveillance and privacy protection behaviours, by contextualising them in the COVID-19 pandemic, which serves as a foundation for researchers, practitioners, and policymakers, which fight as the current pandemic as well as future health crises using the power of digital technologies as a tool. This work thus contributes to theory and practice by informing the design and development of digital technology and epidemiological tools, such as contact tracing, tracking, screening, quarantine, and clinical management applications, used in the COVID-19 pandemic, which can be valuable for managing future epidemics/pandemics and health crises. This work highlights the need for privacy-preserving aspects in such digital solutions, informing governments about the appropriation of such technologies, highlighting the need to consider and integrate people’s perceptions of privacy and surveillance into relevant policies and frameworks.

2. Theoretical background and hypotheses

Surveillance has been defined as “any collection and processing of personal data, whether identifiable or not, for purposes of influencing or managing those whose data have been garnered” [13]; p. 2) and “any systematic and routine attention to personal details, whether specific or aggregate, for a defined purpose” [14]; p. 13). Surveillance can be physical (e.g., security checks at a country’s borders) or digital/transactional (e.g., monitoring of online activities and transactions) [11]. This study focuses on the latter. The advancements in information and communication technologies (ICTs) have given governments the opportunity to harness the immense power of digital tools to collect, process, and store large amounts of citizens’ data to effectively prevent and detect crimes and terrorist activities, privacy and security breaches, and fraudulent events [9]. Surveillance policies and measures adopted by governments include communication monitoring through the collection and analysis of phone calls logs, email communications, and information gathered from social networking sites, location determination through mobile phones’ geospatial location, visual surveillance through CCTV, collection and analysis of passengers’ data when traveling by air or sea, biometric identification through biometric signatures including face, iris, and fingerprint [8,11]. More recently, surveillance as a concept has attracted significant attention and interest from governments’ and the media around the world, especially due to the alarming increase of terrorist events the last decades (e.g., 9/11 attacks), and recently a virus pandemic (COVID-19) [15].

According to Ref. [16]; most privacy research can be viewed under the Antecedents – Privacy Concerns – Outcomes (APCO) model where privacy concerns, influenced by other antecedents, determine behavioural reactions. Recently, few studies on privacy and surveillance have been conducted in the COVID-19 pandemic context. A summary of related work is presented in Table A1 in Appendix A. Three key issues are evident from the summary: (1) most empirical research has focused on privacy and surveillance in general contexts, (2) research on privacy, surveillance, and COVID-19 has mainly focused on the acceptance of contact tracing applications, with little consideration on other types of digital surveillance, such as monitoring of real time location, travel history, biometric data, and quarantine enforcement, and (3) most empirical COVID-19 research has been limited to examining public privacy and surveillance opinions by conducting frequency analysis, with scarcity in research that develops a theoretical model and assesses the relationships of the constructs in a nomological framework. Thus, using the APCO model as an overarching framework and informed by the results from past research, the present study aims to extend previous work to better understand privacy and government surveillance attitudes as well as identify the antecedents of surveillance acceptance, and assess its impact on privacy protection behaviours in the COVID-19 pandemic context.

2.1. Antecedents of acceptance of government surveillance

Information privacy can be defined as “some form of control over the potential secondary uses of one’s personal information” [17]; p. 1018), describing the feelings of individuals regarding what happens to personal information they disclose to online providers. Since privacy concerns reflect one’s inherent worry about the potential negative consequences that may arise due to the disclosure of personal information across different online environments and providers [18]; P. [19], it can be argued that government intrusion concerns encompass somewhat similar feelings of worry as they describe the ‘negative belief[s] about the proactive gathering and processing of personal information and monitoring online behaviour by the government’ [19]; p. 220). Government surveillance involves the collection, secondary use, processing, and analysis of personal information, where individuals’ control is limited. Privacy and government intrusion concerns are closely related, but distinct in the fact that the latter can exist even without any violation of privacy; having the knowledge that one is being monitored can result in substantial changes in conscious behaviour [10]. For decades, the major source of concern and principal threat around
individual privacy has been the commercial data exploitation – monetisation from business firms (e.g., targeted advertising) [20]. However, the recent emergence of privacy and surveillance scandals (e.g., Edward Snowden’s disclosure of governments’ intelligence services of mass surveillance practices) has highlighted the fact that government monitoring activities and security policies also introduce high privacy risks [20]; while recently, research has argued that surveillance and lack of privacy can pose a threat to an individual’s freedom [21].

Epidemiological digital surveillance has already been employed in previous disease outbreaks, such as the cholera epidemic in 2010 and Ebola in 2014 [5,22], where a wide range of digital data sources were used. These approaches have been shown effective in accurately tracking the spread of a disease and detecting a virus epidemic early [22]. However, mass collection of users’ personal data triggered concerns over privacy and data protection [22]. In the context of COVID-19, as digital footprints are being tracked through new monitoring tools, people may feel that their privacy is being threatened, and they would lose control over the management of their data [23]. For example, authorities in South Korea publish information of confirmed COVID-19 patients publicly (e.g., gender, nationality, occupation, routes and location histories) to provide greater transparency and offer a sense of trustworthiness to the public but raising concerns of the patients’ privacy [23]. Privacy concerns also relate to the ‘problematic’ aspects of various applications, such as difficulty to anonymise real time location data (e.g., Israel, South Korea), systems developed with centralised architecture (data are not stored locally on the user’s mobile phone but in a governmental server thus being controlled by authorities) (e.g., UK), issues relating to user consent (i.e., users have to consent to the use of their data not only for tracking of the disease, but also for research purposes) (e.g., Norway) [3] [23].

Theoretical evaluations and opinions on privacy and surveillance have been more prominent than empirical research on the topic. Existing empirical research has mainly focused on cross-cultural differences in attitudes towards government surveillance in general contexts [24]. Investigated differences in online privacy concerns and surveillance attitudes of Internet users across five cities: Bangalore, New York, Seoul, Singapore, and Sydney. Results revealed that people in Seoul expressed the most negative attitudes towards surveillance, while people in Bangalore the most positive ones. Exploring cultural differences between Italy and US [9], found that coming from a more individualistic society, US users showed more accepting attitudes towards government surveillance, while Italian users had lower tolerance on privacy intrusion and found such practices an inhibiting factor to performing online activities [25]. Examined users’ opinions about surveillance concerns in post-communist countries such as Croatia and showed that older people show less trust in governmental institutions, resulting in enhanced privacy protection behaviours such as falsifying information or refusing to disclose personal information online.

Furthermore, existing research has also focused on identifying factors contributing to concerns over government intrusion, beliefs, and privacy-related behaviours [10]. Demonstrated that privacy concerns and surveillance attitudes are important predictors of behavioural intention to make online transactions with e-commerce providers. Moreover [26], argue that the exposure to news stories relevant to government surveillance can contribute to higher concerns over (government) intrusion and the use of weaker passwords to protect user personal information [27]. Found that people who are more accepting of surveillance measures tend to adopt weaker protection behaviours, such as changing privacy settings on social media or using more complex passwords. While Nam, (2019) revealed that surveillance concerns, regulatory needs, and perceived transparency constitute the main determinants of individual’s acceptance of government surveillance.

Recently, research investigating public surveillance attitudes in the COVID-19 context has emerged, mostly focusing on contact tracing applications. Recent evidence suggests that privacy and surveillance attitudes vary systematically across countries, with the US being less supportive of such digital surveillance measures and concerns about privacy and security identified as an important barrier in adoption of contact tracing app [28]. Similar findings have been found by Ref. [29] who investigated the intention to use a wide range of COVID-19 applications (e.g., contact tracing, symptom tracking, quarantine enforcement) in three countries: Germany, US, and China. Results suggest that privacy concerns were identified as the major negative aspect regarding the use of COVID-19 related applications, with US participants reported more worries about government surveillance. In their study [30], argue that the public is reluctant to support not only the use of contact tracing applications during the COVID-19 pandemic but also the implementation of other forms of surveillance: CCTV cameras, drones, thermal cameras, device monitoring, and checking of credit card transactions. Features such as Bluetooth without location tracking and decentralised storage of citizens’ data increase the likelihood that an individual will install the contact tracing application, revealing the major role of concerns about privacy and surveillance in the acceptance of digital surveillance technologies [31]. Show that 80% of participants in their study were willing to install contact tracing applications that are perfectly private and accurate. Overall, it is apparent that privacy and surveillance concerns play a critical role in the acceptance of digital surveillance measures during COVID-19.

The aforementioned studies indicate the negative effects of concerns over (a) privacy and (b) surveillance on acceptance of digital applications. Hence, it is expected that during COVID-19 pandemic people with higher levels of concerns over the collection and use of their personal information (in this case through mobile applications) and concerns over governments’ monitoring of online activities during the pandemic will be less likely to accept government surveillance:

H1. Mobile privacy concerns will negatively influence acceptance of government surveillance

H2. Government intrusion concerns will negatively influence acceptance of government surveillance

One of the major purposes of government surveillance is the provision of greater security to citizens by preventing and detecting early threats, including crimes and terrorist activities, security breaches, and large-scale tragedy events (e.g., 9/11 attacks). Perceived need for government surveillance refers to individuals’ positive beliefs about the government needing to increase monitoring practices of online activities to ensure the safety and security of citizens [10]. Reflecting the beneficial aspects of surveillance, including protection, security, social order and reduction of risk, perceived need for government surveillance can encourage voluntary participation of citizens (e.g., use of contact tracing applications) and support for such monitoring practices during the pandemic. Past research has shown that perceived need for surveillance is an important predictor of acceptance of government surveillance [27]. During the COVID-19 pandemic, people who support the installation of contact tracing applications mentioned that the protection of their family and friends, responsibility to the community, and the potential stopping of the pandemic are the main reasons behind their willingness to use such apps [28]. [29] found that tracing of infected people, getting information about their area, identifying hotspots, and keeping people safe were perceived as the positive aspects of using such applications. Perceived need for surveillance, such that individuals perceive surveillance initiatives as measures for ensuring protection and reliability, can be a positive factor [10]. People who believe that the government performs surveillance in an ethical manner and implements fair policies in practice have less concerns about their privacy [10]. Thus, during COVID-19, citizens who perceive surveillance as a positive factor will find government surveillance beneficial. Therefore, it can be suggested that people with higher beliefs that governments need to be proactive in ensuring a secure environment for their citizens will be more likely to accept monitoring measures for better management of the COVID-19 pandemic.
H3. Perceived need for government surveillance will positively influence acceptance of government surveillance

Most applications developed for the management and containment of the pandemic (e.g., contact-tracing and symptom tracking apps) have one thing in common: their usage is completely voluntary. Trusting that government authorities are acting towards serving peoples’ best interests and needs, including the protection of individual personal privacy, is crucial to the successful implementation of such tools. After major incidents (e.g., 9/11 attacks), people demonstrated more trusting attitudes towards the government and its associated authorities and were more willing to trade-off civil liberties (e.g., privacy) to gain greater protection and security [32]. Previous research has shown that people who are more trusting towards governments and political institutions express more positive beliefs about surveillance-oriented security technologies, considering them as effective solutions in enhancing security while at the same time avoiding the infringement of their privacy [33]. In their study [8], demonstrated that higher levels of citizens’ political trust can encourage the support of surveillance measures used by governments. In the context of COVID-19, recent evidence suggests that trust in the government to handle the health crisis is positively associated with the acceptability of such digital epidemiological solutions [34]. Trust in the government to “do what is right” is an important determinant of support of contact tracing applications deployed in the COVID-19 pandemic [28]. That is, people who trust the government are more likely to accept digital surveillance measures, while people who trust the government less express more concerns about privacy and surveillance [28]. Therefore, we expect that during the COVID-19 pandemic, people with higher levels of trusting beliefs in the government (i.e., political system) are more likely to accept digital surveillance measures that the government enacts to better manage and contain the disease and protect citizens’ welfare:

H4. Trust in the government to act towards protecting citizen’s best interest will positively influence acceptance of government surveillance

2.2. Privacy protection behaviour

Privacy protection behaviours can be described as strategies adopted by individuals to control and prevent the potential loss of privacy and personal information [35]. Privacy studies have operationalised privacy protection behaviours in several ways, including using stronger passwords [26], changing passwords more often [35], installing antivirus software [35], falsifying information [36,37], and even refusing to share personal information [36,37]. Indeed, users have adopted a variety of obfuscating tools to protect their online privacy and digital traces, such as temporary email addresses, encryption in digital communications, anonymizers, and virtual private networks (VPN) [20,27,38]. Evidence suggests that in the aftermath of critical privacy and security related events, (e.g., 9/11 attacks, NSA revelations from Edward Snowden), privacy and surveillance concerns have been exacerbated and people experienced increased levels of anxiety and worry about the potential negative consequences that might occur [39]. More specifically in the post Snowden era, evidence indicates a surge in information seeking and browsing behaviours regarding privacy related topics as well as adoption of privacy enhancing technologies (e.g. anonymisation proxies) and privacy enhancing configuration behaviours such as adjusting privacy settings in web browsers and installing add-on services hiding IP address [40]. In the COVID-19 context, people with higher privacy concerns in the US, compared to other countries, reported less willing to install and use COVID-19 related applications [28,29], and more likely to mention concerns about government surveillance as one of the reasons against the installation of such applications [28,29]. This demonstrates the important role of concerns about privacy and government intrusion in forming individual privacy behaviours. Research has shown that people with higher privacy concerns are more likely to adopt risk reduction behaviours [41], while individuals who tend to accept governments’ monitoring and surveillance policies are less likely to deploy privacy protections [27]. Also, people worrying about their online activities being monitored and their transactions scrutinised by governmental authorities are more reluctant to share personal information with business firms and providers [10]. Overall, it is expected that during COVID-19 people experiencing higher levels of concerns about privacy and government intrusion will undertake stronger actions to protect their privacy; while individuals who find government surveillance practices directed towards the better management of the outbreak more acceptable will adopt less risk reduction privacy behaviours. Therefore, it can be hypothesized that:

H5. Mobile privacy concerns will positively influence privacy protection behaviours

H6. Government intrusion concerns will positively influence protection behaviours

H7. Acceptance of surveillance will negatively influence protection behaviours

2.2.1. Demographic factors

Demographic factors have been deemed as important predictors of privacy concerns [42]. Prior studies suggest that there are gender differences in privacy behaviours with female users expressing higher privacy concerns [42,43]. For users with more Internet experience, privacy concerns may decrease over time, although results have been inconsistent [44,45]. As a result, these demographic factors are included in the multigroup analysis of the present study to evaluate the proposed theoretical model.

3. Research methodology

To test the proposed hypotheses, this study followed a cross-sectional approach and developed an online survey. Data were collected from the 4th until the June 5, 2020 June 2020 through Amazon Mechanical Turk (MTurk), an online crowdsourcing market that has been validated by previous research as an equivalent to other pools of participants [46]. Participants were offered an incentive of US$0.50 (fifty cents) upon completion of the survey and were given 30 min to submit their responses. At first, the online survey presented questions about mobile privacy concerns, followed by questions about the Internet and social media usage of participants before and during the pandemic as well as the current use of contact tracing applications. Then, items regarding government intrusion concerns were presented, followed by items about perceived need of surveillance, trust in the government, acceptance of government surveillance and privacy protection behaviours. Lastly, demographic questions (i.e., age, gender, education) were presented to participants. At the time of the data collection, there was only one tool approved by the US government called the “the COVID screening tool”, which was available on the 27th of March. Developed by Apple, the tool is a web and mobile application allowing users to check their symptoms and potential exposure to COVID-19, while it provides recommendation on next steps, such as self-isolation, getting tested, or contacting a medical provider [47]. The pandemic reached the US around mid-March 2020 and by the time of the study, almost two million cases and 110 thousand deaths were recorded [48].

The measurement items for the constructs were adopted from existing research and adapted in the context of COVID-19 pandemic. An overview of all items used in this research is provided in Appendix B (Table B1). All items in the survey were measured on a 5-point Likert-type scale. Demographic questions (i.e., gender, age, and education) and those pertaining participants’ Internet and social media usage frequency before and during the pandemic were included.
4. Empirical analysis

This research applied partial least squares (PLS) for data analysis, using SmartPLS 3 software. Following the recommendations of [52], PLS was selected for this study because the proposed theoretical model has not been tested empirically before in the context of COVID-19 pandemic and the complex theoretical model includes many constructs, indicators, and relationships. Following the two-stage approach suggested by [52], the measurement model assessment was conducted first, followed by the structural model evaluation.

4.1. Sample characteristics

The data collection resulted in 407 responses. However, after cleaning the data (i.e., removal of incomplete responses and those indicating loss of attention), the usable sample was N = 380. According to Ref. [49], the estimation of the adequate sample size for a study using PLS can be performed by multiplying the maximum number of indicators per construct by 10. In our study, this estimate results in 370, thus the sample size of N = 380 can be deemed sufficient. Also, according to Ref. [50]; at a significance level of 1%, minimum R² = 0.50, and maximum number of arrows pointing at a construct being 4, the recommended sample size is 58. As a result, the sample size for this study can be considered sufficient.

More men participated in the survey (67.4%), most participants are between the ages of 26–35 (42.6%) and with a higher education background achieving a Bachelors’ degree (63.4%) (see Table 1).

Most participants are ‘heavy’ Internet users who use the Internet several times a day (55.8%). During COVID-19 outbreak almost 61% of the participants reported an increase in such use. Moreover, almost 75% can be characterised as ‘socially and digitally connected’ as they are using social media applications once or more every day. Furthermore, results suggest that during the lockdown measures the use of social media changed [51], as 62% of participants reported an increase in their use (see Figs. 1–2). Overall, evidence suggests that the COVID-19 crisis, which led governments to implement strict lockdown measures, resulted in a substantial increase in online activities and social networking of users.

Furthermore, few participants (28%) are using contact tracing applications, most of them being rolled out by governments (15%). It should be noted that in the subject country of the study (i.e., USA), the use of contact tracing applications is currently voluntary. Almost 36% of participants consider the likelihood of using such an application in the near future (see Figs. 3–4).

4.2. Common method bias

Several tests were conducted to evaluate the extent of common method bias (CMB) in the results of the analysis. All tests are presented in Appendix C. Results showed that common method bias does not pose a major concern in this study; however, we decided to continue the analysis with the retention of the marker variable in order to support the robustness and validity of our results.

4.3. Exploratory factor analysis

Before testing the hypotheses, exploratory factor analysis was performed using Maximum Likelihood extraction with Varimax rotation to examine the construct and factorial validity of the adapted measurement items for acceptance of surveillance, government intrusion concerns, and privacy protection behaviour. Results show values of 0.927, 0.898 and 0.968 for the Kaiser-Meyer Olkin measure of sampling adequacy test, respectively. The Bartlett’s test of sphericity was significant (p < 0.001) for all three constructs. These indicate that the data is suitable for factor analysis. One factor per variable was extracted as expected and all items loaded strongly on the construct that were purported to measure, with factor loadings higher than 0.5.

4.4. Measurement model evaluation

Factor loadings were first checked to ensure that all are above 0.708 as recommended by existing literature (see Table B1 in Appendix B) [52]. Next, composite reliability (CR) as well as reliability of measurement items in the model were examined, followed by examination of convergent validity and discriminant validity. As presented on Table 2, CR values, and Cronbach α values for all constructs are above 0.7, signifying satisfactory levels of reliability [52]. Average variance extracted (AVE) values for each variable exceeded 0.50, confirming that all variables explain at least 50% of the variance in the items, thus showing good convergent validity. Regarding discriminant validity, heterotrait-monotrait ratio (HTMT) of correlations was performed as suggested by [52]; all values fall below 0.90, confirming discriminant validity (see Table 3).

4.5. Structural model analysis

The analysis proceeds by evaluating the structural model and testing the proposed hypotheses. Following the guideline of [52], the assessment criteria to use to evaluate the structural model include the coefficient determination R², the blindfolding measure Q², and the statistical significance of the path coefficients. The R² value refers to the ability of the model to explain the endogenous variable demonstrating the model’s explanatory power. For the privacy protection behaviour variable R² is close to 0.60, thus signifying that the model can substantially explains this behavioural outcome. Regarding the blindfolding procedure, there are three levels of predictive accuracy that a model can achieve, with Q² values > 0 signifying small, >0.25 medium, and >0.50 large effects [52]. Results revealed that Q² is close to 0.32, showing that the model is very relevant in predicting the privacy protection behaviour of individuals during COVID-19 pandemic (see Table 4).

Hypotheses testing results along with the significant paths of the proposed model are presented in Table 5 and Fig. 5, H3, H4, and H6 were supported, while H1, H2, H5, and H7 were rejected.

4.6. Multigroup analysis

4.6.1. Gender

A multi group analysis was conducted in order to evaluate the model between the two groups of gender (male/female). Results showed that there are no differences between the two groups for hypotheses H1-H6, however there are significant differences (t = 2.89, p < 0.05) for H7; the relationship between acceptance of surveillance and privacy protection behaviours is stronger for men (b = 0.689, p < 0.001) than women (b = 0.452 p < 0.001).

Table 1
Demographic profile of participants (N = 380).

| Items      | Percentage (%) |
|------------|----------------|
| Gender     |                |
| Male       | 67.4           |
| Female     | 32.4           |
| Other      | 0.3            |
| Age        |                |
| <25 years  | 8.7            |
| 26–35      | 42.6           |
| 36–45      | 24.5           |
| 46–55      | 16.1           |
| 56–65      | 6.6            |
| Over 65    | 1.6            |
| Education  |                |
| High School| 13.2           |
| BSc        | 63.4           |
| MSc        | 20.3           |
| PhD        | 2.9            |
| Other      | 0.3            |
4.6.2. Contact trace app use

Additionally, a multigroup analysis was performed to assess the model between the groups of people who stated that they use contact tracing applications at the time of the survey and those who do not. Results showed that there are significant differences between the two groups only for H7 and H2; acceptance of government surveillance significantly and positively affected privacy protection behaviours for the group that does not use contact tracing applications \( (b = 0.577, p < 0.001) \) stronger than the group that has adopted such apps already \( (b = 0.224, p > 0.05) \). Regarding H2, results showed that the effect of government intrusion concerns was stronger on acceptance of government surveillance for the group that uses contact tracing applications \( (b = 0.279, p > 0.05) \) than the group who has not adopted such apps yet \( (b = -0.093, p > 0.05) \). Overall, in applying and testing the model between genders (male 67.4%, female 32.4%) and people who use (27.6%) and do not use (72.4%) contact tracing applications, we establish the validity of our findings and conclusions.

4.6.3. Internet usage

A multigroup analysis was conducted to evaluate the model comparing between two groups: ‘heavy’ Internet users (i.e., people reporting higher frequency of Internet usage) and ‘non-heavy’ Internet users. Results suggest that there are no significant differences between the two groups for all proposed hypotheses, except H1. Privacy concerns showed a significantly stronger effect on acceptance of government surveillance for the group reporting lower Internet usage frequency \( (b = 0.330, p > 0.05) \) than the other group \( (b = -0.038, p > 0.05) \).
Table 2
Descriptive statistics, Reliability and Validity.

| Construct | Mean | Std. Deviation | Cronbach’s Alpha | Composite Reliability | Average Variance Extracted (AVE) |
|-----------|------|----------------|------------------|------------------------|---------------------------------|
| ACC       | 3.35 | 1.00           | 0.941            | 0.940                  | 0.615                           |
| GIC       | 3.82 | 0.83           | 0.916            | 0.916                  | 0.609                           |
| MPC       | 3.14 | 1.16           | 0.917            | 0.916                  | 0.578                           |
| PNG       | 3.86 | 0.78           | 0.945            | 0.945                  | 0.742                           |
| PPB       | 3.13 | 1.07           | 0.964            | 0.964                  | 0.658                           |
| TRS       | 3.36 | 1.08           | 0.858            | 0.860                  | 0.673                           |

Table 3
Heterotrait-Monotrait (HTMT) ratio.

|         | ACC | GIC | MPC | PNG | PPB | TRS |
|---------|-----|-----|-----|-----|-----|-----|
| GIC     | 0.066 |    |     |     |     |     |
| MPC     | 0.066 | 0.853 |     |     |     |     |
| PNG     | 0.835 | 0.102 | 0.073 |     |     |     |
| PPB     | 0.610 | 0.411 | 0.295 | 0.709 |     |     |
| TRS     | 0.817 | 0.079 | 0.060 | 0.813 | 0.639 |     |

Table 4
Coefficient determination ($R^2$) and Blindfolding measure $Q^2$.

|         | $R^2$ | $Q^2$ |
|---------|-------|-------|
| ACC     | 0.706 | 0.426 |
| PPB     | 0.593 | 0.378 |

Table 5
Results of hypotheses testing.

| Path coefficients | t-statistics | P Values | Result |
|-------------------|--------------|----------|--------|
| H1: MPC $\rightarrow$ ACC (−) | −0.001 | 0.111 | NS | Reject |
| H2: GIC $\rightarrow$ ACC (−) | −0.111 | 1.830 | NS | Reject |
| H3: PNG $\rightarrow$ ACC (+) | 0.472 | 5.995 | *** | Accept |
| H4: TRS $\rightarrow$ ACC (+) | 0.233 | 4.740 | *** | Accept |
| H5: MPC $\rightarrow$ PPB (−) | −0.044 | 0.763 | NS | Reject |
| H6: GIC $\rightarrow$ PPB (−) | 0.303 | 4.867 | *** | Accept |
| H7: ACC $\rightarrow$ PPB (−) | 0.347 | 6.152 | *** | Reject |

***p < 0.001, **p < 0.01, NS not significant.
5. Discussion and implications

This study investigates individual attitudes towards privacy and surveillance as well as privacy protection behaviour during the COVID-19 pandemic by empirically testing the theoretical model with participants residing in the US. With the deployment of digital surveillance tools during the current COVID-19 pandemic, individual privacy concerns have become an emerging research topic. However, most studies conducted to date are dominated by theoretical evaluations and opinion papers, hence lacking in empirical evidence. This study contributes and provides empirical support to explain people’s attitudes toward privacy and surveillance during the COVID-19 pandemic by developing and validating a theoretical model to explain the antecedents of acceptance of surveillance and its impact on privacy protection behaviours. Our results highlight the important role of concerns for government intrusion in predicting privacy protection behaviours during the pandemic and demonstrate that perceived need for surveillance and trusting beliefs are antecedents of acceptance of government surveillance. Finally, this study showcases the importance of investigating privacy and surveillance attitudes during a health crisis (i.e., the COVID-19 pandemic).

In comparing our results with previous studies focusing on the general contexts [27], our study shows that trust has a stronger impact on surveillance attitudes during a health crisis (i.e., the COVID-19 pandemic). In previous studies, the importance of investigating privacy and surveillance attitudes during a health crisis has been demonstrated, with trust being a significant predictor in predicting privacy protection behaviours during the pandemic. Moreover, the relationship between those concerns and surveillance acceptability might be moderated by other factors, such as perceived benefits. Grounded on the notion of the privacy calculus, participants might be willing to trade off their privacy in exchange for certain benefits (e.g., health, security). During major security incidents in the past (e.g., 9/11 attacks), people reported willing to accept the trade-offs between privacy and their civil liberties to gain greater safety and security [32]. This demonstrates that one’s willingness to exchange those liberties with security increases as the perceived threat for an attack increases [32]. In the context of COVID-19 pandemic, scholars have highlighted that it is still largely unknown whether people are more

5.1. Theoretical implications

Our findings reveal that participants are concerned about individual online privacy as well as about government surveillance and monitoring of online activities and transactions during the pandemic. Participants are moderately concerned about the collection and use of their personal information from mobile applications (M = 3.86) and government surveillance of online activities (M = 3.82). This study contributes to privacy and surveillance literature as well as COVID-19 research by providing empirical evidence on the significant role of concerns over government intrusion on acceptance of surveillance and privacy protection behaviours during the COVID-19 pandemic. This study empirically demonstrates that the exploitation of people’s data by commercial firms is not the only privacy threat, as people are also concerned about government surveillance practices posing a risk to individual privacy [20], leading to changes in their privacy behaviours, including reducing the amount of personal information they share online, changing smartphone privacy settings, and reducing the use of mobile apps requiring location-based services.

However, this study found no evidence indicating a link between concerns for privacy and government intrusion and acceptance of government surveillance (H1 & H2). Previous research has reported mixed empirical results on the relationships between these constructs [27, 29]. One explanation can be that participants might not associate the collection of their personal information via mobile applications and government authorities during COVID-19 pandemic with the concept of state surveillance. Although the media increasingly cover topics around technologies being used for health surveillance purposes, it might be that participants are not aware of or associate other measures implemented during the health crisis, such as data mining and machine learning algorithms applied on social media posts and search engine terms, with the idea of being monitored or ‘watched’ by the government.

Moreover, the relationship between those concerns and surveillance acceptability might be moderated by other factors, such as perceived benefits. Grounded on the notion of the privacy calculus, participants might be willing to trade off their privacy in exchange for certain benefits (e.g., health, security). During major security incidents in the past (e.g., 9/11 attacks), people reported willing to accept the trade-offs between privacy and their civil liberties to gain greater safety and security [32]. This demonstrates that one’s willingness to exchange those liberties with security increases as the perceived threat for an attack increases [32]. In the context of COVID-19 pandemic, scholars have highlighted that it is still largely unknown whether people are more
likely to use epidemiological tools (e.g., contact trace) that prioritise privacy considerations (e.g., de-identification of data) as people might be more likely to share their personal data when it is for public health benefit [53]. Future research is essential to conduct empirical investigations to better understand how people balance and weigh the trade-offs between personal privacy and public safety during a health crisis context and to evaluate the efficacy and likelihood of the use of technological solutions that aim to enhance public safety in light of varying levels of privacy concerns.

Furthermore, personality characteristics and individual tendencies might also influence the association of intrusion concerns and acceptance of government surveillance. Recently [54], examined the impact of prosocial responsibility, a state of high awareness that one’s behaviour has consequences for others related to their well-being, on the acceptance of government digital surveillance for the sake of public health using participants in the US. They revealed that out of concern for others, people are willing to sacrifice their own privacy, accepting a loss in their individual privacy rights, while also identifying prosocial responsibility as an important predictor of acceptance of surveillance. Overall, there is a need for further exploration of the association between government intrusion concerns and surveillance acceptability. Future research should examine the impact of other confounding variables, such as personality characteristics, cultural differences and beliefs, on privacy and intrusion concerns as well as acceptability of surveillance.

This study contributes to privacy and surveillance literature by identifying government intrusion concerns as a major predictor of individual privacy protection behaviour during the pandemic, which has not been evaluated before (H6). Perceptions of intrusion have been linked to behaviour modifications [55]. In a study focusing on privacy behaviours in the pre and post Snowden era [40], found that users demonstrated increased interest in privacy protection after the incident and adopted privacy enhancing technologies. Our findings suggest that participants are worried that their online activities are monitored, and personal information gathered by authorities for better management of COVID-19 pandemic, and also adopt stronger actions to protect their privacy, such as changing privacy settings or turning location tracking off on their mobile phone.

However, we found no evidence that mobile privacy concerns result in enhanced privacy protection behaviour (H5). While participants reported worried about their privacy and personal data collection from mobile applications during the pandemic, these concerns did not result in risk reduction actions to protect their personal information. In this study, we expected that due to the attention given by the media and privacy advocates about individual privacy and privacy rights, individuals would be more concerned during the COVID-19 pandemic about the collection of their personal data by providers and applications, which would result in them adopting privacy protection behaviours. These findings come in accordance with past research showing that privacy concerns do not always contribute to the formation of privacy protection behaviours [27]. One explanation can be that although participants are concerned about their privacy, they consider it a price they have to pay in order to interact with online providers (i.e., mobile applications). The adoption of a protection behaviour, such as refusal to disclose personal information during the interaction with providers, will not prove to be of value but rather hinder the whole interaction process. Another explanation could be that participants trust that have implemented additional privacy settings on their mobile phone, hence they will be sufficiently protected even as the collection of information intensifies during the pandemic. Future research should explore the prevalence of this practice to better understand the relationship between mobile privacy concerns and privacy protection behaviour.

Moreover, our findings confirm that the level of trust in the government (H4) as well as beliefs that the government needs greater access to peoples’ personal information and transactions to manage and contain the COVID-19 pandemic (H3) can increase one’s likelihood to accept such government surveillance with the latter showing the strongest path towards acceptance of surveillance. Our findings come in agreement with previous studies indicating that people who believe in the political institutions and the necessity of government surveillance in order to protect citizens’ health and welfare are more accepting of government surveillance [27,28,34]. Thus, our results add to the limited base of existing privacy and surveillance literature by identifying and empirically confirming trust and perceived need for surveillance as important antecedents of acceptance of government surveillance during the COVID-19 pandemic.

Contrary to our expectations, acceptance of government surveillance was found to positively impact privacy protection behaviours during the COVID-19 pandemic (H7). One possible explanation for the observed positive effect could be that participants who have higher privacy and intrusion thresholds are accepting the surveillance monitoring practices employed by the government as a “necessary evil” towards fighting the global health crisis, while still feeling the need to protect their personal information from high scrutiny, thus resorting in privacy protection behaviours. People may accept government surveillance as an essential measure that needs to be implemented for others, but not for them personally. Scholars have argued that people can accept government surveillance even if they are aware that their civil liberties (i.e. privacy) are threatened [11,56]. Evidence from a survey conducted two years after Edward Snowden’s revelations showed that 87% people who are aware of the existence of government surveillance programs have changed their technology usage such as the way they use their email or search engines [57]. As a result, during the COVID-19 pandemic it might be that people who are aware of the current epidemiological surveillance are accepting it as a necessary means to help states overcome the current health crisis, while also feeling the need to protect themselves and their individual privacy by adopting risk reduction strategies. Future research is essential to confirm the nature of the relationship between acceptance of government surveillance and privacy protection behaviour as well as whether such relationship still exists in other contexts (e.g., monitoring the phenomenon during a crisis event vs daily life). Also, it would be important for future research to explore the thought and decision-making process of individuals during the trade-off between personal privacy and public health in crisis events as well as factors that may encourage or hinder such decisions.

5.2. Practical implications

The findings from this study offer important practical implications. First, our findings inform and bring awareness to governments and policymakers as well as health organisations and private companies working towards managing the COVID-19 pandemic about the public’s concerns about privacy, intrusion, and acceptance of surveillance during the current health crisis. Participants are concerned about the collection and use of their personal information by mobile applications as well as with the monitoring of their online activities by governments. These concerns result in privacy protection behaviours, such as turning off location tracking or sharing less information online or even leaving their smartphone at home in fear of tracking location and data, that may hinder the potential effectiveness of digital technologies and epidemiological tools aiming to manage as well as contain the virus outbreaks. For example, in the case of contact tracing applications that largely depend on people’s adoption rate, such applications will prove to be of significant value if most citizens are using them. Such participation is currently on a voluntary basis in the context of the subject country in this study, US. The same applies to other mobile applications and wearable devices apart from contact tracing (i.e., to inform people who have been exposed to someone infected), such as those deployed to monitor compliance with quarantine measures (e.g. self-isolation after exposure to the virus) and to assess the extent of virus outbreaks (e.g., people being asked to report their symptoms and the severity) in different regions (e.g. smaller cities) or different contexts (e.g. schools
and universities). For example, in Taiwan people who are required to self-isolate are provided a government mobile device by GPS to identify any breaches in the quarantine of the individual. Although adoption is not voluntary in this example, privacy concerns regarding such solutions can result in bypassing behaviours, such as leaving the phone at home. Overall, in order to increase the adoption of voluntary applications and ultimately boost the effectiveness of all relevant technologies, certain issues need to be considered and solutions to be found. Sincere consideration of user privacy during the design, development, and deployment of such solutions is crucial. Users’ consent should be requested upfront, delineating the precise types of personal information that will be collected and used, as well as the period of data storage and what happens to the data after that period. Also, the deployment of privacy preserving and enhancing technologies as well as de-identification technologies on personal information collected from users, before being stored and handled by health authorities, can potentially ease concerns over privacy and intrusion.

Furthermore, our results signify the importance of enhancing political trust as well as the belief that governments’ need to be proactive in protecting peoples’ welfare during a crisis. These beliefs can substantially increase people’s acceptance of government surveillance. One potential way is to develop solutions following the guidelines of existing strong legislative frameworks, such as the General Data Protection Regulation (GDPR), thus reassuring the public that their individual rights to privacy and data protection are being safeguarded. Although it has been noted that during emergency situations, such as the current public health crisis, such regulations can be suspended, it is crucial that governments communicate in a clear and transparent way any changes to existing legislation, thus cultivating public trust and easing worries or fear about individual privacy. Furthermore, the effective communication and explanation of the public benefits accompanying the implementation and use of such digital epidemiological solutions can strengthen the positive beliefs about the need of surveillance. These include contributing to the prediction of future disease outbreaks, controlling or reducing current infections and local outbreaks, allowing economies to restart and societies to recover from the unprecedented costs.

6. Conclusion, limitations, and future research

Digital technologies have been heavily deployed during the COVID-19 health crisis to help governments and health authorities to better understand the spread and fight the virus, as well as to manage and contain the pandemic. However, such technological implementations brought forward concerns about individual privacy as well as concerns about government surveillance of people’s activities. The present study explores individual attitudes towards privacy and surveillance during the COVID-19 pandemic by developing a theoretical model grounded in previous IS research to explain the relationship between concerns for privacy and surveillance, acceptance of surveillance, and privacy protection behaviours. By identifying the antecedents of acceptance of government surveillance and its impact on privacy protection behaviour, this study addresses important gaps in existing privacy, surveillance, and COVID-19 research and offers recommendations to policymakers and public health organisations on the implementation of technologies to manage health crises. It can be suggested that the technological implementation for the management of health crises will only be effective if certain considerations and actions towards respecting individual privacy are also undertaken.

As with all empirical research, this study has several limitations. First, this study was conducted as a cross-sectional study; future research should employ a longitudinal approach to compare privacy protection behaviours at different times during the pandemic, measuring changes in privacy concerns and the resulting behaviours. Moreover, this study focuses more on characteristics that relate to technological skills and experience of participants (i.e., Internet and social media usage), while health-related characteristics, such as participants belonging in a ‘low’ or ‘high’ risk groups, or skills and knowledge about privacy issues (e.g., privacy literacy) have not been captured. It is important for future research to examine whether such factors may have an impact on privacy protection behaviours of participants as well as the potential differences in the application of the proposed theoretical model between these groups. Also, this study recruited a sample of N = 380 of participants from the US, which is considered as a sufficient sample size for this investigation. However, future research should strive to recruit a larger sample to achieve replication and generalisation of our results. Furthermore, the sample in this study leans towards relatively younger age groups (under 55 years old). Thus, it is important for future research to examine privacy and surveillance attitudes of older generations, such as those above 65 years old, which might yield different results. Also, this study collected data from participants residing in one country (i.e., US); future studies should aim to replicate our results in different countries, comparing between nations (e.g., China vs European countries), areas of residence (e.g., big cities and small towns), cultures (e.g., Western vs Asian), and political beliefs (e.g., democratic vs authoritative states) to gauge the possibility of differential results. Furthermore, future studies should examine other factors that might influence acceptance of government surveillance, such as social norms, culture, and legal frameworks as antecedents and/or moderating contextual variables. Digital surveillance solutions that have been implemented effectively in some countries might not be accepted by citizens in other countries. For example, in the US, the HIPAA privacy rule prevents public disclosure of patients’ health information (a practice that has been implemented in South Korea). However, during emergency situations such frameworks can be suspended. In Europe, the legal privacy framework of GDPR prohibits the collection and use of users’ personal identifiable information, such as biometrics; however, in other countries such regulations might not exist. Lastly, as existing empirical privacy research focusing on COVID-19 pandemic is still very limited, it would be important for future research to conduct qualitative studies to examine in more depth the specific aspects of privacy and surveillance concerns, the relationship of government intrusion concerns and surveillance, as well as the extent of potential trade-offs that people are willing to accept in exchange for health benefits.

Acknowledgement

This work was part of the PRIvacy-aware personal data management and Value Enhancement for Leisure Travellers (PriVELT) Project, funded by the UK’s Engineering and Physical Sciences Research Council (EPSRC) under grant number EP/R033196/1.
### Appendix

#### A. Relevant Literature

| Table A1 | Summary of relevant literature on privacy and surveillance |
|----------|----------------------------------------------------------|
| **Author** | **Findings** | **Methodology** | **Focus** |
| **COVID-19 Context** |  |  |  |
| [23] | The paper discusses about the responses to the pandemic having increased concerns about the control of one’s data and privacy. | Theoretical | Privacy in COVID-19 |
| [22] | The paper discusses about responsible data collection from the public during COVID-19, as privacy and public trust should be respected and preserved. | Theoretical | Privacy in COVID-19 |
| [60] | Disease surveillance and surveillance perspectives for the COVID-19 pandemic. | Theoretical | Surveillance in COVID-19 |
| J [3]. | The paper conducts a short review of the flaws and challenges related to Bluetooth contact tracing applications. | Theoretical | Contact tracing apps COVID-19 |
| [38] | People in the US report reluctant to install contact tracing applications as well as support the implementation of other surveillance measures (e.g., thermal cameras). | Empirical – Frequency analysis | Acceptance of surveillance measures in COVID-19 |
| [31] | A survey with US participants showed that 80% of them are willing to install contact tracing applications that are perfectly privacy and accurate. | Empirical - Frequency analysis | Acceptance of COVID-19 Contact Tracing apps |
| [28] | Public surveillance attitudes during COVID-19 vary among countries (UK, US, Germany, France, Italy). Trust in the government is an important determinant of acceptability of contact tracing applications. | Empirical – testing effects on outcome variables | Acceptance of Contact Tracing apps in COVID-19, Cross cultural |
| [29] | Investigating the acceptance of corona applications, including contact tracing apps, symptom checks, quarantine enforcement and health information across three countries (Germany, US and China). US public reported less willing to use corona applications than Chinese citizens. Moreover, when asked about the negative aspects of corona apps, participants from all countries expressed concerns about privacy, while US participants reported more worried about government surveillance. | Empirical – testing effects on outcome variables | Acceptance of digital surveillance measures in COVID-19 - Cross cultural |
| [34] | Trust in the government is positively associated with acceptability of contact tracing applications in France. | Empirical - testing effects on outcome variables | Acceptance of COVID-19 Contact Tracing apps |
| [53] | Discussion about the design, utility, risks, and benefits of the implementation of contact tracing applications. | Theoretical | Acceptance of COVID-19 Contact Tracing apps |
| [58] | Discussion of South Korea’s epidemiological approach responding to the COVID-19 pandemic. | Theoretical | Privacy and use of personal data |
| [59] | Understanding the privacy risks associated with the publishing of contact trace data of infected people in South Korea. Results reveal that inferences on one’s personal sensitive information are possible when contact trace data is public. | Empirical - testing effects on outcome variables | Privacy and use of personal data |
| [60] | Development of a symptom tracking system that considers user privacy issues. | Empirical – beta testing of symptom tracking application | Privacy concerns and personal data |
| **General Context** |  |  |  |
| [24] | The paper investigates big five cities. Results show that People in Seoul expressed the most negative attitudes towards surveillance, while people in Bangalore the most positive ones. | Empirical – Frequency analysis | Generic Surveillance concerns Cross cultural |
| [9] | Comparing Italy and the US, US users showed more accepting attitudes towards government surveillance, while Italian users had lower tolerance on privacy intrusion and found such practices an inhibiting factor to performing online activities. | Empirical – Theoretical model - testing effects on outcome variables | Generic Surveillance concerns Cross cultural |
| [25] | In Croatia, older people show less trust in governmental institutions, resulting in enhanced privacy protection behaviours. | Empirical – Cluster analysis | Generic Surveillance concerns |
| [10] | Privacy concerns and surveillance attitudes are important predictors of one’s intention to make online transactions with e-commerce providers. People worrying about their online activities being monitored by authorities are more reluctant to share personal information online. | Empirical - testing effects on outcome variables | Antecedents of government intrusion and privacy concerns, behaviours |
| [26] | The exposure to news stories relevant to government surveillance can contribute to higher concerns over (government) intrusion and the use of weaker passwords to protect user personal information. | Empirical - Theoretical model - testing effects on outcome variables | Antecedents of government intrusion and privacy concerns, behaviours |
| [27] | People who are more accepting of surveillance measures tend to show less privacy protection behaviours. People who tend to accept government monitoring are less likely to deploy privacy protections. | Empirical - Theoretical model - testing effects on outcome variables | Antecedents of government intrusion and privacy concerns, behaviours |
| [11] | Surveillance concerns, regulatory needs, and perceived transparency constitute the main determinants of individual’s acceptance of government surveillance. | Empirical - Theoretical model - testing effects on outcome variables | Antecedents of government intrusion and privacy concerns, behaviours |
| [32] | After major incidents (e.g., 9/11 attacks), people demonstrated more trusting attitudes towards the government were more willing to trade-off civil liberties (e.g., privacy) to gain greater protection and security. | Empirical - testing effects on outcome variables | Trust in the government |
| [33] | People who are more trusting towards governments express more positive beliefs about surveillance-oriented security technologies. | Empirical - Theoretical model - testing effects on outcome variables | Trust in the government |
| [8] | Higher levels of citizens’ political trust can encourage the support of surveillance measures used by governments. | Empirical - testing effects on outcome variables | Trust in the government |
| [39] | The aftermath of privacy security events, people experienced increased levels of anxiety and worry about the potential negative consequences that might occur. | Report from Pew Research Center – Frequency analysis | Privacy Protection Behaviour |
| [40] | In the post-Snowden era, evidence indicates a surge in information seeking and browsing behaviours regarding privacy related topics as well as adoption of privacy enhancing technologies. | Empirical – Frequency analysis | Privacy Protection Behaviour |
| [41] | People with higher privacy concerns are more likely to adopt risk reduction behaviours. | Empirical - Theoretical model - testing effects on outcome variables | Privacy Protection Behaviour |
### B. Measurement Items

**Table B1**

| Construct                                | Item                                                                 | Question                                                                 | Loading |
|-------------------------------------------|----------------------------------------------------------------------|--------------------------------------------------------------------------|---------|
| **Acceptance of surveillance [8,57]**     | ACC1                                                                | A: Introducing biometric passports and biometric identity cards containing a digital face image and fingerprints. | 0.755   |
|                                           | ACC2                                                                | B: The establishment of a database to which authorities have access. Information in this database includes name, address, prior health history. | 0.799   |
|                                           | ACC3                                                                | C: Granting authorities access to track real time position of citizens.  | 0.889   |
|                                           | ACC4                                                                | D: Retention of data about telephone calls, emails, and websites visited by telecom providers for a period of 6 months. | 0.887   |
|                                           | ACC5                                                                | E: Granting authorities access to personal information, through third party mobile applications, such as daily body temperature, movements/activities/steps. | 0.898   |
|                                           | ACC6                                                                | F: Gathering of air and ship passenger data to the government authorities. Information includes name, gender, nationality, and detailed information on travel movements of all passengers. | 0.740   |
|                                           | ACC7                                                                | G: Granting authorities access to track recent contacts and others located in close proximity at any given time. | 0.862   |
|                                           | ACC10                                                               | I find it acceptable for the government to use people’s cellphones to track the location of people to ensure they are complying with experts' advice on limiting social contact during the Covid-19 outbreak. | 0.726   |
|                                           | ACC8                                                                | I find it acceptable for the government to use people’s cellphones to track the location of people who have tested positive for Covid-19 in order to understand how the virus is spreading. | 0.579   |
|                                           | ACC9                                                                | I find it acceptable for the government to use people’s cellphones to track the location of people who may have had contact with someone who tested positive for Covid-19. | 0.634   |
| **Government Intrusion Concerns** [10] [57] [11] | GIC1                                                              | I am concerned about the power the government has to monitor online activities | 0.804   |
|                                           | GIC2                                                                | I am concerned that my online accounts and information (e.g., e-mails, shopping records, tracking my Internet surfing, etc.) will be more open to government scrutiny | 0.791   |
|                                           | GIC3                                                                | I am concerned about the government’s ability to monitor online activities | 0.770   |
|                                           | GIC4                                                                | I am concerned that the government will use surveillance powers to investigate citizens | 0.751   |
|                                           | GIC5                                                                | I am concerned that the government is collecting too much information about me | 0.835   |
|                                           | GIC6                                                                | I am concerned that the government is monitoring my online activity (e.g., search engines, cell phone, email messages and mobile smartphone applications) | 0.765   |
|                                           | GIC7                                                                | I am afraid to share my personal information with government authorities | 0.744   |
| **Mobile Privacy Concerns** [70]          | MPC1                                                                | I am concerned that mobile device apps are collecting too much information about me. | 0.845   |
|                                           | MPC2                                                                | I am concerned that mobile device apps may monitor my activities on my mobile device. | 0.827   |
|                                           | MPC3                                                                | I feel that as a result of my using mobile device apps, others know about me more than I am comfortable with. | 0.827   |
|                                           | MPC4                                                                | I believe that as a result of my using mobile device apps, information about me that I consider private is now more readily available to others than I would want. | 0.708   |
|                                           | MPC5                                                                | I feel that as a result of my using mobile device apps, information about me is out there that, if used, will invade my privacy. | 0.760   |
|                                           | MPC6                                                                | I am concerned that apps may use my personal information for other purposes without notifying me or getting my authorization. | 0.703   |
|                                           | MPC7                                                                | When I give personal information to use mobile device apps, I am concerned that apps may use my information for unintended purposes. | 0.707   |
|                                           | MPC8                                                                | I am concerned that mobile device apps may share my personal information with other entities without getting my authorization. | 0.688   |
| **Perceived Need for Government Surveillance [10]** | PNG1                                                              | the government needs to have greater access to personal information ... | 0.864   |
|                                           | PNG2                                                                | the government needs to have greater access to individual credit card transactions and records ... | 0.880   |
|                                           | PNG3                                                                | the government needs to have greater access to individual real time positions and physical movement ... | 0.822   |
|                                           | PNG4                                                                | the government needs to have greater access to individual health information ... | 0.844   |
|                                           | PNG5                                                                | the government needs broader monitoring authority ... | 0.868   |
|                                           | PNG6                                                                | the government needs to have more authority to use high tech surveillance tools for Internet monitoring ... | 0.888   |
| **Privacy Protection Behaviour [57]**      | PPB1                                                                | Changed my privacy settings in social media. | 0.872   |
|                                           | PPB10                                                               | Changed the way I use my smartphone. | 0.858   |
|                                           | PPB11                                                               | Used anonymity software (e.g., VPN). | 0.593   |
|                                           | PPB12                                                               | Used a temporary username or email address. | 0.848   |
|                                           | PPB13                                                               | turned off location tracking feature on my smartphone. | 0.707   |
|                                           | PPB14                                                               | left my smartphone at home when I went outside. | 0.777   |
|                                           | PPB2                                                                | Reduced the use of technology for communication (e.g., video call, teleconferencing). | 0.910   |
|                                           | PPB3                                                                | Reduced the amount I use social media. | 0.835   |
|                                           | PPB4                                                                | Reduced the use of digital platforms for consumption (e.g., online shopping, delivery). | 0.870   |
|                                           | PPB5                                                                | Reduced the amount I use mobile apps requiring location-based services. | 0.793   |
|                                           | PPB6                                                                | Reduced the amount of personal information I share online. | 0.720   |
|                                           | PPB7                                                                | Changed privacy settings in my smartphone. | 0.813   |
|                                           | PPB8                                                                | Used a search engine that doesn’t keep track of a user’s search history. | 0.814   |
|                                           | PPB9                                                                | Changed the way I use my social media. | 0.883   |
| **Trust in government [8]**                | TRS1                                                                | The government | 0.901   |
|                                           | TRS2                                                                | The legal system | 0.788   |
|                                           | TRS3                                                                | The police | 0.765   |
C. Common Method Bias

According to Ref. [61], a full collinearity assessment test, by calculating the variance inflation factors (VIF) for every endogenous variable in the model, constitutes a comprehensive procedure and appropriate method to test for the existence of common method bias. VIF values equal or lower than 3.3 signify the absence of common method bias [61], while VIF values less than 5 are also acceptable [62]. Our results show that most VIF values are very close to the cut-off 3.3 threshold, while only three values exceed 4 and reach the cut-off threshold of 5 (Table C1). As a result, we further assessed common method bias in a second evaluation.

Table C1
Collinearity Assessment Method (VIF)

| Construct | VIF |
|-----------|-----|
| ACC       | 4.34 |
| GIC       | 3.85 |
| MPC       | 3.76 |
| PNG       | 4.27 |
| PPB       | 2.86 |
| TRS       | 3.67 |

We followed the procedures suggested by Refs. [63, 64] by adding a common latent factor in the PLS-model and comparing the standardised regression weights with and without the common latent factor (Table C2). Results showed that the average substantively explained variance is 64%, while all differences in regression weights, except one, are very small (less than 0.02) [65]. Thus, we can conclude that common method bias is not a major concern in our data.

Table C2
Comparison of standardised regression weights

| Construct | Indicator | Substantive Factor loading (R1) | R1² | Factor loading with CLF | Delta |
|-----------|-----------|---------------------------------|-----|-------------------------|-------|
| ACC       | ACC1      | 0.755                           | 0.570 | 0.759                   | −0.004|
| ACC2      | 0.799     | 0.638                           | 0.796 | 0.003                   |
| ACC3      | 0.889     | 0.790                           | 0.883 | 0.006                   |
| ACC4      | 0.887     | 0.787                           | 0.885 | 0.002                   |
| ACC5      | 0.888     | 0.806                           | 0.883 | 0.000                   |
| ACC6      | 0.740     | 0.548                           | 0.742 | −0.002                  |
| ACC7      | 0.862     | 0.743                           | 0.856 | 0.006                   |
| ACC8      | 0.579     | 0.335                           | 0.584 | −0.005                  |
| ACC9      | 0.634     | 0.402                           | 0.642 | −0.008                  |
| ACC10     | 0.726     | 0.527                           | 0.734 | −0.008                  |
| GIC       | GIC1      | 0.804                           | 0.646 | 0.785                   | 0.019 |
| GIC2      | 0.791     | 0.626                           | 0.803 | −0.012                  |
| GIC3      | 0.770     | 0.593                           | 0.774 | −0.004                  |
| GIC4      | 0.751     | 0.564                           | 0.732 | 0.019                   |
| GIC5      | 0.835     | 0.697                           | 0.833 | 0.000                   |
| GIC6      | 0.765     | 0.585                           | 0.768 | −0.003                  |
| GIC7      | 0.744     | 0.554                           | 0.764 | −0.020                  |
| MBC       | MB1       | 0.845                           | 0.714 | 0.835                   | 0.010 |
| MB2       | 0.827     | 0.684                           | 0.838 | −0.011                  |
| MB3       | 0.827     | 0.684                           | 0.844 | −0.017                  |
| MB4       | 0.708     | 0.501                           | 0.713 | −0.005                  |
| MB5       | 0.76      | 0.578                           | 0.765 | −0.005                  |
| MB6       | 0.703     | 0.494                           | 0.686 | 0.017                   |
| MB7       | 0.707     | 0.500                           | 0.693 | 0.014                   |
| MB8       | 0.688     | 0.473                           | 0.684 | 0.004                   |
| PNG       | PNG1      | 0.864                           | 0.746 | 0.861                   | 0.003 |
| PNG2      | 0.880     | 0.774                           | 0.881 | −0.001                  |
| PNG3      | 0.822     | 0.676                           | 0.822 | 0.000                   |
| PNG4      | 0.844     | 0.712                           | 0.843 | 0.001                   |
| PNG5      | 0.868     | 0.753                           | 0.87  | −0.002                  |
| PNG6      | 0.888     | 0.789                           | 0.89  | −0.002                  |
| PPB       | PPB1      | 0.872                           | 0.760 | 0.866                   | 0.006 |
| PPB2      | 0.910     | 0.828                           | 0.900 | 0.010                   |
| PPB3      | 0.835     | 0.697                           | 0.839 | −0.004                  |
| PPB4      | 0.870     | 0.757                           | 0.866 | 0.004                   |
| PPB5      | 0.793     | 0.629                           | 0.801 | −0.008                  |
| PPB6      | 0.720     | 0.518                           | 0.73  | −0.010                  |
| PPB7      | 0.813     | 0.661                           | 0.819 | −0.006                  |
| PPB8      | 0.814     | 0.663                           | 0.82  | −0.006                  |
| PPB9      | 0.883     | 0.780                           | 0.875 | 0.008                   |
| PPB10     | 0.858     | 0.736                           | 0.851 | 0.007                   |
| PPB11     | 0.593     | 0.352                           | 0.611 | −0.018                  |
| PPB12     | 0.848     | 0.719                           | 0.846 | 0.002                   |
| PPB13     | 0.707     | 0.500                           | 0.711 | −0.004                  |
| PPB14     | 0.777     | 0.664                           | 0.772 | 0.005                   |
We also followed the measured latent marker variable method (MLMV) and more specifically the construct level correction (CLC) in order to detect as well as correct common method bias [66]. According to Ref. [67]; the selection of the marker variable should be based on the premise that it does not relate theoretically with at least one the constructs included in the proposed model. As a result, in the present study the variable fashion consciousness, described as one’s interest in fashion as well as wearing latest fashionable clothing, was adopted from Ref. [68] as a marker variable, as an unrelated construct with the rest of the variables in the study. The path coefficients as well as t-values with and without the marker variable are compared as well as the R² values. Our results below (Tables C3–C4) show that there no significant changes in these parameters in most cases (less than 10%), however in one case the change is large enough to suggest the presence of CMV. As a result, we decided to continue the analysis with the retention of the marker variable in the model.

### Table C3
#### Construct Level Correction Analysis

| Relationship          | CLC estimation (Path coefficients) | Original PLS (Path coefficients) | CLC estimation t-value | Original Estimate t-value |
|-----------------------|------------------------------------|----------------------------------|------------------------|--------------------------|
| MPC -> ACC            | 0.001                              | 0.017                            | 0.011 NS               | 0.191 NS                 |
| GIC -> ACC            | -0.111                             | -0.084                           | 1.830 NS               | 0.913 NS                 |
| PNG -> ACC            | 0.472                              | 0.529                            | 5.995***               | 4.675***                 |
| TRS -> ACC            | 0.303                              | 0.395                            | 4.440***               | 3.327***                 |
| MPC -> PPB            | -0.044                             | -0.178                           | 0.763 NS               | 1.586 NS                 |
| GIC -> PPB            | 0.303                              | 0.575                            | 4.867***               | 4.959***                 |
| ACC -> PPB            | 0.347                              | 0.620                            | 6.152***               | 14.343***                |

Note: Critical values ** 1.96 (5% sig level) and *** 2.57 (1% sig level).

### Table C4
#### Comparison of R² values in CLC

| Endogenous Construct | CLC Estimation (R²) | Original PLS Estimate (R²) |
|----------------------|---------------------|-----------------------------|
| ACC                  | 0.706               | 0.694                       |
| PPB                  | 0.593               | 0.511                       |

### D. Discriminant Validity

#### Table D1
#### Fornell Larcker Criterion

| ACC | GIC | MBPC | PNG | PPB | TRS |
|-----|-----|------|-----|-----|-----|
| 0.784 | -0.011 | 0.781 | 0.019 | 0.856 | 0.761 |
| 0.643 | 0.483 | 0.440 | 0.511 | 0.689 |

#### Table D2
#### Cross loadings

| ACC | GIC | MBPC | PNG | PPB | TRS |
|-----|-----|------|-----|-----|-----|
| 0.755 | 0.006 | -0.001 | 0.617 | 0.464 | 0.647 |
| 0.643 | 0.689 | 0.440 | 0.511 | 0.734 |

(continued on next page)
Table D2 (continued)

| ACC   | GIC  | MBPC | PNG  | PPB  | TRS  |
|-------|------|------|------|------|------|
| GC1   | 0.19 | 0.75 | 0.07 | 0.19 | 0.06 |
| GC2   | 0.20 | 0.76 | 0.08 | 0.21 | 0.07 |
| GC3   | 0.21 | 0.77 | 0.09 | 0.22 | 0.08 |
| GC4   | 0.22 | 0.78 | 0.10 | 0.23 | 0.09 |
| GC5   | 0.23 | 0.79 | 0.11 | 0.24 | 0.10 |
| GC6   | 0.24 | 0.80 | 0.12 | 0.25 | 0.11 |
| GC7   | 0.25 | 0.81 | 0.13 | 0.26 | 0.12 |
| GC8   | 0.26 | 0.82 | 0.14 | 0.27 | 0.13 |
| GC9   | 0.27 | 0.83 | 0.15 | 0.28 | 0.14 |
| GC10  | 0.28 | 0.84 | 0.16 | 0.29 | 0.15 |
| GC11  | 0.29 | 0.85 | 0.17 | 0.30 | 0.16 |
| GC12  | 0.30 | 0.86 | 0.18 | 0.31 | 0.17 |
| GC13  | 0.31 | 0.87 | 0.19 | 0.32 | 0.18 |
| GC14  | 0.32 | 0.88 | 0.20 | 0.33 | 0.19 |
| GC15  | 0.33 | 0.89 | 0.21 | 0.34 | 0.20 |
| GC16  | 0.34 | 0.90 | 0.22 | 0.35 | 0.21 |
| GC17  | 0.35 | 0.91 | 0.23 | 0.36 | 0.22 |
| GC18  | 0.36 | 0.92 | 0.24 | 0.37 | 0.23 |
| GC19  | 0.37 | 0.93 | 0.25 | 0.38 | 0.24 |
| GC20  | 0.38 | 0.94 | 0.26 | 0.39 | 0.25 |
| GC21  | 0.39 | 0.95 | 0.27 | 0.40 | 0.26 |
| GC22  | 0.40 | 0.96 | 0.28 | 0.41 | 0.27 |
| GC23  | 0.41 | 0.97 | 0.29 | 0.42 | 0.28 |
| GC24  | 0.42 | 0.98 | 0.30 | 0.43 | 0.29 |
| GC25  | 0.43 | 0.99 | 0.31 | 0.44 | 0.30 |
| GC26  | 0.44 | 1.00 | 0.32 | 0.45 | 0.31 |

Credit author statement

Athina Ioannou: Conceptualization, Methodology, Investigation, Writing – original draft, Writing – review & editing, Iis Tussyadiah: Conceptualization, Methodology, Investigation, Writing – original draft, Writing – review & editing, Supervision, Project administration, Funding acquisition.

References

[1] Worldometer, Coronavirus Cases, Worldometer, 2020, https://doi.org/10.1101/2020.01.23.20018549v2.
[2] OECD, Using Artificial Intelligence to Help Combat COVID-19, 2020. http://www.oecd.org/coronavirus/policy-responses/using-artificial-intelligence-to-help-combat-covid-19-9aa4cf21.
[3] J. Li, X. Guo, COVID-19 Contact-Tracing Apps: A Survey on the Global Deployment and Challenges, 2020, pp. 1–7. ArXiv Preprint ArXiv:2005.03599, http://arxiv.org/abs/2005.03599.
[4] S. Whitelew, M.A. Mamas, E. Topol, H.G.C. Van Spall, Applications of digital technology in COVID-19 pandemic planning and response, in: The Lancet Digital Health, vol. 2, Elsevier Ltd, 2020, pp. e435–e440, https://doi.org/10.1016/S2589-7500(20)30142-4.
[5] M. Bates, Tracking disease: digital epidemiology offers new promise in predicting outbreaks, IEEE Pulse 8 (1) (2017) 18–22, https://doi.org/10.1109/MPUL.2016.2627238.
[6] R. Calvo, C. Deterding, R. Ryan, Health Surveillance during Covid-19 Pandemic: How to Safeguard Autonomy and Why It Matters, 2020, https://doi.org/10.1136/bmj.m1373, BMJ (Online).
[7] C.G. Redick, A.T. Chatfield, P.A. Jaramillo, Public opinion on National Security Agency surveillance programs: a multi-method approach, Govern. Inf. Q. 32 (2) (2015) 129–141, https://doi.org/10.1016/j.giq.2015.01.005.
[8] E.M. Trüding, L.C. Steckermeier, Trusting and controlling? Political trust, information and acceptance of surveillance policies: the case of Germany, Govern. Inf. Q. 34 (3) (2017) 421–433, https://doi.org/10.1016/j.giq.2017.07.003.
[9] T. Dinev, M. Belotto, P. Hart, C. Colautti, V. Russo, I. Serra, Internet users’ privacy concerns and attitudes towards government surveillance: An exploratory study of cross-cultural differences between Italy and the United States, in: 18th Bled EConference EIntegration in Action - Conference Proceedings, December, 2005.
[10] T. Dinev, P. Hart, M.R. Mullen, Internet privacy concerns and beliefs about government surveillance - an empirical investigation, J. Strat. Inf. Syst. 17 (3) (2008) 214–233, https://doi.org/10.1101/jis.2007.09.002.
[11] T. Nam, What determines the acceptance of government surveillance? Examining the influence of information privacy correlates, Soc. Sci. J. 56 (4) (2019) 530–544, https://doi.org/10.1111/jcom.12276.
[12] P.J. Ägerfalk, K. Conboy, M.D. Myers, Information systems in the age of pandemics – COVID-19 and beyond, Eur. J. Inf. Syst. (2020) 1–5, https://doi.org/10.1080/0960085X.2020.1771968, 00(00).
[13] D. Lyon, Surveillance Society, McGraw-Hill Education, 2001.
[14] D. Lyon, Surveillance after Snowden, 2015 (Cambridge).
[15] J. Bedford, D. Enria, J. Giesecke, D.L. Heymann, C. Ihekweazu, G. Kobinger, H. C. Lane, Z. Memish, M. don Oh, A.A. Sall, A. Schuchat, K. Unghchas, L.H. Wieler, COVID-19: towards controlling of a pandemic, Lancet 395 (10229) (2020) 1015–1018, https://doi.org/10.1016/S0140-6736(20)30673-5.
[16] H.J. Smith, T. Dinev, H. Xu, Information privacy research: an interdisciplinary review, MIS Q. 35 (4) (2011) 1063–1078, https://doi.org/10.2307/4149970.
[17] F. Belanger, R.E. Crossler, Privacy in the digital age: a review of information privacy research in information systems, MIS Q. 35 (4) (2011) 1071–1041, https://doi.org/10.2307/4149970.
[18] L. Barath, E. Secinti, Z. Gemalchari, Online privacy concerns and privacy management: a meta-analytical review, J. Commun. 67 (1) (2017) 26–53, https://doi.org/10.1111/jcom.12276.
[19] P. Li, H. Cho, Z.H. Goh, Unpacking the process of privacy management and self-disclosure from the perspectives of regulatory focus and privacy calculus, Telematics Inf. (2019), https://doi.org/10.1016/j.tele.2019.04.006.
[20] R. Wilton, After Snowden – the evolving landscape of privacy and technology, J. Inf. Commun. Ethics Soc. 15 (3) (2017) 328–335, https://doi.org/10.2307/4149970.
[21] H.S. Satra, Freedom under the gaze of Big Brother: preparing the grounds for a liberal defence of privacy in the era of Big Data, Technol. Soc. 58 (2019) 101160, https://doi.org/10.1016/j.techsoc.2019.101160.
